From Cyber-Utopia to Cyber-War.

Normative Change in Cyberspace.

Dissertation
zur Erlangung des akademischen Grades

doctor philosophiae (Dr. phil.)

vorgelegt dem Rat der Fakultät für Sozial- und Verhaltenswissenschaften der Friedrich-Schiller-Universität Jena

von Matthias Schulze (M.A.) geboren am 28.03.1986 in Weimar

15.03.2017

Gutachter
1. Prof. Dr. Rafael Biermann (Friedrich-Schiller Universität Jena)

2. Dr. Myriam Dunn Cavelty (ETH Zürich)

3. Prof. Dr. Georg Ruhrmann (Friedrich-Schiller Universität Jena)

Tag der mündlichen Prüfung: 08.08.2017

Table of Contents

Acknowledgement

The purpose of this acknowledgement is to clarify my subjective position in front of the reader, as criteria for good qualitative research suggest (Creswell, 2012, p. 51). Since this is a qualitative case study, the subjective position of the researcher always is a potential source for bias.

Writing this thesis was a tremendous experience. It allowed me, to scientifically engage with the technology and medium I grew up with. I experienced much of the evolution of the World Wide Web with the eyes of a curious teenager. I became a cyber-utopian believing in the grand vision that the Internet could foster global cooperation, exchange of ideas and democratization. Speaking for the first time with a total stranger from the other side of a globe over the Internet was (and is) a powerful experience. Being able to digitally access almost any written book, music or piece of art within a matter of seconds still is remarkable. We seldom acknowledge the fact that for the first time in human history, we can access almost all human knowledge with a mouse click. I strongly believe that the global communication enabled by the Internet allows us to solve global problems like climate change, pollution or economic inequality. Having said that, I am skeptical of any actor who tries to control or manipulate this global conversation, either via censorship, surveillance, digital-disruption (I.e. cyber-war) or any other means. At the same time, this thesis allowed me to confront my early utopian ideas about cyberspace and reflect upon them more deeply. While researching this thesis and struggling with the problems of hacking, terrorism and inter-state espionage, much of my cyber-utopian euphoria declined.

National security actors indeed have a point when they warn about the national security implications of the Internet and this work allowed me to better understand their position. I understand why surveillance of Internet data-streams is a political demand and acknowledge, that it might (!) have some positive effects on catching terrorists. Surveillance is neither good nor bad, but it depends on the political governance, as surveillance scholar David Lyon argues. I do believe that the conduct of intelligence agencies is necessary to protect democracy from outside forces, as long as it is transparent, accountable, proportional and under independent evaluation. "Given the history of abuse by governments, it's right to ask questions about surveillance, particularly as technology is reshaping every aspect of our lives" as President Barack Obama once said (Obama, 2014). We must be able to evaluate the costs and benefits of Internet control systems, which is currently complicated because of secrecy. We must critically ask the question whether the minimal gain of security is worth the tremendous financial and political costs Internet

surveillance has for democratic states and global civil society, especially given the danger that these tools fall into hand of an authoritarian leader with little regard for checks and balances. While the Internet has the enormous potential of uniting mankind by creating a real-time global conversation that might enable us to solve global challenges, chances are that human ignorance, fear, populism and unchecked powers threaten the existence of the Internet. There are powerful forces at work that try to control the global conversation. This thesis sheds light on these dynamics from a critical perspective.

As you will see, this work is highly interdisciplinary, drawing from a variety of field such as International Relations, Political Science, Critical Security Studies, Sociology, Science and Technology Studies and History. During the doctoral seminars with my supervisor and other colleagues I often encountered a fundamental critique with my work along the lines "well, all that technological stuff is quite interesting, but where is the political science in it?" I agree, and apologize, that my presentations during these years were somewhat "techy" and "nerdy" and not really "political sciency". To respond to this critique, I argued that the individual parts may not be political science, but the big picture will be (and hopefully is). While studying technology scholars such as Lawrence Lessig and Landgon Winner, I discovered two important insights. First, we should think politics bigger: not just in terms of formal political institutions and laws but also in terms of hard- and software. Technologies are politics. This will become clearer during the thesis. Second, the inventor of cybernetics Norbert Wiener argued that "it is these 'boundary regions' of science which offer the richest pickings to the researcher. This is because they are ideas where the traditional methods simply don't work" (Naughton, 1999, p. 62). That is why I am a strong advocate of an interdisciplinary perspective.

I want to thank the following persons (in no particular order). I want to thank Anna Fritsch for countless times of psychological and emotional support through all the ups and downs such a long project has. I am also thankful for inspirational comments and the endless proof-reading sessions by Charlie Fritsch. I want to thank my supervisor Prof. Rafael Biermann for being so open and enthusiastic about my interdisciplinary research style, allowing me to explore the boundaries of political science. The feedback was always super constructive and the working atmosphere at the department excellent. I want to thank Dr. Myrian Dunn-Cavelty for being so nice to evaluate my work and give valuable comments. I also want to thank my colleagues at the department, Sven Morgen for constantly thinking outside the box and maintaining a constructive critical stance towards many ideas, Carolina Rehrmann for the uplifting work-spirit, Marianne Beyer and Jana Thierbach for almost everything that had to be organized, managed or solved. I want to

thank my doctoral colleagues, Johannes Gold for always excellent critique and discussions and Christian Opitz for proof-reading and the positive spirit. I really appreciate it. I also want to thank the student assistants at the department for political science in Jena, among them Katrin Pakizer, Helena Falk, Katrin Oestmann, Frank Wieber, Thea Schatz and Torben Kruse who scanned endless pages and thus supported this research.

Academically, I want to thank Miles Townes, whose paper on TCP/IP norms was one of the first papers from an IR perspective of which I thought, that "this is it", the point to start this dissertation. Miles pointed me in the right direction, combining norm research and Internet history. Ronald Deibert and the team at the Citizen Lab initiated my interest in Internet control practices of states and offered many insights during my research trip in summer 2015 to Canada. Among them Erik, Christopher and Ben with whom I had endless discussions (and Poutine). I am also very grateful to Prof. Leonard Kleinrock, Dr. Vinton Cerf, Dr. Steven Crocker who kindly responded to my Emails regarding the technicalities of the Internet protocols.

Matthias Schulze
Leipzig, February 2017

About this digital version

This digitally published version is the original Ph.D. thesis that was handed-in in March 2017. It contains all original graphics, a more detailed description of the causal mechanisms and all the little errors that the proof-readers and I did not discover. This version is published under an open commons license, mimicking the original spirit of the Internet. There will be a slightly edited book version containing a more streamlined and refined text, fewer graphics and hopefully less punctuation errors. This will come out later as a 2nd, revised print edition, for those of you who still prefer physical books.

Matthias Schulze,
Berlin, June 2018

Abstract

This dissertation analyzes a normative change in state perception and political action towards the Internet. This change is currently reflected in certain measures aimed at the exercise of control and state sovereignty in and over cyberspace. These include phenomena such as the total surveillance of data streams and the extensive collection of connection data by secret services, the control (political censorship) and manipulation of information (information war) as well as the arms spiral around offensive cyber capabilities to disrupt and destroy information infrastructures. States face a loss of control that they want to compensate for. The phenomenon of the perceived loss of control and the establishment of a norm of control (filter and monitoring technology) is equally evident in various democratic and non-democratic states, as various studies show.

This militarized perception of the Internet is remarkable in so far as Western politicians used to perceive the same Internet technology in the 1980s and 1990s in a completely different way. Back then the lack of state control was seen as desirable. Instead of controlling and monitoring all aspects of the Internet, a "hands-off" and laissez-faire idea dominated political behavior at the time: the possibilities of democratization through information technologies, the liberalization of authoritarian societies through technology and the free availability of global knowledge. The idea of national control over communications technology was considered innovation-inhibiting, undemocratic and even technically impossible. The topic of this work is the interaction between state power and sovereignty (e.g. political control through information sovereignty) and digital technologies. The research question is: Which process led to the establishment of norms of control and rule (surveillance, censorship, cyber-war) with regard to the medium Internet? Furthermore, the question arises: What are the implications of this change in standards for the fundamental functioning of the Internet? The aim is to examine in detail the thesis of the militarization of cyberspace empirically on the basis of a longitudinal case study using the example of Internet development in the USA since the 1960s. An interdisciplinary and multi-theoretical approach is chosen from constructivist norms research and the Social Construction of Technology approach.

List of Abbreviations

ACLU	American Civil Liberties Union
ALOHANET	Aloha Network
ARDA	Advanced Research and Development Activity
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
AT&T	American Telephone and Telegraph Company
BBN	Bolt, Beranek and Newman
BND	Bundesnachrichtendienst
BSD	Berkeley Software Distribution
C3I	Command, Control, Communications and Intelligence
CDA	Communications Decency Act of 1996
CERN	Conseil Européen pour la Recherche Nucléaire
CERT	Computer Emergency Response Team
CNA	Computer Network Attack
CNCI	Comprehensive National Cybersecurity Initiative
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operation
DARPA	Defense Advanced Research Projects Agency (same as ARPA)
DDoS	Distributed Denial of Service (attack)
DHS	Department of Homeland Security
DNS	Domain Name System
DoD	Department of Defense
DoJ	Department of Justice
DPI	Deep Packet Inspection
EFF	Electronic Frontier Foundation
EPIC	Electronic Privacy Information Center
EW	Electronic Warfare
FBI	Federal Bureau of Investigation
FBI-DITU	FBI Data Intercept Technology Unit
FCC	Federal Communications Commission
FISA	Foreign Intelligence Surveillance Act
FISAAA	Foreign Intelligence Surveillance Act Amendment Act 2008
FISC	Foreign Intelligence Surveillance Court
FTP	File Transfer Protocol
FY	Fiscal Year
GCHQ	Government Communications Headquarter
GII	Global Information Infrastructure
GWOT	Global War on Terror
HTML	Hypertext Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
HUMINT	Human Intelligence
IAB	Internet Activities Board
IC	Intelligence Community
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technologies
IETF	Internet Engineering Task Force
IMP	Interface Message Processor
INWG	International Network Working Group
IO	Information Operation

IP	Internet Protocol
IPO	Initial Public Offering
IPTO	Information Processing Techniques Office
IRPTA	Intelligence Reform and Terrorism Prevention Act 2004
IRTF	Internet Research Task Force
ISP	Internet Service Provider
IW	Information Warfare
IXP	Internet Exchange Point
JFCC-NW	Joint Functional Component Command for Network Warfare
JSOC	Joint Special Operations Command
JTF-CND	Joint Task Force Computer Network Defense
JTF-CNO	Joint Task Force Computer Network Operations
LAN	Local Area Network
MILDEC	Military Deception
MILNET	Military Network
MIT	Massachusetts Institute of Technology
NCP	Network Control Protocol
NCR	National Research Council
NII	National Information Infrastructure
NIST	National Institute of Technology
NSA	National Security Agency
NSF	National Science Foundation
NSFNET	National Science Foundation Network
NSL	National Security Letters
NSPD	National Security Presidential Directive
NWG	Network Working Group
OPSEC	Operations Security
PFF	Progress and Freedom Foundation
PSYOP	Psychological Operation
R&D	Research & Development
RFC	Request for Comments
RMA	Revolution in Military Affairs
ROC	Remote Operations Center
SAGE	Semi-Automatic Ground Environment
SATNET	Satellite Communication Network
SIGINT	Signals Intelligence
SRI	Stanford Research Institute
SSL	Secure Socket Layer
STRATCOM	Strategic Command
TAO	Tailored Access Operation
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TIA	Total Information Awareness Program
UAV	Unmanned Aerial Vehicles
UCLA	University of California, Los Angeles
URL	Uniform Resource Locator
VPN	Virtual Private Network
WELL	the The Whole Earth 'Lectronic Link
WWW	World Wide Web

List of Tables and Graphics

1. Introduction

I am disturbed by how states abuse laws on Internet access. I am concerned that surveillance programmes are becoming too aggressive. I understand that national security and criminal activity may justify some exceptional and narrowly-tailored use of surveillance. But that is all the more reason to safeguard human rights and fundamental freedoms."
Ban Ki-moon

Let me start with a thought experiment. Just imagine that in the 1970s, Russian agents had been able to photocopy large portions of the file-cabinets from the US Office of Personnel Management (OPM). This data would have included sensitive information such as fingerprints, social security IDs, postal addresses and national security clearance of the majority of staffers within the political bureaucracy. Imagine further, that Russian spies had been able to photocopy the campaign files (funding, strategy etc.) and personal communication of a democratic party during an election, using this material to blackmail one of the candidates.

Imagine further, that like the Stasi in the former German Democratic Republic, domestic and foreign intelligence agencies strive to monitor every communication channel in their own country *and* in other countries as well. Imagine that intelligence agencies would demand capabilities to send covert agents or saboteurs to critical infrastructures like dams, electricity plants or water supplies. These saboteurs would plant remote-controlled bombs, waiting to be activated on demand, destroying or disrupting the operation of the facility.

Finally, imagine that the KGB and every other intelligence agency in the world had placed surveillance bugs *everywhere*: on every person, in every home, car, office and government building in every country on earth and that these could be switched on from afar. Imagine that intelligence agencies worldwide would lobby their governments to receive capacities to switch on these surveillance bugs on demand.

These events sound like a Tom Clancy novel but all of them are based on real empirical events that happened, not in the Cold War, but in the last few years. These events did not happen in the physical world, but in the *digital* domain. For example, in 2014 the OPM was hacked and sensitive information of US Government officials had been stolen over the Internet (Office of Personnel Management, 2015). In 2016, Russian hackers stole sensitive information from the Democratic National Committee during the US Election (Harris, 2016). The planting of surveillance bugs everywhere refers to smartphones or smart home appliances connected to the Internet. Most states equip their intelligence

agencies with special Trojan software and legal competences to "cyber-attack"[1] these devices with malware, to turn on the microphone, extract private data or to save every keystroke on the device. This practice is not limited to national territory but also includes the jurisdiction of other states because these bugs can be sent electronically.

The wiretapping of the entire communications infrastructure refers to the Snowden leaks of 2013, when it was uncovered that US Intelligence agencies where copying large portions of Internet communication to intercept communication of both citizens and international users. Whereas the Stasi monitored only audio phone calls and relied on informants (Foschepoth, 2013), Internet communication contains all types of audio-visual or behavioral data. If one would print all this data on A4 paper, it would require an estimate of 42 billion file-cabinets to store it. The Stasi had around 48000 file cabinets in its entire archive (Stasi versus NSA, 2017).

Why do I present these examples? Because they are examples of how states begin to control the Internet and digital technologies, which this thesis is about. They offer a glimpse of how states behave in cyberspace. When one picks up a random newspaper, chances are that one discovers headlines such as "we're on the verge of cyber-war" (Giamoia, 2016), "how America can beat Russia in Cyber War" (Singer, 2017) or intelligence agency X "wants to start cyber-counterattacks" (DPA, 2017). Now, more than ever, the Internet is understood in terms of *war*: "cyber-attacks", "arms race in cyberspace", "cyber-deterrence" and more have become buzzwords in public discourses. We are taking it for granted that "cyber-soldiers" from Russia or the National Security Agency (NSA) hack into the digital infrastructures, threatening to shut down power-grids or worse.[2]

The premise of this thesis is that we witness an ongoing *militarization* and securitization of the Internet (Deibert, 2003). This means that the Internet is more and more understood as a domain of national security and that surveillance, espionage, sabotage and hacking have become the preferred tools of statecraft. More and more states perceive the Internet as a national security problem and try to deal with this threat with military and intelligence capabilities (Shafqat & Masood, 2016). I argue that the militarization of cyberspace with practices of Internet surveillance, cyber-attacks and

[1] Defined as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks" (Singer & Friedman, 2014, p. 68).

[2] Observe that the "cyber"-prefix is used in all kinds of way in current discourses, which often is problematic because it subsumes highly diverse issues under one umbrella. I agree with Thomas Rid who argues that the use of "the cyber" as a noun should be avoided and often indicates a superficial understanding of topic (Rid, 2013, p. ix). The author apologizes in advance for the extensive use of the cyber prefix throughout the thesis. I will use hyphens like cyber-security, cyber-attacks unless I refer to quotations.

digital espionage have become so normalized in the last few years, that we do not fully understand their meaning and overall societal impact. That is why I have presented current events with the Cold War metaphor to reveal how extraordinary they are. We have become so accustomed to this militarization that there is little public debate about questions of whether it should be considered a norm that states hack each other's elections with cyber-attacks or whether it should be considered normal that democratic and authoritarian regimes likewise hack the Internet infrastructure to monitor global communications both domestic and abroad. Should we consider it a norm that democratic and authoritarian states develop specialized malware to hack into smartphones to turn them into surveillance devices? All these questions should be asked yet there is very little public debate about this.

All of this indicates that states controlling the Internet has become normalized. The militarization of the Internet has become a norm, a standard of state behavior. Some even argue that "the struggle to control cyberspace is defining American national security in the twenty first century" (Harris, 2014, p. Prologue).[3] The norm states that it is the appropriate right of a state to control cyberspace itself, or information stored or send therein, globally as well as domestically. Control derives from the French word "contreroller" and means in its etymological sense "to check, to verify, to register, to regulate or to exert authority" (Etymonline, 2016). States try to exercise authority over the Internet with the means of digital surveillance, espionage and cyber-warfare[4] capabilities. These measures follow a security logic and are often legitimized with threats from cyber and terrorist attacks. For example, the former German minister for the interior, Hans Peter Friedrich argued that "a loss of control monitoring communication of criminals must be compensated by new technological and legal [Internet surveillance] means" (KGP, 2013).[5] Another example is the Internet surveillance program by British intelligence agencies leaked by Edward Snowden which, by no accident, is called "mastering the Internet" (Goertz & Obermaier, 2013). These two examples are indicators of the norm of control I will analyze in this thesis.

Why is this relevant? Because the norm of controlling cyberspace stands in conflict with many norms of democratic societies. The ongoing trend of the militarization of cyberspace is the reason why former UN General Secretary Ban Ki-moon warns in the entry quote about these practices and their impact on human rights. Internet surveillance

[3] Since some ebooks only have dynamic page numbers that depend on the font size, I can only refer to the chapter of the book as a source.
[4] "Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke & Knake, 2010, p. 6). Intelligence collection is another purpose of cyber-war.
[5] Square brackets always mean inclusions by the author.

can have severe consequences for human rights, the rule of law and the functioning of democracies. In December 2014, the UN General assembly reinforced these concerns with a resolution (68/167) "The right to privacy in the digital age." The UN is:

> "deeply concerned at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights […]" (United Nations General Assembly, 2014a).

For example, controlling content on the Internet via filter software or "truth ministries" checking for "fake news" contests the norm that censorship should not take place in democracies. Suspicionless or preemptive mass surveillance of citizens' Internet data streams contests the norm that such intrusive surveillance measures should be based on a probable cause. That is why several constitutional courts and the European Court of Justice argued that the mass retention of Internet meta-data "exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society" (DW, 2016). Surveillance is potentially harmful for democracies because it can undermine the trust in government and limit citizens' freedom of association and expression, as some social psychological studies show (Turner, 2016). More so, clandestine cyber-war activities blur the dichotomy of war and peace and domestic and foreign. They thus limit the democratic control of the military and intelligence agencies. Controlling the Internet in terms of censorship, by manipulating information stored therein, or disrupting the information space in other country, for example during elections, invites for abuse. While most liberal democracies still have checks and balances in place, authoritarian regimes engage in the same practices without much restraint and oversight. That both democratic and authoritarian states adopt very similar measures to control cyberspace is very peculiar and one of the puzzles addressed in this thesis.

1.1 Puzzle & Research Question

The trend that more and more states begin to control the Internet and the information therein is a somewhat puzzling development for three reasons.

First, it is peculiar that both liberal-democratic and authoritarian regimes more and more adopt the *same* perspective on cyberspace and begin to control the Internet with very similar techniques and practices. The behavior of both liberal-democracies and authoritarian regimes in cyberspace is in fact very similar, as Betz and Stevens argue:

> "What is rarely acknowledged in Western security discourse is that recent moves by democratic governments into these regulatory spaces have much in common with the practices of other states whose control regimes are often the subject of Western opprobrium and condemnation" (Betz & Stevens, 2012, p. 67).

For example, most Internet surveillance activities in Western countries are legitimized with the war on terror. Cyber-war activities are legitimized with external threats like Russia and the perceived loss of control. Authoritarian regimes likewise use terrorism as a pretense to exercise more control over the Internet. However, once enabled these activities tend to "mission-creep" to areas besides fighting terrorism, for example tracking minorities (Muslims) or the political opposition.

Likewise, cyber-war and surveillance feature prominently in most recent national security strategies of democratic and nondemocratic states alike and are in fact very similar in their goals, means and even terminology (Shafqat & Masood, 2016). For example, with its Investigatory Powers Bill, the United Kingdom introduced one of the most far reaching Internet surveillance laws in a democracy. The bill has a close resemblance to the legal regimes in China and Russia and thus was struck down by the European Court of Justice as being in violation of democratic norms (Woollacott, 2016).

Although we mostly hear of Russian or Chinese hacking in the US or Europe, Western intelligence agencies are similarly active abroad as many of the Snowden leaks of 2013 indicate (Intercept, 2014). Intelligence agencies from liberal and authoritarian regimes even struggle with similar problems and lobby their government for more capacities, for example allowing them to break encryption. Currently, we witness a worldwide initiative, led by Germany, France, the United Kingdom and the USA for "exceptional access" into cryptographic messengers. Encrypted smartphone apps circumvent Internet surveillance and thus intelligence agencies lobby for capacities to circumvent encryption, for example by using malware, i.e. cyber-attacks (Schulze, 2016b). Meanwhile Russia (Szoldra, 2016) and China (Gierow, 2016) adopted very similar measures by regulating the use of encryption by their citizens. While western governments want to break encryption to hunt terrorists, Russia and China use the very same techniques to crackdown on dissidents. The goals might differ, but the means are the same.

The same can be seen with censorship, which is a traditional tool of authoritarian rule, but is currently actively demanded in many Western states, for example to deal with pornography, propaganda or what is nowadays called "fake news" (Schulze, 2016a). I argue that all these phenomena are a indicators that state control over the Internet has become a new, so-called "dark" norm. Dark norms contest traditional liberal democratic

norms which most Western democracies (still) adhere to (Heller, Kahl, & Pisoiu, 2012). It is very puzzling that both liberal democracies and authoritarian regimes show a very similar behavior in cyberspace. We might expect information controls, censorship and cyberspace control in authoritarian regimes, because it has been an integral part of these regimes for ages. Controlling information and information spaces is a means of power to stabilize a regime. The fact that many democratic countries nowadays demand similar capabilities is curious. Democracies normally adhere to fundamental norms such as freedom of speech, privacy rights and laws like the 4th amendment that guarantees protection from unnecessary state surveillance of private lives and communications. Thus, one would expect a certain *democratic constraint*. Suspicionless surveillance violates core rule of law principles such as the need for a probable cause before surveillance is initiated. These norms are contested by Internet mass surveillance and censorship practices which target everyone without suspicion. The question is, why do both democratic and authoritarian states adopt similar measures regarding the Internet?

There is a second puzzling aspect that becomes only apparent if one considers the behavior of democratic states in cyberspace *before* the war on terror. During the 1980s and 1990s, liberal democracies had a very different position regarding state control of information technologies. Former US Secretary of State George P. Shultz argued in 1985 that controlling information technologies is both democratically and economically inappropriate. He argued that information and communication technologies (ICT) bring economic advantages and important technical developments such as micro processing. If authoritarian states restrict or control these technologies, they would fall behind economically. If they allowed ICT to spread in their country, they might lose the information monopoly and censorship capacities which they require to maintain order. ICT would create a "dictator's dilemma": either authoritarian states allow ICT and lose control over their population and catch up economically. Or they continue blocking and censoring information and maintain power, but loose economically. The idea that states could or should control the new ICT and information was perceived as bad for innovation, undemocratic and even impossible (Kedzie & Aragon, 2002). In other words, during the 1980s and 1990s the aforementioned democratic constraint regarding surveillance and ICT control actually existed and was promoted by key politicians. Former President Bill Clinton said in 2000: "Trying to control the Internet is like trying to nail Jell-O to the wall" (Allen-Ebrahimian, 2016).

This indicates a completely different perception of the Internet and other information technologies. In the past, the Internet was not militarized. It was not seen predominantly as

a national security threat. During the 1990s, the Internet was primarily seen as a tool for liberalization and democratization and not as a method for warfare and surveillance. Back in the day, democratic regimes actively argued that democracies *should not* control these technologies and argued for democratic constraint, whereas nowadays they want to control cyberspace like their authoritarian counterparts. Why do democratic states adopt norms that are the complete opposite of what they preached in the past?

The third puzzle includes the combination of the militarization and the technical features of the Internet itself. Militaries worldwide try to position themselves as dominant actors within cyberspace, aiming to gain more and more control over the technical and social infrastructure. At the same time, they are ill-suited to do so because of technical features of the Internet. The Internet is managed by private entities and is operating on a *global* scale beyond the jurisdiction of one single state. Internet governance studies diagnose a creative chaos of different actors with different responsibilities, indicated by the dominant research question in this field: "who controls the Internet?" (Goldsmith & Wu, 2008; Eriksson & Giacomello, 2009). That is because the Internet was designed not to be in possession of one entity alone. The Internet protocols actively prevent control of one single entity, as later chapters will show (see chap. 4.1.3.1 Artifact: Internet Protocols and Norms). Additionally, the Internet knows no borders and no separation between the domestic and the international, which alters traditional notions of territorial defense, the prime duty of militaries. Therefore, the Internet cannot be defended in the same way as a country, by building fortifications around critical infrastructure. Thus, the military is neither in a logical position to defend cyberspace, nor do most militaries have the technical capacities to do so (at least until a few years ago). In contrast, private companies and Internet service providers (ISP) are technically better suited to provide essential cyber-security. For example, both German and US forces struggle with recruiting, because cyber-security jobs in the private sector are more lucrative (Wiegold, 2016). Some argued that the militaries' relationship to the Internet is that of a colonial force, coming in from the outside, claiming to be in charge of security (Barlow, 1996). It is puzzling that an entity that is in no logical position to control the technology tries do so because this process costs a lot of money and resources could be spend on a more civic cyber-security.

It is puzzling that within the last 30 years our meaning and perception of the Internet has made a 180 degree turn. Whereas during the 1990s, the Internet was seen as a positive force of democratization, a global library that would benefit education and would usher in economic growth, new innovations, new forms of governance and would ultimately bring mankind closer together, current discourses describe the complete opposite. Discourses on

cyber-war and surveillance often have the character of doomsday scenarios or operate with dystopian predictions (Lawson, 2011). In other words: whereas the Internet was once described as a digital, cyber-utopia, we now only see it in terms of war, cyber-war. This change of perception and state behavior, *from cyber-utopia to cyber-war,* is what this thesis is about.

The (preliminary) guiding questions of this dissertation are: *How can we explain this change? How could the norm of Internet control become dominant in Western democracies?* I argue that the utopian perspective of the 1990s and the current dystopian or war perspective to the Internet resemble two competing world views or paradigms, which guide state-behavior towards the Internet. Thus, the change from cyber-utopia to cyber-war is understood as a *paradigm and norm-change in cyberspace*. This paradigm change alters what the Internet means for states and what appropriate state behavior towards this technology is. I argue that Internet control practices such as mass surveillance and cyber-war in both democratic and authoritarian states are part of the same mind set, which is promoted by a particular understanding of the Internet. Mary McEvoy Manjikian called the military narrative towards the Internet "cyber-realism", and the utopian/democratic narrative "cyber-utopianism" (McEvoy Manjikian, 2010). I will use her terminology but advance her argument. I argue that these two paradigms propose and advocate different norms: cyber-realism advocates for Internet control of states in terms of more surveillance and cyber-war capabilities whereas cyber-utopianism argues that states ought not control cyberspace and that governance of this technology should lie in the hands of decentralized civil-networks, not states.

Taking into account these theoretical insights, the research question is reformulated: *Which process leads to the development of Internet control as the dominant norm for states in dealing with Internet?*

1.2 Literature Review

Having outlined the research question, the task is to determine what research has to say about the militarization of the Internet and the dominance of Internet control norms.

Political science and International Relations (IR) are late-comer to Internet studies (Margetts, 2013). Until the mid 2000s, researching the technology ranked not high. Wellman describes three generations of Internet studies (Wellman, 2004). The first was driven by utopian ideas of an information or network society (Castells, 1999) bringing a new form enlightenment. This was mostly dominated by sociologists, futurologists, media-studies (focusing on use) and computer science (focusing on protocol design and

development), as well as early Internet advocates themselves. Since the end of the millennium, policy-makers, academics and economists have began to see the relevance of this new technology and asked for systematic study, ushering in the second generation of Internet studies (Wellman, 2004). Here, the first questions about Internet governance came up, which since then has been one major approach to study the Internet within political science (Hofmann, 2005). The general theme of research was the impact of ICT upon society. Since 2004, we have been able witness the third generation, which is asking for general theories. In the recent *Oxford Handbook of Internet Studies*, Dutton argues that the key issues of Internet studies can be summarized with the question: Who shapes the Internet, why and with what implications for whom (Dutton, 2013a)?

As one of the first works, Lawrence Lessig's influential book *Code: And other Laws of Cyberspace* theorized the interrelationship of law, policy and technology and is seen by many as a catalyst for political science, turning its attention towards the Internet (Lessig, 2000). For political scientists, the first issues were questions about the relationship between the Internet and democracy (Margetts, 2013), but systematic approaches were lacking. In 2006, Eriksson and Giacomello published a provoking article: "The Information Revolution, Security, and International Relations: (IR)relevant Theory?", pointing to the fact that IR theory did not have much to say about the Internet (Eriksson & Giacomello, 2006). This changed, however, with the hacking incident in Estonia 2007 (see appendix. Table 9. List of Internet Milestones and Security Incidents). Events like the 2011 Arab Spring or the Wikileaks cable-gate triggered an increased interest in Internet-related phenomena. Studies include the use of social media by social movements (Etling et al., 2010; Hofheinz, 2011), or in presidential campaigns (Harfoush, 2009; Lilleker & Vedel, 2013) and politics in general. Around the same, time a fourth-generation of Internet studies was developing. These studies aimed to demystify early utopianism and focused on how authoritarian and democratic regimes use the Internet to control their citizens (Deibert et al., 2008; Morozov, 2011) or focused on the negative aspects of digitalization and globalization in general (Keen, 2014).

Since the revelation of Edward Snowden in 2013, there has been an increased interest in power-politics and surveillance studies (Murakami Wood, 2015) and more and more dissertations are produced on this issue. It can be argued that within political science, there are three theory-inspired branches of studying the Internet: Internet governance, IR-realism and constructivism. Governance, inspired by neo-liberal institutionalism, focuses on Internet governance international bodies such as the EU or UNO (Betz & Kübler, 2013; Mueller, 2010). These works often focus on the question: *"Who controls the Internet?"*

(Hofmann, 2005; Goldsmith & Wu, 2008; Eriksson & Giacomello, 2009) and illuminate different answers. There are studies on Internet governance within the European Union (Radu, 2015; Kremer & Müller, 2014) global bodies such as ICANN (Mueller, 2010) or the different standard consortiums like the World Wide Web Consortium (W3C), the Internet Engineering Task Force (IETF), the Regional Internet Registries (RIRs), the International Telecommunication Union (DeNardis, 2009; Denardis, 2013). Other topics include questions of good or effective governance (Khazaeli & Stockemer, 2013), Internet security (Mueller, Schmidt, & Kuerbis, 2013; Schmidt, 2014), the comparison of different national approaches (Giacomello, 2005) and questions of legal ownership (Mueller, 2005). The problem with this body of research is that it is not that much focused on change and thus not that much suited for this project. Additionally, the security perspective on Internet governance only came up recently (Wolff, 2016).

Besides the *who* question, there is also the question: *"how to control cyberspace?"* It is often tackled by interdisciplinary research inspired by computer science (Deibert & Crete-Nishihata, 2012). Especially noteworthy here are the American Berkman Center and Canadian Citizen Lab. This branch of research focuses on the modality of Internet controls, for example via technical *censorship* (Rundle & Birdling, 2008; Deibert et al., 2008; Zittrain & Palfrey, 2008; Zuckerman, 2010b) or legal control of corporations and Internet intermediaries (Roberts & Palfrey, 2010; Zuckerman, 2010b; Goldsmith & Wu, 2008). Researchers from the Citizen Lab and from the OpenNet Initiative pioneered the work on researching Internet and information controls[6] and they identified the historical evolution of these controls which are a product of the militarization of cyberspace (Deibert et al., 2010). Historically, controlling the Internet or information thereon via censorship could first be witnessed in authoritarian regimes. The great Firewall in China or Middle-Eastern countries where religious, political or sexual contents are blocked from the Internet, are examples. The second generation of Internet control included laws that regulate appropriate information production, diffusion and consumption on the Internet. An example are slander-laws that erase (take-down) indecent material from the web and making website hosts responsible for user-generated content so that they have to face legal consequences if the state wishes so. These controls are present in democratic and authoritarian regimes, although they take different forms (copyright for example). The third generation of information controls is more recent and more offensive. New

[6] "Actions conducted in and through cyberspace that seek to deny, disrupt, manipulate, and shape information and communications for strategic and political ends. Information controls include an array of technologies, regulatory measures, laws, policies, and tactics. These can include media regulation, licensing regimes, content removal, libel and slander laws, and content filtering" (Deibert & Crete-Nishihata, 2012, p. 343).

techniques aim not just at denying certain information or Internet access (like censorship) but try to contest it, to produce counter-information (propaganda) as well as to disrupt online activities with cyber-attacks (Deibert et al., 2010). Disrupting the website of the political adversary during an election or spreading "fake news" are the latest iteration of this.

A second approach to study the Internet within political science is IR-realism. Realist scholars tend to focus on questions of state-sovereignty in cyberspace (Betz, 2012; Betz & Stevens, 2012) or the modalities of power (Nye, 2010; Nye, 2011). There is also a body of literature dealing with national security issues, often indicated by adding the "cyber" prefix: cyber-security (Nissenbaum, 2005; Geers, 2011), cyber-terrorism (Lewis, 2002) and related concepts such as cyber-deterrence (Libicki, 2009). The evolution of this body of literature will be traced in a following chapter in order to keep this section rather short (see chap. 4.4 Information Warfare and the Origin of Cyber-Realism).

Within realism, there is the mostly military-inspired discourse on cyber-warfare to which this thesis also contributes. Dunn-Cavelty (Dunn Cavelty, 2010) describes two general sets of literature bodies: one military and one academic. I would also add a legal body of literature which focuses on the compatibility of cyberspace with international law. Military scholars (Arquilla & Ronfeldt, 1993; Molander, Riddle, & Wilson, 1996; Pfaltzgraff & Shultz, 1997; Papp & Alberts, 2000) theorized cyber-war in terms of a fundamental revolution in military affairs (RMA), speculating about its game-changing nature. They argued that cyberspace is ultimately a new phenomenon that cannot be grasped by traditional concepts of war and peace and therefore negates many established truths (like the offense-defense balance, the concept of retaliation and deterrence). There is also a critical generation of academic literature that questions whether cyber-war is indeed war (Rid, 2013; Healey & Grindal, 2013; Valeriano & Maness, 2015; Kaplan, 2016).

A third political science approach to the Internet is driven by constructivism. IR-constructivism is dominated by the securitization framework (Buzan, Waever, & Wilde, 1997), which analyzes how the Internet and related phenomena such as hacktivism, crime and war are rhetorically constructed as national security threats (Deibert, 2003). There already is a substantial body of literature analyzing the social framing of cyberspace. These studies focus on language aspects, such as doomsday narratives (Lawson, 2011; Dunn Cavelty, 2013b), metaphors (Lawson, 2011; Hansen & Nissenbaum, 2009) and the general mechanisms of threat policy and framing (Dunn Cavelty, 2007; Dunn Cavelty & Jaeger, 2015; Morozov, 2009). These are studied in different countries like Sweden (Eriksson, 2001), the USA (Bendrath, 2003) and Germany (Schulze, 2012) and after cyber-security

events such as the NSA-scandal[7] (Schulze, 2015). Probably there are other country studies the author is unaware of. There are also first attempts of theory building, for example by using Ulrich Becks "risk society framework" to explain Internet threats (Aradau, 2010; Barnard-Wills & Ashenden, 2012) or Bruno Latour's Actor Network Theory (Dunn Cavelty, 2015).

Surprisingly, another branch of constructivism has little to say about cyber-war and the Internet: *norm-research*. Although many practitioners and scholars agree that there are norms in cyberspace and that actors, for example conflict parties should be guided by legal principles (Grove, Goodman, & Lukasik, 2010) such as the law of armed conflict (Schmitt, 2013) or due-diligence duties (Bendiek, 2016), detailed norm-research studies are lacking. Recent critical norm research has discovered the existence of dark norms within the war on terror that contest traditional liberal norms, for example in terms of the reemergence of torture, but digital surveillance and cyber-war have not been systematically studied yet (Heller & Kahl, 2013). There is a gap in the literature this thesis tries to fill.

Within norm research, there are two exceptions however, which are important foundations for this thesis. First, Miles Townes was among the first who combined the constructivist framework of norm-diffusion (see chap. 2.1 Norms and Theories of Normative Change) with the global spread of the Internet. Townes argues that "the Internet embodies prescriptive decisions about how networking technology ought to work, and what privileges and responsibilities parties to the technology ought to have; these decisions have important political consequences" (Townes, 2012, p. 44). He correctly argues that academic norms, and not military ones shaped the design and global diffusion of the Internet. He does not really specify what these norms are in detail and where they come from. With high detail, he shows the global diffusion of networking technologies and exemplifies the working of the norm-life cycle until the early 1990s, but not further. Furthermore, he does not analyze the consequences of these norms and only focuses on the academic epistemic community. Policy or military norms are neglected. Nevertheless, his paper is highly insightful and was a major source of inspiration for this thesis.

Another source of inspiration was the exemplary work of Mary McEvoy Manjikian, who observed in her study three distinct narratives, or the "origin stories" of cyberspace: a utopian, a liberal and a realist reading of the technology. She focused on a narrative perspective, on creation stories "to describe cyberspace—its essence, its utility, and its relation to issues of state power" (McEvoy Manjikian, 2010, p. 382). She analyzes how these origin stories frame cyberspace and infers from them implications for IR theory in

[7] National Security Agency.

terms of power, territory and citizenship (McEvoy Manjikian, 2010). Her argument is that the utopian narrative became replaced by Realpolitik, which is another version of the militarization thesis that also underlies my argument.

Her focus is not so much on norms though. I will build on her assessment and initial typology of cyber-utopianism, cyber-liberalism and cyber-realism and complement these narratives with a paradigm perspective. This means that it is not just about the discursive narrative, but also about the norms, practices and policies embedded in political paradigms that shape the perception of the Internet and guide state behavior. Additionally, Manjikian argues that the creators of the technology adhered to the liberal narrative. While this seems to be partly the case, I would argue that the construction perspective represents a fourth origin story of the Internet. Because this thesis has a focus on the construction of the artifact called the Internet, the norms and visions of the designers have to be recognized. They established the first reading, the first narrative of this technology.

In sum, I will analyze the developmental path of four paradigms (cyber-realism, cyber-liberalism, cyber-utopianism, and the engineering perspective) and argue that the norm change in cyber-space towards more control can be understood as a paradigm change from cyber-utopianism to cyber-realism. This allows me to bridge the gap between the different theoretical camps outlined so far. Let me now briefly introduce the goals of the study.

1.3 Contributions of the Study

Besides addressing the aforementioned research gaps, the aim is to provide a minimally sufficient explanation of the dominance of the cyber-realist norm of control (Beach & Pedersen, 2012, p. 63). To do this, this thesis develops a norm-research approach that provides an alternative to the discursive dominance of securitization studies in explaining the Internet. Most constructivist studies remain in the discourse analysis tradition, focusing on speech acts alone. What is seldom analyzed is the material impact of those speech-acts, as Dunn-Cavelty criticizes (Dunn Cavelty, 2015). This thesis acknowledges the securitization of cyber-space thesis, which can be broadly defined as a:

> "[…] process whereby more issues, problems, behaviors, and phenomena get defined in "security" terms and subjected to the "protectionist reflex" (Beck 1998). If an issue is successfully securitized it is possible to legitimize extraordinary means to solve the perceived problem(s), with the corollary that the issue becomes an inappropriate topic for critical debate or resistance (Buzan et al. 1998)" (Bennett & Parsons, 2013).

However, this thesis goes beyond the discursive securitization because we need to look at the material and ideational causes and effects of cyber-phenomena. This thesis builds on securitization assumptions and norm-research but addresses some of their shortcomings.

First, it argues that we also need to study the material impact of securitization of cyberspace in terms of legal, normative and technological change. I argue that normative and technological change are related processes that do not just have discursive, but also material impacts. For example, we can witness in China that the desire to control the Internet leads to a reengineering of the Chinese part of the Internet to allow better censorship (Lindsay, Cheung, & Reveron, 2015). The desire for state-control leads to re-engineering practices that affect the global functioning of the Internet. State-produced malware like Stuxnet, so-called "cyber-weapons" (that would shut down a nation's Internet in case of war), as well as efforts to break or weaken encryption standards are real material effects of the norm of control (Moore & Rid, 2016; Schulze, 2017).

Internet control also has security implications. Intelligence officials for example argue that weakening Internet encryption in the name of national security makes countries more vulnerable in cyberspace. Internet control can harm cyber-security (Hayden, 2016a). The more states develop tools to break into each other's systems, the more insecure the entire Internet infrastructure gets, representing a classical security dilemma. This thesis will include frameworks from Science and Technology Studies (STS) to theorize normative and technological implications. Technological change also often is a norm-change, which is widely ignored by IR-constructivism (Herrera, 2003, p. 567). By including the literature on technological change, we can expand IR-constructivist frameworks which is important for the next argument.

Second, I argue that we should modify norm research to make it useful for Internet and technology studies. In a later chapter I offer a detailed critique of dominant theories of normative change so that I will keep this section rather short (see chap. 2.1.3 Critique of Diffusion Models). My general argument is that it is not enough to focus on singular ideational factors like ideas (Risse-Kappen, 1994; Checkel, 1997; Legro, 2000) or individual norms (Goertz & Diehl, 1992; Klotz, 1995; Katzenstein, Jepperson, & Wendt, 1996; Florini, 1996; Checkel, 1999) but that one must combine these under one umbrella. It makes sense to analyze the interaction of multiple norms and ideas. Thus, another aim of this thesis is to provide further explanations for norm change. I do this with the paradigm approach.

My third argument is that we should adopt a longitudinal perspective. Most securitization or Internet studies adopt a snap-shot nature. Due to pragmatic reasons, most

studies focus on single events or single discourses to analyze the impact of the securitization of the Internet. The empirical trend of the militarization of cyberspace (Deibert, 2003) has not been studied in detail and more importantly not over a long period of time. Only Thomas Rid's excellent history of cybernetics provides valuable longitudinal insights (Rid, 2016). However, theoretical explanations of why this process is happening and what causal consequences it might have are lacking. This is an advantage of norm-change literature, which often focuses on longer timeframes.

The few longitudinal studies that exist are histories of the Internet itself. These historic books often focus on technical aspects and do not include the political or the military dimension (Hafner & Lyon, 1998; Abbate, 2000). They also are rather descriptive and do not tend to theorize, maybe with the exception of Burman (Burman, 2003) and (Townes, 2012). In contrast, studies arguing from a more military perspective (Healey & Grindal, 2013; Kaplan, 2016) do not illuminate the civil or political dimension. I would argue that we need a holistic perspective to analyze a norm change in cyberspace.

A longitudinal study allows us to incorporate a constructivist norm framework for the study of the Internet and thus can act as an alternative or supplement explanation to securitization. This thesis argues that the phenomenon of militarization of the Internet can be conceptualized as a normative change (Finnemore & Sikkink, 1998) or a norm diffusion (Gilardi, 2013). Because the Internet developed within our life-time, it is a perfect case to analyze the genesis, diffusion and regression of norms (McKeown, 2009). A longitudinal or process-tracing study allow us not just to analyze the diffusion of one norm (cyber-realism), but also the regression of others (cyber-utopianism). The empirical trend of the militarization of cyberspace (Deibert, 2003) has not been studied in detail, and more importantly over a long periods of time. Only Thomas Rid's excellent history of cybernetics provides valuable longitudinal insights (Rid, 2016). But being more a historical book, theoretical explanations why this process is happening and what causal consequences it might have are lacking. This is peculiar because the emergence of the Internet (from the late 1960s to the mid 1980s) and the mainstream diffusion of it (since 1992) represents an interesting case. With the Internet, humankind has the unique opportunity to observe an emergent structure that, in the memory of most, is merely around 25 years old. We can observe the formation of meaning and norms that are produced by different actors who engage with the technology from the start or *ex-nihilo*. In that sense it represents a tabula rasa to study state behavior which had to be developed from sratch. It is a new technology which opened a completely new discourse and meaning space that was quite uncontested in its early days. As such it is a perfect situation to study the emergence

and diffusion of new norms that surround a technology. The question that remains however is, what type of case should we select to study the militarization and the norm change in cyberspace?

1.4 Case Selection: The United States

Normative change is typically studied with a methodology called *causal-process-tracing*, a within-case technique, which is explained in higher detail in a later chapter (see chap. 3. Methodology & Research Design). Process-tracing typically asks questions like how did an outcome (like a the norm of Internet control) come into being? As a case study technique, causal process tracing requires a case selection, an instance where the assumed normative change from utopian to cyber-realist norms happened.

Only one case is selected to trace the process of norm change. Ideally, the case must show a strong positive effect on the *outcome variable,* in my case is the change or variance in norms: cyber-utopian norms becoming replaced by cyber-realist norms. Since cyber-realist norms aim to establish control over the Internet it is necessary to select a case where this outcome is present. Internet control itself can be divided in different practices such as surveillance of data streams, active censorship of content, active repression and persecution of dissidents, active propaganda and information war and psychological operations (Deibert & Crete-Nishihata, 2012). Research from the Citizen Lab in Canada shows that historically, authoritarian regimes were the first to adopt Internet control and surveillance measures and that democratic countries began to follow this trend after 9/11 (Deibert et al., 2010). This thesis will put forward the argument that cyber-war capabilities are another instance of control.

If authoritarian regimes are front-runners of surveillance and Internet control, then it would make sense to pick for example China, Russia or theocratic regimes like Saudi Arabia or Iran (Deibert et al., 2010). Some of these states are also known to heavily invest in offensive cyber-war capabilities (Lindsay et al., 2015; Geers, 2015). But China and Russia present a difficulty which is a reduced *accessibility* of data, the main criterion for case selection in the process-tracing approach. It means that as much data as possible must be available and readable (Blatter & Haverland, 2012, p. 82). This concerns both language barriers and classification, since cyber-warfare activities are often carried out by intelligence agencies and shrouded in secrecy. Therefore, data-access is limited (Kaplan, 2016, p. chap. 15). To draw a comprehensive storyline and to analyze the sequences in detail, diverse forms of evidence must be considered in order to create a detailed picture of the process. Thus, China and Russia are not feasible for this study.

Besides the accessibility problem in China and Russia, there is a theoretical issue with authoritarian regimes in general. It could be argued that authoritarian regimes did not witness a norm *change* from liberal and often democratic cyber-utopian norms to cyber-realist ones. The transition from more liberal conceptions of cyberspace towards a more realist perspective did not happen to the same degree. There was not much of a norm change because in authoritarian regimes, Internet or media control in general already is the norm, not the exception. Therefore, it becomes interesting or puzzling if a liberal democracy adopts the very same measures. The case could be made that the ongoing militarization of the Internet is another indicator for the current "crisis of liberal democracy" or the "right-wing authoritarian turn" we currently can witness in states like Poland, Hungary, the USA and more.

A report from Reporters Without Borders concludes that the United States and United Kingdom are on their way to become authoritarian in cyberspace because of the extended Internet mass surveillance revealed by Edward Snowden:

> "The mass surveillance methods employed in these three countries [India, UK, USA], many of them exposed by NSA whistleblower Edward Snowden, are all the more intolerable because they will be used and indeed are already being used by authoritarian countries such as Iran, China, Turkmenistan, Saudi Arabia and Bahrain to justify their own violations of freedom of information" (Reporters without Borders, 2014, p. 4).

Other human rights organizations come to similar conclusions. According to Freedom House, between 2012 and 2015, the Internet freedom in the US declined from 12 to 19 points (0 being the best) on their index (Freedom House, 2016). They attribute this to increased Internet control practices. The assessment that the United States (US) is currently on a dangerous path, or on a transition, towards an Internet control regime installed in the name of terrorist prevention is not just shared by advocacy groups. As a reaction to the Snowden disclosures in 2013, the United Nations Special Rapporteur on the promotion and protection of human rights argued that:

> "Mass surveillance of digital content and communications data presents a serious challenge to an established norm of international law. In the view of the Special Rapporteur, the very existence of mass surveillance programmes constitutes a potentially disproportionate interference with the right to privacy. Shortly put, it is incompatible with existing concepts of privacy for States to collect all communications or metadata all the time indiscriminately" (United Nations General Assembly, 2014b, p. 7).

Here, the assumed norm change becomes visible: Internet control practices such as mass surveillance of data streams contests core norms of international law. In his report, the UN rapporteur explicitly names the United States and the United Kingdom as the main sources for concern because the majority of Internet traffic is routed through these countries. This means that traffic can be potentially intercepted and/or altered by intelligence agencies in these countries (United Nations General Assembly, 2014b, p. 6). The report even calls some of these surveillance and cyber-war initiatives attempts to take "secret control (or "ownership") over servers in key locations on the "backbone" of the Internet (United Nations General Assembly, 2014b, p. 8). The report then advises that these states review their Internet control practices to make them compatible with international law.

These statements indicate that there is indeed a norm-change going on with the emergence of Internet control norms in the United Kingdom and the United States. More so, this change represents a norm-regression of liberal norms such as privacy. Therefore, the USA is going to be selected the *case of interest* for analyzing normative change in cyberspace. Why chose the US instead of the UK?

The primary reason for the US is a practical one: the Internet was invented in the United States and it is the country which saw the first widespread diffusion of this technology before any other country (see diffusion statistics in the appendix, Quantifying the Internet and the Digital Revolution). It was also the country which adopted first Internet policies. This makes it a frontrunner and an example for many other countries and implies that Internet norms potentially developed there first and then diffused to other countries. The US was also the first country to theorize about cyber-war. Furthermore, American academia played a major role in creating this technology. There is a vast body of literature on the origins of the Internet which means there is a lot of data to be generated. Most of the initial inventors of the technology (who are still alive), are American and live in the United States which makes it possible to conduct first hand interviews to determine the goal oriented construction dimension. To sum up, the process of normative change regarding cyberspace is analyzed within the case of the United States.

1.5 Structure and Logic of the Argument

Now, let me explain the structural logic of the thesis. Explaining outcome process tracing studies require a broad array of theoretical elements that explain how an outcome was created (see chap. 3. Methodology & Research Design). "Theories are used here in a much more pragmatic fashion that is, as heuristic instruments that have analytical utility in

providing the best possible explanation of a given phenomenon" (Beach & Pedersen, 2012, p. 13).

I start by synthesizing the dominant explanations and approaches for explaining *normative change* (see chap. 2. Explaining Normative Change). The purpose is not to identify variables, but to have a broad, and eclectic framework to explain different parts in the causal process at different points in time. This analysis will show that the focus of traditional norm-research is to narrow (see chap. 2.1 Norms and Theories of Normative Change), and that we need further theories to grasp the complexity of norm-change over longer periods of time.

That is why I will adopt the wider perspective of policy paradigms which includes norms, ideas but also frames and policies. I argue that this expanded framework can account for more things in the causal mechanism. Particularly, I will fuse the concept of advocacy coalitions and that of policy-paradigms (see chap. 2.2 Paradigms and Norm-Change). This will be combined with recent development in norm-research, i.e. a critical or discursive perspective that argues that norms are not singular entities, but represent some kind of semantic network or norm-clusters (see chap. 2.2.3 Degrees of Change).

This expanded notion of norms and paradigms allows to bridge the gap between norms and technology. I fuse norm-research and Science and Technology Studies together to explain the technological and thus structural aspects of the study, i.e. social construction of technical artifacts such as the Internet, the normative implications technology can have and additional mechanisms of diffusion. There is a lot of conceptual overlap between STS and norm-research and to bridge the gap between the two fields is an important aim of the study. Particularly, the element of timing is important: different stages of technological diffusion have different implications for norm diffusion with technology.

This timing aspect is particularly important for the methodology of process-tracing, which will be introduced afterwards (see chap. 3. Methodology & Research Design). Here, I will outline my understanding of causality as well as the overall research design of the study.

The empirical case study in chapter 4 has a distinct temporal and methodological logic to accommodate the requirements of causal process tracing in a longitudinal fashion. The empirical part is structured according to the unfolding of the process and less "according to variables and theories" (Blatter & Haverland, 2012, p. 142) as in other case study types. Generally, the study adopts a historical perspective from the past to the present. Since I am dealing with the evolution of four different paradigms (*engineering paradigm*, *cyber-realism*, *cyber-utopianism/liberalism*), the challenge was how to structure

the logic of the thesis. The focus on the four sub processes of paradigm and norm evolution requires to analyze the same timeframe, a period like the construction of technology from four different angles. Structurally, there would be two ways of doing this.

One way would have been to discuss the combined, linear unfolding of each paradigm in a distinct timeframe (or element of the causal chain). Main chapters would represent a decade or so and sub-chapters the four individual paradigms. Since I also want to focus on different aspects of each paradigm (i.e. paradigmatic components such as ideas, norms, problem definitions and blind spots, as well as on distinct outcomes of each, such as policies, or technical artifacts), this *linear-sequence structure* would have become too complicated and unfriendly to read. Another downside was that the thesis operates with different actors that matter at different points in time and that accommodate different central or peripheral positions in the policy process. For the causal mechanism to make sense, a shift of the units of analysis is required (as well as the analysis of different types of data), which ultimately would have become very confusing with a linear, combined structure.

Instead, I chose to structure the thesis in a *parallel-sequence*: each paradigm is analyzed separately from the other, from past to present. This means, the same decade is covered from the perspective of the different paradigms. This temporal logic is the basis of the four major subsections (4.1 - 4.4). Each subsection discusses the evolution of one Internet paradigm in a longitudinal timeline. This means that each paradigm has an individual starting point, which will be explained at the beginning of each chapter.

Chapter 4.1 discusses the social construction of the technical artifact Internet and the norms and motivations of the designers (what I call the *engineering paradigm)* from the late 1960s until the mass market diffusion of the World Wide Web in 1993. Since all other paradigms react to the Internet, this is a logical starting point. Chapter 4.2. traces the evolution of ideas from the early users of the Internet and the formation of the *cyber-utopian paradigm* from the 1960s until the present day, with a particular focus on the late 1980s and early 1990s (where much of the Internet usage modalities or norms evolved). The purpose of the chapter is to trace the evolution of the first cyber-utopian Internet norms, the idea that the state ought not to have control over cyberspace. Cyber-utopianism was the first widely shared meaning and frame of reference for understanding the Internet and thus this chapter represents the first part of the norm change in the thesis's title.

The "hands-off" norm got politically institutionalized in the early 1990s. This will be discussed in chapter 4.3, which shifts the perspective from the Internet's users to policy-makers and analyzes how the Clinton administration reacted to the Internet. The focus is

more on political ideas and policy-making, establishing the "*hands-off norm" of cyber-liberalism*, a distinct political-technological perspective that argues for the primacy of the private and civil actors in controlling the Internet. This represents the logical starting point for a norm-change from utopian to realist norms, which will be introduced in the next chapter.

Chapter 4.4. shifts the analytical focus to military and intelligence advocacy groups and their perception of digital technologies or what is called *cyber-realism*. This chapter represents the center-piece of the argument and thus has the highest level of detail since it includes the evolution of the concept of cyber-war, with its norm of Internet control. It focuses on ideas (military doctrines), policies, as well as the construction of counter-artifacts to the Internet, i.e. the creation of offensive cyber-war capabilities and mass surveillance technology. The aim is to trace the origin of the norm of controlling the Internet because of national security concerns. The outcome of this process is the cyber-realist norm that the state (the military and intelligence community) claims the right to monitor and control all information traversing and the very functioning of the global Internet, even beyond their national jurisdiction. This *"norm of control"*, will be analyzed and criticized in high-detail.

The final empirical chapter of this thesis (see chap. 4.5 From Cyber-Utopia to Cyber-War: The Obama Presidency (2008-2013)) does not talk about one paradigm, but two. It is the culmination of the militarization and norm-change thesis, where cyber-realism replaces utopianism. Therefore, the interaction of these paradigms within the Obama administration will be discussed.

This parallel-sequence structure creates a challenge and a potential downside the reader must be aware of. The parallel-sequencing makes the cross-paradigm interactions harder to follow. Initially, the plan of the study was to conduct a discourse analysis at different junctures, indicating the discursive struggle and framing of the paradigms. Due to place constraints, this was left out and the evolution and interaction of paradigms is discussed in a narrative fashion. I follow the example of Nina Tannenwald and Jeffrey Legro, who have opted for the same approach in their longitudinal studies of tracing the nuclear taboo (Tannenwald, 1999) or change of dominant ideas and epistemes in US foreign policy (Legro, 2000). Structurally and logically, this thesis was highly inspired by their work.

Another issue with parallel-sequencing is that sometimes chapters include a concept that is introduced in higher detail in the following chapter, because it belongs to another paradigm. This creates a hermeneutic dilemma: to understand a concept during linear-

reading at a point in time t1, one requires the in-depth knowledge that is provided in the chapter which is read later at t2. To reconcile this hermeneutic dilemma, I used two tools: First, when a concept occurs that is discussed in high detail later, I provide a limited definition or description in a footnote that makes sense for the moment of reading. Second, I used a core-technique developed by Internet-engineers who struggled with the same problem of physical text, the Hyperlink. When a new concept is introduced, a link to the chapter where it is discussed in high detail is provided (like this, see chap. 4.1.4 Artifact: The World Wide Web (1989-present)). These links will be clickable in the digital copy of the thesis.

After having introduced about what this thesis will talk about, it is now worth mentioning what cannot be discussed due time and space constraints. For example, several scholars note that attempts to regulate and control the Internet also come from the economic sector. From a certain economic perspective, it makes sense to impose restrictions on the Internet, and thus controlling its content, for example in terms of copyright infringement and file-sharing (Zuckerman, 2010b, p. 79). These initiatives are driven by Internet intermediaries and a vast array of companies. It would be worthwhile to analyze how these companies perceive the Internet and the norm change, but since there are so many different business models, perspectives and stakeholders, it would further complicate the thesis.

Other economic aspects are Big Data, social media and the commodification of data generated by Internet users when using online-services such as Google or Facebook. There is a synergy between the business-model of collecting user-data and selling advertisement on a large scale and the surveillance interest of states. Both surveillance and the commodification of data are driven by the same idea to generate as much information about a user as possible, since the very same data could be useful for profiling and law-enforcement (Morozov, 2011, pp. 147-152). Deibert argues "'Big Brother' and 'Big Data' share so many of the same needs, the political economy of cybersecurity must be singled out as a major driver of resurgent authoritarianism in cyberspace" (Deibert, 2015, p. 74). This powerful dynamic and interplay of private company surveillance and the intelligence community (IC) is an interesting, yet complex and relatively new field of study. It could be argued that this aspect could either represent an entirely new paradigm, or a fusion of the military-inspired cyber-realism and cyber-liberalism with a neo-liberal flavor (Mayer-Schönberger & Cukier, 2014). However, since this is primarily a work of political science and I have no background in economics and digital humanities, I will exclude this topic from the thesis and refer to other excellent studies (Lyon, 2014). Other important

arguments are the space and time constraints of this thesis. Instead of introducing this aspect only superficially, I will exclude it entirely.

Another issue that is left out is the question of digital activism and hacktivism that emerged out of cyber-utopian thinking in the mid 2000s, mostly because it is such a complex and diverse field of actors. Norm entrepreneurs and advocates such as Wikileaks, arguing for total transparency and the free flow of information or hacker groups like Anonymous and others are not part of the thesis. It could be argued that although Wikileaks and hacktivism saw a peak of public recognition between 2007 and 2011, these groups are relatively marginalized nowadays. Additionally, the topic is relatively well-studied (Jordan & Taylor, 2004; Nissenbaum, 2004; Benkler, 2011; Assange et al., 2013; Wong & Brown, 2013) which means there is no immediate need to replicate these findings.

Now let us turn to theories explaining normative change in cyberspace.

2. Explaining Normative Change

One of the core assumptions of this thesis is that ideational factors such as ideas, beliefs and norms have an impact on policy and technology. Ideas shape our perception of the world, which in turn influences how we act. What we think about technology is influenced by our ideas and when ideas change, so do policies. In turn, ideas shape technical artifacts such as the Internet. If we want to analyze the shift from more liberal conceptions of the Internet towards more authoritative control and a military logic, we need to examine the role which ideas play in this transformation and how these ideas shape standards of behavior. This chapter conceptualizes the interplay of sets of ideas and norms, called political paradigms and technology. The aim of this chapter is to evaluate the relationship between norms, ideas and policy change in International Relations. This is the first step, followed by a theoretical discussion about the conditions of normative change and which role agents play therein.

Ideas, norms and politics are intertwined, they drive political change. Think for example how the idea of Keynesian economic practice became replaced by monetarist and more neo-liberal stances of capitalism in 1980's Britain (Hall, 1993) or how Mikhail Gorbachev's "new thinking" led to the transformation of the Soviet Union, leading to its collapse in 1991 (Risse-Kappen, 1994). It was during the 1990s that ideas, norms and identity became key variables in explaining policy change, promoting the so-called "constructivist turn" in the discipline of International Relations. This led to an intensive "third debate" (Lapid, 1989) within the discipline of IR and resulted in a theoretical opening, which allowed sociological approaches and *reflectivist thinking* to gain traction in IR. Reflectivist approaches argue that knowledgeable practices or ideational factors constitute subjects and objects alike (Goldstein & Keohane, 1993a, p. 3). Max Weber already argued at the beginning of the 20th century that if one wants to understand social action, one must analyze not just the objective conditions, but the subjective interpretations of those conditions by actors. Weber argued that an action can only be social to the extent that meaning is attached to mere behavior (Weber, 1968, p. 12). Meanings, in turn, arise with human interaction and are used to make sense of the "ongoing streams of happenings" (Scott, 2008, p. 57). Even though there are several branches of reflectivist thinking (from moderate pragmatism to post-structuralism and radical constructivism) the underlying core assumption of these approaches is that the social reality is not objectively given or "out there", but rather only conceivable through our interpretation and language (Adler, 2013, p. 113). In this view, the process of knowledge construction is based on collective meanings that are, via discourse, attached to material objects such as the Internet. Reflexivity in this

regard means that "knowledge *of* the world, when imposed on material reality, becomes knowledge *for* the world – the power to change the world in accordance with collective understandings" (Adler, 2013, p. 113). The focus of analysis shifts from material factors that prescribe preferences towards ideational factors and the process of meaning creation that guides action. Therefore, ideational factors like ideas, world views (Goldstein & Keohane, 1993b), paradigms (Hall, 1993), norms (Katzenstein et al., 1996), identity (Wendt, 1994), habits (Hopf, 2010) and practice (Adler & Pouliot, 2011) become important factors for social action.

What is still missing is a systematic reflection of all the ideational factors and their connections. Scholars tend to focus on singular ideational factors like ideas (Risse-Kappen, 1994; Checkel, 1997; Legro, 2000) or individual norms (Goertz & Diehl, 1992; Klotz, 1995; Katzenstein et al., 1996; Florini, 1996; Checkel, 1999), but fail to analyze the connection between them. The important gap in research is to address the fact that norms and ideas in fact do not float freely (Risse-Kappen, 1994, p. 197) but are embedded in a normative-ideational context. Norms do not exist in isolation. We therefore need to ask, what is the connection between ideas and norms? How are they interrelated? How do sets of ideas and norms correspond in bigger frameworks (such as world views, paradigms or ideology)?

2.1 Norms and Theories of Normative Change

How can we explain that changes in state behavior lead to totally oppositional policies and positions towards an issue over time? How can we analyze policies that become practices and ultimately unquestioned standards of behavior? To this end, constructivist scholars developed several frameworks to analyze what they call normative change – the replacement or evolution of one set of behavioral guidelines and practices with another. In this logic, policies change because their underlying normative guidelines and ideas change. Before we come to that, we need to define norms.

Within constructivism, norms are generally defined as a "standard of appropriate behavior for an actor with a given identity" (Finnemore & Sikkink, 1998, p. 891). Norms are instructional units that influence behavior that tell actors, either explicitly or implicitly, what a culturally appropriate action in any given situation or for a certain type of identity is (Florini, 1996, p. 363f.). They both constitute actors (as a civil-power for example) and regulate their behavior. According to Searle, regulative rules constrain "antecedently existing activities" and constitutive rules "create the very possibilities of certain activities" (Searle, 1995, p. 27). "Constitutive rules define the set of practices that make up any

particular consciously organized social activity – that is to say, they specify what counts as that activity" (Ruggie, 1998, p. 22). Constitutive rules operate according to the principle: "X counts as Y in context C (an American Dollar bill counts as legal currency in the US)" (Scott, 2008, p. 28). The concept of civil powers helps to illustrate this idea (Maull, 2000; Berger, 1996). If a state considers its identity to be a civil power, it "agrees" to behave in a manner compatible with this identity (i.e. not waging war, relying on civil means of conflict-resolution, strong notions of multilateralism etc.). Norms attached to the identity of civil powers are for example the taboo of waging offensive war out of self-interest or possessing certain types of weaponry (like chemical or nuclear weapons). The norms connected to civil power restrain state behavior by defining what is appropriate for that civil-power identity and what is not. Identity-based norms are obeyed because they are seen as legitimate and not necessarily because they are enforced by a community of actors (although this is important as well)

"Unlike rationality, which is about the efficient means for gaining a predeter-mined goal, norms are concerned with the desirability of the means and goals themselves" (Goertz & Diehl, 1992, p. 636). In other words, norms influence the goal and preference construction of actors as well as the means to achieve them (Florini, 1996, p. 366). They delimit the *what*, but also the *how* – the range of tools and actions that can be done and should or should not be done. Action that is likely to produce suffering is then to be avoided. It would be too short-sighted to focus on rational-interests alone. Even national interest or hard national security concepts can be understood with a constructivist framework (Weldes, 1996).

All these elements require a *social element* like social pressure, sanctions and stigma. Norms are relevant only in normative systems of practice. Norms must be adhered to in repeated practice, otherwise they would just be normative guidelines without any consequences (like empty words). Repeated, reciprocal interaction creates reciprocal expectations and constitute what Emile Durkheim called *social facts* that exist exogenously from any actor and reside within a social group or can become embedded into institutions. For example, if a civil power identity coherently acts according to a set of prescribed norms (like multilateralism, civil conflict resolution), this creates expectations over time within the social group that future behavior of that actor will look similar to current behavior. Every action by an actor is evaluated by the rest of the social community whether it adheres to the abstract list of appropriate action (or the normative framework of the community). The result of this reciprocal process is that only a specific range of action counts as norm-following for a given actor and a whole range of other actions become

inappropriate (for example engaging in offensive warfare). Over time, groups will develop some type of catalogue of actions that are deemed inappropriate. Only then norms become "organizing principles or standardized procedures that resonate across many states and global actors, having gained support in multiple forums" (Wiener, 2009, p. 183f.). This process can be called *normalization*. Not just norm-following defines the right course of appropriate action, but also norm-breaking. Norm-breaking behavior often creates social sanctions by other actors, which might change behavior in the first place (Goertz & Diehl, 1992, p. 638). Over time, this repeated interplay between action, expectation, actual behavior and sanctions creates standards of behavior and can in fact lead to the institutionalization of social rules, such as in international law.

Norms are only valid for an actor with a specified identity. They not only determine how to act, but also *who* should act. Most international norms are state-centric whereas in micro-contexts, norms can be directed at individuals as well. For example, a customer in a restaurant (an identity in a given context) is expected by the social context to behave in a certain way (order food, eat quietly). Here, it becomes obvious that different disciplines of the social sciences have different perspectives on norms. Whereas ethnography and sociology focus mostly on micro-level norms, IR focuses often on macro-level norms.

2.1.1 Norm Diffusion and Norm Entrepreneurs

Now that we have defined norms, it is necessary to analyze how they change. The mainstream focus of constructivist theories dealing with normative change is on norm diffusion (Klotz, 1995; Finnemore & Sikkink, 1998; Checkel, 1999; Farrell, 2001; Acharya, 2004; Wiener, 2007; Kelley, 2008; Ganguly, 2010; Hyde, 2011; Gilardi, 2013). Norm diffusion is defined as the transmission of one norm from one context into another. The transition of global environmental standards such as a prohibition of whaling, onto local policies (Epstein, 2008) would be an example. This diffusion can happen via different mechanisms like coercion, dynamics of state-competition, social learning, emulation and strategic implementation by norm entrepreneurs like persuasion (Payne, 2001) and framing (Snow & Benford, 1992). The aim of diffusion research is to show the link or the mechanism that indicates that one norm was influenced by another one. Since I am interested in normative change, diffusion research offers many useful insights for the study of norms in general.

One of the most influential frameworks for studying norms is by Finnemore and Sikkink, who analyzed the evolution of norms and constructed a *norm life-cycle* consisting of three stages: first *norm emergence,* where new rules of appropriate behavior are put on

the radar by norm entrepreneurs with the help of transnational advocacy networks and other organizational platforms that act as norm entrepreneurs (Finnemore & Sikkink, 1998). *Norm entrepreneurs* are public promoters of norms who engage in advocacy. During the second stage, norm entrepreneurs try to socialize other actors to follow the norms until a tipping point, a critical mass of norm-followers is reached. This tipping point triggers a self-reinforcing feedback loop, a so-called *norm-cascade,* through which the norm automatically diffuses globally. During this second stage, a norm is adopted by more and more actors and thereby creates peer pressure for others to follow. The norm diffusion process resembles an "S-curve" of technological development where the rate of adoption increases towards a ceiling (many countries adopt the norm), and then flattens (Gilardi, 2013, p. 453). If enough actors adopt a norm, the third stage, *internalization,* kicks in, where a new norm becomes normalized and taken for granted in a target society (or globally, since the model works on both levels). Whereas in the first two stages, norms leave an extensive discursive trail, there is a systematic lack of discourse in the third stage because the norm is not contested anymore (Wiener, 2007). Internalized norms are taken for granted standards of behavior and as such, part of common sense. There is extensive research focusing on the tipping point, where a norm is about to become globally accepted. Issues of norm emergence and internalization are discussed less often, which is no accident. During the tipping point, it can be assumed that the public discourse surrounding a norm is at its peak, which means it leaves a highly visible discursive trail (Finnemore & Sikkink, 1998, p. 892). The situation is more difficult during the emergence stage, and even more so, during the internalization stage, where a norm is taken for granted and thus not talked about anymore. This and other elements caused a lively debate within IR constructivism. The next chapters introduce some critique on the norm-diffusion model that I will address in this thesis.

2.1.2 Critique of Deontological Norms

Although norm research has many advantages, there are some shortcomings that need to be discussed. In their evaluation of the status quo of the norm literature in 2001, Finnemore and Sikkink write that there is a bias towards "nice or progressive norms" in IR (Finnemore & Sikkink, 2001, p. 403). Within constructivism most studies focus on progressive norms such as protecting the environment, promoting democracy, human rights, the Responsibility to Protect, weapon taboos and so forth. What is interesting is that these norms clearly have a moral dimension. These norms are often centered in the international arena while neglecting domestic spaces. They often are cosmopolitan and

have a Western-liberal bias (McKeown, 2009, p. 9). But there is more to be criticized. My argument is that this bias stems from how norms are conceptualized within IR, which predominantly focuses on the dimension of oughtness, while neglecting the role of repeated practice and the process of internalization.

The dominant way to analyze norms in IR is to focus on their *normative* or moral components. "Norms reflect patterned behavior of a particular kind: a prescribed pattern of behavior which gives rise to normative expectations as to what *ought* to be done" (Hurrell & McDonald, 2013, p. 69). The oughtness of norms indicates "*how* an actor should behave", therefore making a statement about legitimate behavioral claims (Florini, 1996, p. 364). It defines the *right course of action* from a moral position: "When many people engage in the same behavior, that behavior comes to be associated with a sense of oughtness" (Horne, 2001, p. 6). Finnemore and Sikkink call these *prescriptive norms*, because they prescribe behavior and the quality of oughtness differentiates them from other types of rules (Finnemore & Sikkink, 1998, p. 891). Key here is the normative or deontological dimension of social rules which must be followed or else sanctions will be the consequence (Goertz & Diehl, 1992, p. 638f). Deontology is the study of moral obligation. In that sense norms, are understood as "good" or moral practice. The underlying premise of diffusion research is that the rightness and wrongness of social action can be determined by actors, and that they can be socialized into norm-followers. In their influential article, Finnemore and Sikkink clearly recognize the deontological focus by quoting James Fearon:

> "Good people do (or do not do) X in situations A, B, C ... " [Because] "we typically do not consider a rule of conduct to be a social norm unless a shared moral assessment is attached to its observance or non-observance" (Finnemore & Sikkink, 1998, p. 892).

Originating from moral philosophy, deontological ethics deals with the evaluation of behavior based on the *intrinsic motivation* or sense of duty and obligation of actors. Whether an action is morally desirable or appropriate depends not on the consequences (as in Utilitarianism), but on the intrinsic character of an action (which can be determined by the Kantian categorical imperative or the golden rule). The right thing to do must be internalized by the actors themselves. It can be argued that norm-research and constructivism are inspired by the deontological heritage of the enlightenment period, which explains the bias.

In this view, global norm diffusion is a development into a better, more civilized world and resembles the idea of enlightenment (and of IR idealism). Kant for example

argues that humans must be educated (socialized) in order to be able to recognize what morally good behavior entails (acting according to the categorical imperative). In his book "Perpetual Peace" (1976 [1795]) he argues that if all humans were educated enough, they would follow the same normative principles, creating a reasonable and enlightened cosmopolitan society, which would ultimately result in peace. Deontological ethics as well as norm research tend to see normative principles as *universal*. Because all humans are reasonable beings, they all can discover the same universal truths and act accordingly. The process of norm diffusion similarly assumes a *teleological* norm adaptation (McKeown, 2009, p. 7) on a cosmopolitan scale (a critical mass of state actors internalized the norm and follow their normative imperatives). There is no room for cultural variation and local norms (Mackie, 1977) and the local dynamics and domestic processes of norms are black-boxed (McKeown, 2009, p. 8).

Critical norm-researchers now argue that this focus on progressivism covers a darker and hidden aspect of norms, which is their underlying power dimension (Engelkamp, Glaab, & Renner, 2012). Local norms are suppressed and delegitimized by global and cosmopolitan norms, which are framed as universal. By trying to educate or socialize local actors to follow international norms, power is exercised. Interestingly, the artificial distinction between norm-givers (or entrepreneurs) and norm-takers (those who do not have internalized the norm) resembles the idea of a classroom where the teacher (norm entrepreneur) educates the children, which are seen as a tabula rasa (Bucher, 2014). In world politics, cosmopolitan norms are constantly normalized and universalized, which reproduces their hegemonic status, as critical theories, postcolonial and feminist studies have uncovered (Deitelhoff & Zimmermann, 2013; Engelkamp, Glaab, & Renner, 2013; Krook & True, 2012; Epstein, 2014; Epstein, 2008). At the same time, local norms are overruled and excluded by international norms, which implies a hidden, undertheorized power component. Therefore, the task is to uncover power dynamics of norms and to shift the focus beyond the deontological perspective. This includes a critique of classical norm-diffusion models, which will be explained in the next chapter.

2.1.3 Critique of Diffusion Models

Generally, Finnemore's and Sikkink's framework outlines the most relevant elements of normative change (Finnemore & Sikkink, 1998). But in recent years, the framework has been criticized. The following paragraphs outline theoretical weaknesses of the concept. The purpose is to build upon this critique and to develop a more detailed research program.

First, the deontological aspect of the norm concept must be questioned. Krook and True argue that most constructivist research falsely assumes that a norm's content, its essence, is *static* (Krook & True, 2012, p. 104). Often, diffusion studies assume that static norms become transplanted in a different context without alteration. The view that norm-givers and norm-takers have the same perspective (meaning) of the norm has been questioned by Archarya (Acharya, 2004). The same norm might mean different things for global and local actors because these are observed from different contexts or viewing angles. Krook and True point to the constant reevaluation and discourse about norms and their legitimacy (Krook & True, 2012, p. 104). Their normative content is not fixed but in constant flux, as post-structuralist scholars would argue. Local contexts matter and global norms become transformed through local adaption. This is one of the core insights of IR constructivism which is forgotten by mainstream constructivism – all perception is influenced by the position from which it happens. Therefore, local contexts matter because they shape the to-be-adapted norm.

Second, norm research in general tends to focus on norms in singular (Bucher, 2014). Most papers are about one norm, such as sovereignty (Barkin, 1998), *the* nuclear weapon taboo (Tannenwald, 1999), *the* anti-whaling norm (Epstein, 2008), or the recent debate about whether the responsibility to protect actually is *a* norm (Fröhlich, 2011). However, many studies have problems identifying what *the* norm actually is, which is due to their constant contestation (Wiener, 2007). This indicates that there is not one internal norm-essence that is accepted by all actors. When looking closer, it often becomes apparent that there are different sub-norms at work, or what Bucher calls *norm-networks* – meaning normative ideas and practices that are related to each other (Bucher, 2014). Different normative ideas are in contrast to each other and struggle to become dominant. Focusing on norm-networks or clusters, of norms that relate to or even reinforce one another is a fruitful endeavor that will be used in this thesis.

The third shortcoming in IR scholarship revolves around the question where norms come from in the first place (Krook & True, 2012, p. 108). Finnemore & Sikkink's highly influential work on norm dynamics merely touches the issue by pointing to norm-entrepreneurs (Finnemore & Sikkink, 1998). By pointing to norm-entrepreneurs, the question is simply shifted because then we must ask where the norm-entrepreneurs get their norms from. Most studies focus on the process of diffusion through norm cascades and internalization (for an overview of diffusion studies see Gilardi 2013). The origin of norms, often on the domestic level, is under-theorized. Therefore, it is important to conceptualize these early factors that influence the development of norms and the first

stage of norm emergence. My argument is that in order to understand the development of norm-networks, we must take a close look at the core ideas that these norm entrepreneurs hold. Research from other disciplines of political science can be helpful here, for example the work around ideas (Jachtenfuchs, 1995), policy paradigms (Hall, 1993) or advocacy coalitions (Sabatier, 2007). Ideas and norms are clearly related. Not just single ideas are relevant but coherent *sets of interrelated ideas* which provide the basis for any social action. This is also in line with post-structuralist theorizing about networks of meaning. The next main section will do this theorizing (see chap. 2.2 Paradigms and Norm-Change). Fourth, Finnemore and Sikkink (2001) are aware of this and argue that slavery or the unequal status of women have been the unquestioned norm in many societies of the past. Xenophobia, extreme nationalism, slavery and misogyny were once normal in certain societies and are examples of normative systems in the sense that they regulate behavior of agents by referring to social standards (Finnemore & Sikkink, 2001, p. 404). Within the context of slavery, it is not appropriate for the slave-identity to rise up against their masters (it is not expected). These norms often exercise power over the behavior of actors but they have no deontological or normative dimension from our point of perception. But within these cultures they were valid. In deontological ethics, slavery as well as mysogyny are definitely morally bad. In some normative systems, certain subject categories are systematically discriminated while other subjects benefit from this discrimination and try to stabilize the status quo. This hidden power dimension of these normative standards is forgotten when focusing only on "nice norms". Therefore, it is important to shed light on this darker dimension of norms. Post-modernism can help us here.

Fifth, Finnemore and Sikkink's diffusion concept is strongly actor-centered, at least during the first stages of diffusion. While this focus is plausible during active contestation phases and the struggle for normative legitimacy, during norm emergence and internalization we must consider structural aspects such as the normative context in which norms become embedded or from which they originate. Norms are social facts and they can become embedded in institutions and other cultural artifacts. This thesis will argue that technology also is a kind of actor, an *actant* as Latour would call it, that can promote norms (Latour, 2005b). In fact, the diffusion of a technology like the Internet also can act as a medium for norm-diffusion. My argument is that norms can be transported via technology, which is a promising venue for norm-research that has been overlooked. At the same time, a technological perspective might be fruitful to explain many other shortcomings discussed so far: the early emergence process of norms with the construction

of a technical artifact, the diffusion of this very artifact and its possible decay as well as the concept of paradigms and the hidden power dynamic of norms.

The sixth and final issue is the measurement of the tipping-point initiating the norm-cascade, which is mostly used as a heuristic device but seldom measured. I would argue that science and technology studies, where the original s-curve model originated from, can shed a light on tipping-point dynamics which are embedded in concepts such as path-dependency and technological diffusion.

After listing all those shortcomings one might get the idea that the norm diffusion model is to be dismissed because it is faulty. I would not go that far. The general logic of the diffusion model is still valid and it offers all conceptual elements that are worthy considering, although some might be expanded. Finnemore and Sikkink's diffusion model is the basis for the framework I will develop in the next chapter.

2.2 Paradigms and Norm-Change

One of the important premises of this work is that human agents act according to ideational frameworks, which serve as a roadmap to action. Ideas guide policy decisions, but they also guide designs of technical systems such as the Internet. One of the most influential concepts for analyzing the change of ideas, practices, norms and even technology is Thomas Kuhn's concept of paradigm change (Kuhn, 1970). This concept is especially insightful because it combines several necessary conditions for (normative) change and operates on a meso-level (Legro, 2000) between single ideas and broad world-views (Goldstein & Keohane, 1993a), which makes it easier to study than ideologies for example.

Paradigms are "the entire constellation of beliefs, values, techniques and so on shared by the members of a given community" (Kuhn, 1970, p. 175). They define what the world is for actors and are "a way of seeing the world" (Kuhn, 1970, p. 175) by prescribing ontological and epistemological assumptions like "what sorts of entities the universe does contain [or not]." (Kuhn, 1970, p. 7). This corresponds with the constructivist notion that the world is not directly accessible but mediated by our knowledge and the point of observation (Adler, 2013, p. 115). Thus, the same thing can be interpreted completely differently by competing paradigms. They also define the foci for research. Science is a practice of problem-solving and paradigms define legitimate *problems*, *methods* (practices) including techniques and technologies for doing so. With this practice, paradigms automatically create *blind spots* – they ignore or do not recognize things that are not in alignment with the assumptions of the paradigm. By adding the concept of *cognitive dissonance*, paradigms lead to the effect that paradigm-contradicting evidence is ignored.

Paradigms clearly include norms, for example standards of appropriate behavior in terms of problem-solving (for example using the scientific method and not biblical hermeneutics). Rules derive from paradigms, as Kuhn says (Kuhn, 1970, p. 43) and these often are taken for granted (called normal science). As such, paradigms not just have an ideational component, but also a social one – actors who follow a paradigm have a commitment to rules and standards of scientific practice (Kuhn, 1970, p. 11). They are constitutive for science, because:

> "Paradigms provide scientists not only with a map but also with some of the directions essential for map-making. In learning a paradigm the scientist acquires theory, methods, and standards together, usually in an extricable mixture. Therefore, when paradigms change, there are usually shifts in the criteria determining the legitimacy both of problems and proposed solutions" (Kuhn, 1970, p. 109).

Generations of scientists are educated and socialized with a distinct paradigm. Paradigms are carried by textbooks, journal articles and also by material culture with the "the construction of elaborate equipment, the development of an esoteric vocabulary and skills" (Kuhn, 1970, p. 164) and costly research institutes. This creates a professionalization among practitioners. Paradigms are stronger if they are shared by scientific authorities, which often are not questioned by younger scientists. All these factors make paradigms, once established, difficult to change. More so, the paradigm is given to the next generation of paradigm holders through institutionalized educational channels, such as university study programs or career tracks.

Kuhn developed the paradigm concept with science in mind, which definitely is a unique cultural context. But the concept has also been adopted for other disciplines. The difference to the political sphere is that in the latter the notion of power is intertwined with the change of paradigms and that formal institutions of the polity (i.e. like elections in the political system) have an influence on the evolution of paradigm. In contrast to scientific paradigms, social ones need not be based on any criteria of truth and normally there are no mechanisms in place to check truthfulness. The consequence of this missing safeguard is that the *process of paradigm change* works differently (see chap. 2.2.4 Explaining Change). In science, old paradigms become abandoned because their problem-solving capability diminishes and they become incommensurable with newer paradigms. In the social world, paradigms can coexist with each other, even though they might be incommensurable toward each other (Meyers, 1990). Because of the missing safeguard,

there is no way of saying which paradigm is "better" or more truthful. Instead, social dynamics determine the stability and legitimacy of paradigms.

Peter Hall (Hall, 1993) was one of the first who translated Kuhn's argument into political science in order to grasp complex sets of political ideas and norms. Hall argues that policies are the product of a system of descriptive ideas and normative standards. He calls these systems *policy paradigms,* which specify "not only the goals and instruments of policies, but also the very nature of problems that are meant to be addressed" (Hall, 1993, p. 279). Thus, policy paradigms are an interrelated set or cluster of ideas, standards of appropriate behavior and policies. Policy paradigms determine social behavior in the field of politics by defining standards of appropriate problem-solving, which is a clear connection to norm research. The "definition of a problem is always a political act" (Mintrom & Norman, 2009, p. 652) because it defines how actors relate to an issue. It influences if and how individuals pay attention to issues and obviously affects solution strategies. It makes a difference if something is defined as a "banking crisis" or "debt crisis" because it shifts responsibilities. Hall conceptualizes three elements of problem solving: first, the *overarching goals* that guide policy in a field, second the *techniques or policy instruments* used to achieve the goals and finally, the concrete *settings or adjustments* of the policy instruments in a given field (Hall, 1993, p. 278). A goal could be to increase social equality, a policy-instrument could be taxes and the settings the level of the tax. In sum, the paradigm acts as a cognitive filter that determines the goal of action and the appropriate means and ends.

Paul Sabatier builds on the same intellectual sources with his advocacy coalition framework (ACF). It is useful because it provides causal arguments about how the policy process and paradigm competition work and is not just focused on ideational elements internal to paradigms (as Hall for example). Both Hall's and Sabatier's frameworks are mostly concerned with inner-state dynamics and thus are useful for theorizing norm emergence on a domestic level. Policy belief systems or paradigms have three elements that build upon each other.

The *deep core* includes general normative, epistemological and ontological assumptions. It tells actors what the world is, how knowledge can be gathered. It represents the broad roadmap for action. Known dichotomies such as liberal versus conservative, right vs. left or security vs. liberty/privacy operate on this level. Examples are anthropological arguments such as the evil nature of man or even technological beliefs such as "guns don't kill, people do", which will be further elaborated on in a following chapter (see chap. 2.3.1 Theorizing Technology: Traditional Approaches). These deep core

beliefs are socialized and hard to change. Building on top of these are *policy core beliefs*, which are the application of deep core beliefs in a policy (sub)-system. Policy core beliefs often "include projections of an image how policy or a policy subsystem "*ought to be"* (Sabatier, 2007, pp. 194-196). In other words, they include norms that shape the design of certain policy instruments. Norms shape policy problem definitions and goals, as well as the appropriate means-end relation to reach those (Jepperson, Wendt, & Katzenstein, 1996).

Secondary beliefs include applications of deeper beliefs, such as budgetary allocations or public participation guidelines in specific policy fields. They often include rational elements and are easier to change than the other two categories. Generally, alterations of secondary beliefs result from learning, new experience and new information. Deeper beliefs are harder to change and require external or internal perturbation such as shocks, which will be discussed in a later chapter (see chap. 2.2.4 Explaining Change).

Figure 1. ACF Policy Beliefs, Source: (Sabatier, 1998, p. 112)

Table 3 Revised structure of belief systems of policy élites* (1966)

	Deep core	*Policy core*	*Secondary aspects*
Defining characteristics	Fundamental normative and ontological axioms.	Fundamental policy positions concerning the basic strategies for achieving core values within the subsystem.	Instrumental decisions and information searches necessary to implement policy core.
Scope	Across all policy subsystems.	Subsystem-wide.	Usually only part of subsystem.
Susceptibility to change	Very difficult; akin to a religious conversion.	Difficult, but can occur if experience reveals serious anomalies.	Moderately easy; this is the topic of most administrative and even legislative policy-making.
Illustrative components	1 The nature of man: (i) Inherently evil v. socially redeemable. (ii) Part of nature v. dominion over nature. (iii) Narrow egoists v. contractarians. 2 Relative priority of various ultimate values: freedom, security, power, knowledge, health, love, beauty, etc. 3 Basic criteria of distributive justice: whose welfare counts? Relative weights of self, primary groups, all people, future	*Fundamental normative precepts:* 1 Orientation on basic value priorities. 2 Identification of groups or other entities whose welfare is of greatest concern. *Precepts with a substantial empirical component:* 3 Overall seriousness of the problem. 4 Basic causes of the problem. 5 Proper distribution of authority between government and market. 6 Proper distribution of authority among levels of government.	1 Seriousness of specific aspects of the problem in specific locales. 2 Importance of various causal linkages in different locales and over time. 3 Most decisions concerning administrative rules, budgetary allocations, disposition of cases, statutory interpretation, and even statutory revision. 4 Information regarding performance of specific programs or institutions.

The ACF assumes that a variety of policy actors (not just politicians but also journalists, military, scientists and civil actors) try to "translate components of their belief system into actual policy before opponents do the same" (Sabatier, 2007, p. 197). Different actors form advocacy groups around shared beliefs, which are in direct competition to promote their particular belief systems. The more (influential) actors adhere to a belief system, the better its chances to dominate. They create organizations and strategies to influence not just the political process but social discourse in general. The framework is

intentionally open to include a wide variety of actors in different structural positions. *Advocacy coalitions* are defined as:

> "People from a variety of positions (e.g. elected and agency officials, interest group leaders, researcher) who share a particular belief system – that is a set of basic values, causal assumptions, and problem perceptions– and who show a nontrivial degree of coordinated activity over time" (Sabatier, 1998, p. 139).

In this thesis, I use the term *policy-entrepreneur* or *advocate* instead of the term norm-entrepreneur that is often used in IR because it includes advocacy for ideas, norms and policies as well.[8] The key is that actors desire "to significantly change current ways of doing things in their area of interest" (Mintrom & Norman, 2009, p. 650), which means changing the status quo and changing the current orthodoxy or policy paradigm. Advocates try to translate their paradigm not just into the public discourse but also into the political process, also called *politicization,* which means that an issue becomes an issue of politics (Buzan et al. 1997, 23). I use this wider concept because it goes beyond traditional norm research. It opens the norm and policy diffusion process to all kinds of policy participants (McKeown, 2009, pp. 8-9) like interest groups, political parties, journalists, business, military, scientists and epistemic communities, individuals and many more (Sabatier, 2007, p. 192). What unites them is the advocacy for a certain paradigm and its norms (which is the glue that holds coalitions together). To increase their strength, policy entrepreneurs tend to seek allies who hold similar policy core beliefs, because strength in numbers allows for better expertise and more efficient influence. Within a policy subfield, a variety of competing advocacy coalitions can be expected to try to promote their paradigm as the dominant one.

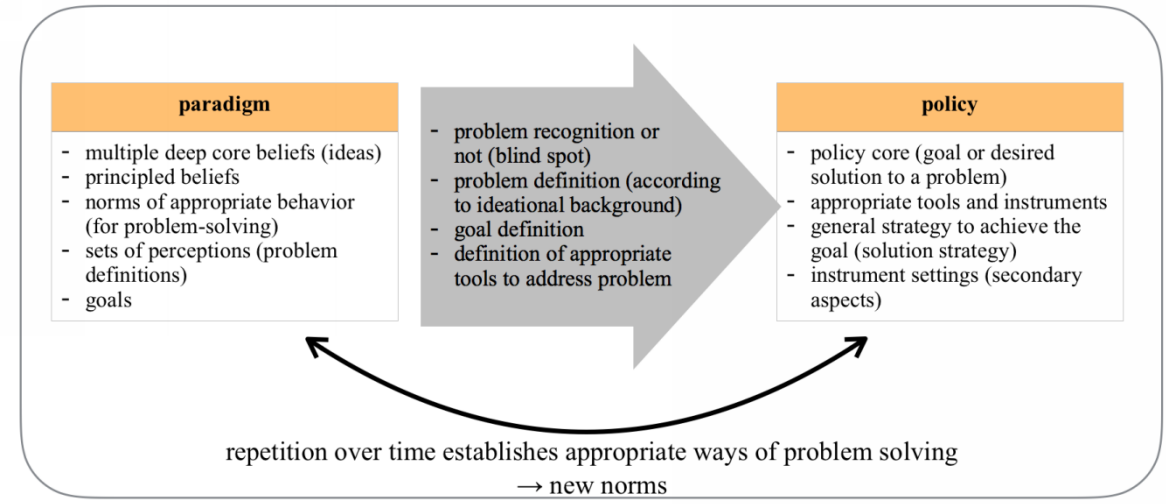
Modern versions of the ACF include elements of the so-called *political opportunity structure* research, which argues that actors have different resources and access to the political process. For example, the openness of a political (sub)-system matters. A policy *subsystem* "is composed of participants who regularly seek to influence policy within the subsystem" (Sabatier, 2007, p. 192). Subsystems are a result of functional differentiation and specialization of policy actors. The ACF differentiates nascent and mature policy subsystems. *Mature subsystems* include participants "who regard themselves as a semiautonomous community who share an expertise in a policy domain and who have sought to influence in that domain for an extended period" (Sabatier, 2007, p. 192). Foreign or national security policy can be assumed to be a mature subsystem which

[8] An alternative term could be "epistemic community", but since I want to include not just networks of actors with specialized knowledge, I use the term policy advocate or entrepreneur (Haas, 1992).

includes a broad range of already established actors like think tanks, military officials and diplomats. It can be assumed that it has a high degree of density and that it is hard for outsiders to get inside, which is easier in *nascent subsystems*. These "are nascent because of the instability of the broader political system and the lack of trained personnel" (Sabatier, 2007, p. 192). Nascent subsystems often do not have established routines and standards of appropriate behavior, which means they can be a fertile ground to study the emergence of new norms and paradigms. Internet policy, a theme of this thesis, is a particularly young subfield and thus a perfect case for studying norm emergence and paradigm change (Hösl, 2016). In general, it can be said that actors with greater proximity to the decision-making process have higher chances to embed their belief systems into policy.

If this statement is true, it allows to extract the normative components of policy bills as well as the underlying policy paradigm through the analysis of discourse surrounding their introduction. The ACF will be used in the empirical section as a blueprint to analyze Internet-related paradigms and policies that derive from these. The following figure summarizes the findings of this chapter and the central elements of a paradigm:

Figure 2. Policy paradigms embedding ideas in policy (own diagram)



Paradigms consist of deeply embedded ideational components such as ideas, beliefs and fundamental norms.[9] This ideational background guides the behavior of the carriers of this paradigm, called advocacy coalitions. These coalitions become policy-entrepreneurs by trying to translate their ideas into the political process, called politicization. To do so, they need to adapt their ideational components to the social reality by defining what counts as a

[9] From now on, different paradigms will be represented by different colors. One paradigm will be orange, another blue. This will be consistent throughout the thesis.

problem (and what not). This is a selection process and includes blind spots because not all problems are seen as such and not all are being resolved. The problem definition process sets goals to be achieved, as well as instruments such as policies and strategies/doctrines to achieve the goals. Advocacy coalitions try to shape the policy process and public discourse by creating policies and technologies, which reflect the paradigmatic elements.

This chapter argued that norms and policy often are interconnected and exist within one broader framework of paradigms, which can be measured empirically with the help of the advocacy coalition framework. Norms derive from ideas, which both are embedded in policy paradigms consisting of different elements (deep core, core beliefs, secondary aspects). Policy paradigms are the carrier medium for norms that influence the goal construction and influence how actual policy bills will be designed. A conservative policy paradigm will include *different* interpretations of social reality and different problem definitions than social democratic or liberal paradigms. Paradigms can be opposite ways of seeing the world, operating with completely different ground assumptions, for example about the nature of mankind or the nature of knowledge. To shed more light on these differences, I will make a short detour to introduce discourse theory.

2.2.1 Discursive Struggles between Paradigms

This chapter introduces some epistemological premises that are the foundation for the constructivist perspective in this thesis and that also represent the foundation for the logic of paradigms. I argue that (policy-) paradigms are sets of interrelated ideas (such as problem definitions, goals), norms (appropriate ways of problem solving and general behavior) and policies that stand in competition with other paradigms. Paradigms are transported by advocates and are written down on carrier-mediums in form of texts, doctrines, policy documents and more. Discourse theory allows us to understand this text and the competitive dynamic between paradigms. It offers some important insights that are useful for norm-research, as was already indicated in a previous chapter (see chap. 2.1.2 Critique of Deontological Norms). Furthermore, it provides some theoretical insights regarding the question of power and how paradigms can become dominant. Finally, discourse theory and the epistemological premises that are outlined in this chapter provide a coherent bridge between political science and Science and Technology Studies, which will play an important role in a following chapter (see chap. 2.3 Technological and Normative Change).

According to Adler, the primary element of (any) constructivist perspective is a metaphysical stance about reality, meaning that knowledge of reality is always mediated

through filters such as the context, socialization and language (Adler, 2013, p. 114). This means that all observation is made from a non-neutral position and already theory-laden. This is very much in line with what I said about paradigms. Because language is our main anchor to the world, the social reality can be conceived as a "text" that can be "read" (interpreted) by actors. Ludwig Wittgenstein rejected the idea that texts have one fixed (objective) meaning embedded in them (Jørgensen & Phillips, 2002, p. 96). Whether Harry Potter is interpreted as an imaginative child's novel or a representation of black magic and heresy depends heavily on the social background and cognitive paradigms of the reader. This means that it is hard, if not impossible, to reach any objective definition.[10] Freedom, ideology, democracy, power and other social concepts will always mean different things to different actors, depending on their cognitive paradigms, their socialization, history and the background discourse.

This focus on language and ideational aspects (ideas, norms) leads to the common critique of constructivism that it allegedly denies the independent existence of the material or objective world "out there" (Torfing, 1999, p. 45). While constructivists have this tendency, this argument confuses the *being (esse) of an objec*t, which is historically changing and the *entity*, which is not (Laclau & Mouffe, 1987, pp. 84-85). This resembles Aristoteles useful distinction between *matter*, meaning the material object, and its *form.* Matter is materially given. A stone is a stone and, depending on its mineral classification, its material components stay the same entity, independent of observation. However, the form or the being (we could also say identity) of the stone changes according to our interpretations and in dependence of social context (Cohen, 2016). The same stone can mean an endless array of things for us. It can be a weapon, a symbol for luck or value. In principle, it can get any conceivable meaning. The important constructivist insight is that the states of being (form, meaning) do not necessarily follow from the mere existence of the entity (material object or matter). Or in other words: "matter does not carry the means of its own representation" (Torfing, 2005, p. 18). Constructivism questions the assertion that the *form/being/meaning* shows us the *essence of an object* (Torfing, 1999, p. 46). Rather, social forms are what makes matter intelligible. Hence, a piece of land (or even technology) can be differently represented as a cultural site, a habitat, fertile farm land and so forth and this construction of the land also constructs different subject positions (land owners, urban developers etc.) and their paradigms (Torfing, 2005, p. 18). This *element of*

[10] I do not follow all the implications of strong interpretivism or post-structuralism and thus adopt a moderate constructivist position throughout this thesis. Moderate versions of constructivism argue that structures are important and that not everything is a matter of discourse. A strong post-structuralist program would also be partly incompatible with the version of process-tracing this thesis uses as a method (Bennett & Checkel, 2014, p. 15).

construction within the term constructivism means the intelligible construction of social forms through discourses. What constructivism constructs is neither matter nor the material object, but the form, the being of the very object.

This construction of meaning (form) happens within *discourse,* which is basically a meaning-formation. *Discourse* can be defined as a "differential ensemble of signifying sequences in which meaning is constantly negotiated" (Torfing, 1999, p. 85). The premise is that the meaning of words/concepts does not lie within them, but is externally attached with a process of signification: establishing a link between signified and signifier.[11] This process is arbitrary and there is no logical bond between the two. Rather, it depends more or less on historical context, social convention or habitualization. Thus, meaning is never stable. The same word, during the course of history, can get vastly different meanings, depending on its context. The central insight for this thesis is that:

> "Meaning of individual signs is determined by their relation to other signs: a sign gains its specific value from being different from other signs. The word 'dog' is different from the words 'cat' and 'mouse' and 'dig' and 'dot'. The word 'dog' is thus part of a network or structure of other words from which it differs; and it is precisely from everything that it is not that the word 'dog' gets its meaning" (Jørgensen & Phillips, 2002, p. 10).

Discourse theory implies a relational understanding of meaning. One meaning assigned to an object always stands in relation to other alternative interpretations from competing idea networks or paradigms (Weber, 2013, p. 46). If these relational arrangements change, the meaning of a concept changes. The premise of discourse theory is that the meaning construction via signification is the same for individual words, but also for social concepts such as norms, ideas, paradigms, but even for technology (which will be explained in a following chapter 2.3.4 The Social Construction of Technology and its Critique). Thus, discourse theory provides a useful bridge between the theoretical camps. Take for example this quote:

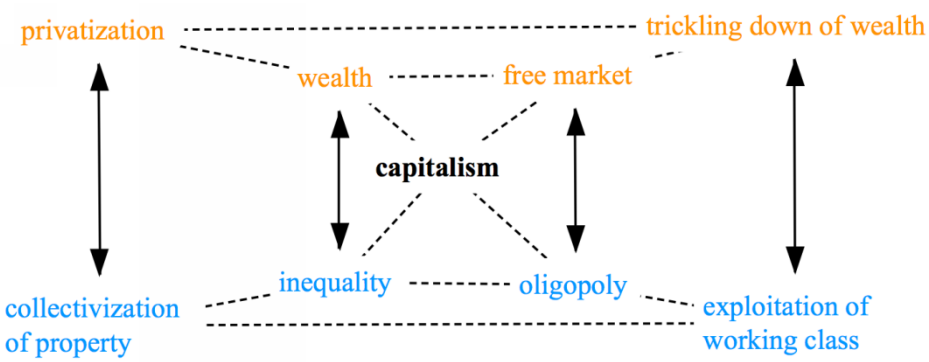
> "The same process - capitalist production and exchange - can be expressed within a different ideological framework, by the use of different 'systems of representation'. There is the discourse of 'the market', the discourse of 'production', the discourse

[11] The concept has origins in linguistics. The smallest element in language is the sign, which is a two-sided entity. Signs combine a signifier or form like a sound-image (a vocalized word) with a concept or content (the signified) (De Saussure, 1981, pp. 65-57). The gap between being (form) and entity (matter) can be traced back to this Saussurean distinction because language is always form, and never substance/essence (De Saussure, 1981, p. 113). The meaning of words does not lie within them (there is no essence), but is externally attached with a process of signification: establishing a link between signified and signifier. This process is arbitrary and there is no logical bond between the two, rather it depends on historical context, social convention or habitualization.

> of 'the circuits': each produces a different definition of the system. Each also locates us differently - as worker, capitalist, wage worker, wage slave, producer, consumer, etc […] All these inscriptions have effects which are real. They make a material difference, since how we act in certain situations depends on what our definitions of the situation are" (Hall, 1996, p. 39).

The following graphic visualizes the statement from the above quote. It shows how two competing paradigms (one we can call Marxism in blue, and the other Neo-liberalism in orange), engage in signification (fixation of meaning) of the same concept called "capitalism".

Figure 3. Meaning network (own diagram)



From the neo-liberal point of view, the concept capitalism is linked to a set of signifiers such as "free market", "innovation" and "wealth" whereas the very same concept "capitalism" within the Marxist paradigm is differentiated (arrows) against a set of other signifiers (like "oligopoly", "exploitation of working class" etc.). The difference in linkage ultimately produces a completely different meaning of capitalism for the actors that adhere to the paradigm. For one group, it is a positive term, for the other the enemy. Thus, meaning is relational. What a term means for a paradigm depends on the sum of signifiers associated with it.

The difference in meaning-relations is the reason why Kuhn argues that old and new paradigms are incommensurable. They may speak about the same things, but have different meanings of these things (Kuhn, 1970, p. 184). These signifiers can include both ideas and norms and thus allow for the conceptualization of *paradigms as interrelated norm- and idea-networks* (see chap. 2.1.3 Critique of Diffusion Models). In computer science these are called semantic networks. I will utilize the term *"norm-cluster"* or *"norm-network"* of similar or supporting norms on one side, being differentiated against opposing norms on the other side. For example, in a liberal paradigm the "norms of noninterference to the market" and "norms of private property" stand in close proximity to each other, but they stand in opposition/difference to competing norms (such as "collective ownership of

private property"). For this thesis, it means that advocacy coalitions with different paradigms compete with each other and engage in signification in order to fix meaning (the form) of social entities (actors, norms, ideas) or material objects (like technology). Discourses try to stabilize what a certain term or concept (for example digitalization) means for a society and thus how we *should* act. This means that they have concrete material effects.

But there is another reason why discourse theory is useful for this thesis and this has to do with the competition of two or more paradigms. Another assumption of discourse theory is that actor coalitions are embedded in a discursive struggle to make their particular paradigm dominant. Discourse theory argues that at the core of politics are "*hegemonic struggles* that aim to establish a political and moral-intellectual leadership [of a paradigm] through the articulation of meaning and identity" (Torfing, 2005, p. 15). Particular meanings can become the dominant reference point for social orientation and action and therefore are not questioned anymore. If the majority adopts one frame of reference, for example understanding capitalism in terms of free-market and privatization etc., this preferred reading is temporally fixed. *Closure* is defined as a "temporary halt in the fluctuations of meanings" (Rear, 2013, p. 7). Closure means that discourses and the signifying practices come to a halt and that one meaning-network becomes unquestioned, common-sense knowledge that requires no further justification. In other words, one particular meaning becomes taken for granted or internalized, which is pretty similar to the assumptions of the norm-life cycle presented earlier (see chap. 2.1.1 Norm Diffusion and Norm Entrepreneurs)

Another way to put this is the concept of *hegemony*, a term coined by Antonio Gramsci (Gramsci, 1971) which means that there is a "social consensus achieved without recourse to violence or coercion, and, like discursive closure, it is achieved through articulation" (Rear, 2013, p. 7). Hegemony does not mean leadership or authority (as in IR realism), but in discourse theory, hegemony is "the expansion of a discourse, or set of discourses, into a *dominant horizon* of social orientation and action […]." (Torfing, 1999, p. 101). The idea is that most participants in discourse adopt the same frame of meaning. In other words, advocacy coalitions want to expand their particular interpretation of the world or things (their problem definitions, their solution strategies) as the dominant frame that is adopted by a wider society. This fixation is an exercise of power, because it means exclusion of other meanings which become not realized. As such, a discourse is a reduction of possibilities. Translating this into power theories – a discourse is a macro

form of agenda setting power (Barnett & Duvall, 2005). One particular set of meanings is represented as universal pattern of recognition within society (Clegg, 1989, pp. 177-179).

This can be facilitated by *hegemonic practices*, discursive strategies that aim to reframe a particular belief set (or paradigm of one advocacy coalition) as universal (a guiding principle for everyone). These hegemonic statements often claim that there is a simple essence of things like: "the basic mechanism of society is supply and demand" or "everything that happens is God's will", etc.. They work through the backgrounding of the *contingent nature of social reality*: any meaning can be different or contingent during all times. No meaning is forever stable because there always are alternatives. Some sets of meanings "appear so natural that members of a society fail to see that they are the result of political hegemonic practices" (Rear, 2013, p. 8). Even terms like "god" change their meaning. For example, understanding "god" in terms of Christian signifiers is a widely accepted, taken-for-granted knowledge in Western societies whereas other significations of god like "Zeus", "Odin" or "Allah" are mostly excluded from public discourse (Hitchens, 2009, p. chap. 18). One single perspective is naturalized and objectified while the others are marginalized and silenced. Hegemonic statements thus often work with naturalizations: a process or a structure is depicted as a natural force that cannot be altered by human agency. These meanings appear as if they are objective. Objectivity is a term for things that appear as given and unchangeable.

Objectification is a process by which meanings "come to confront [the actor] as a facility outside of himself" (Scott, 2008, p. 125). They have become embedded in discourse, practice, institutions and therefore seem to be independent of social actors. Attached meanings can survive without actors of a coalition reinforcing it. The meaning stands on its own and becomes a social fact in Durkheim's terms (Hjern, 1984). Hegemony in this sense is a consensus, not necessarily based on coercion or violence, but rather at the level of "common sense" where the origin of a particular meaning and its intrinsic contingency is forgotten. This mean when a debate reaches closure, there is no more contestation, no more discourse. Philips and Jørgensen exemplify this phenomenon analyzing the social construction of childhood. Western societies perceive the concept of "childhood" as if it has certain essential characteristics and social norms ("children should learn", "live in a child-friendly environment" and "should have fun and eat candy" etc.). This is of course a contingent meaning because in both the agricultural and industrial revolution, children were treated as small adults who had to work and suffer like their adult counterparts (Jørgensen & Phillips, 2002, p. 35). That children should not work is a norm of the 20th century.

The next chapter introduces a final set of theoretical arguments that can be utilized to analyze the process of meaning construction of paradigms.

2.2.2 Framing

This chapter introduces a useful heuristic to assess the meaning produced by paradigms that is a bit more concrete than discourse theory and thus better suited for empirical analysis. Theoretically, this chapter could have been included with the last one, since it focuses on the construction of meaning. But since the last chapter was rather long and technical, I chose to present the framing approach in a separate chapter.

Of course, norm researchers recognize that norm-entrepreneurs or advocates are "meaning managers" and that they "attempt to convince a critical mass of states (norm leaders) to embrace new norms" (Finnemore & Sikkink, 1998, p. 895). Advocates want to convince a political audience to adopt an issue as relevant and to take action. Therefore, they have to translate an issue into an agenda item to gain support, first from their advocacy peer group and then later to gain public support for their cause. The overall aim is to translate a paradigmatic core policy belief (ACF) or a norm into actual policy:

> "The process of translation is directly equivalent to the process of problem definition, whereby objective social, economic, and environmental conditions are portrayed in ways that increase the likelihood that they will receive the attention desired of decision makers" (Mintrom & Norman, 2009, p. 657).

As was shown before (see chap. 2.2 Paradigms and Norm-Change), the *problem definition* is what connects actors, paradigms, norms and policies with each other. Therefore, it plays a crucial role in any framing attempt: "How problems get defined – or what attributes are made salient in policy discussions – can determine what individuals and groups will pay attention to them" (Mintrom & Norman, 2009, p. 652). A problem definition is a special type of articulation that fixes meaning. The way something is defined has fundamental impact on the question how it is solved – if something is defined as a crisis, it indicates urgency and calls for immediate responses rather than the development of more sustainable, long term solutions (Conrad, 2004, p. 315). Similarly, if something is declared as a war (like "war on drugs"), warlike responses are framed as appropriate. There are plenty different plot devices that can be used to signify certain meanings.

Frame analysis is centered on the idea that language is used for demarcating and punctuating important aspects of reality by making events and circumstances intelligible (Poletta & Kai Ho, 2008). Frame analysis is the methodological deconstruction of

signifying practices and hegemonic articulation and thus a useful subset for discourse theory (Lindekilde, 2014). The idea is to analyze:

> "How ideas, culture and ideology are used, interpreted and spliced together with certain situations or empirical phenomena in order to construct particular ideative patterns through which the world is understood, and which can be used to mobilize support of particular political goals" (Donati, 1992, p. 137).

That is why framing is particularly useful for this analysis, because it helps to understand the very process of translating a perceived problem into a general issue that aims at normative change.

Goffman (Goffman, 1974) coined the term *frame* as "schemata of interpretation that enable individuals to locate, perceive, identify and label the world out there but in ways that are intended to mobilize potential adherents and constitutions, to garner bystander support and to demobilize antagonists" (Benford & Snow, 1988, p. 198). Their function is to focus attention and define what is "in frame" and "out of frame" and therefore requires special attention. The visual notion of perspective is relevant to understand the process because frames represent a new angle of vision or vantage point (Benford & Snow, 2000, p. 623). They are strategically used by policy entrepreneurs to highlight certain elements and therefore to underscore a meaning, for example from "routine grievances or misfortunes to injustice and the need for action" (Snow 2004 quoted inLindekilde, 2014, p. 7). Frames are "persuasive devices used to fix meanings, organize experience, alert others that their interests and possibly their identities are at stake, and propose solutions to ongoing problems" (Barnett & Finnemore, 1999, p. 25), which closely connects them to the ideational aspects of policy as outlined in the previous chapters.

The core framing tasks are diagnostic-, prognostic- and motivational-framing, whereas the first two are related to consensus mobilization (creating a shared picture) and the latter aims at action.

Diagnostic framing refers to problem identification (identifying the cause of misery) and attribution of blame. The prime example is the so-called injustice frame, where grievances (bad working conditions for example) are reframed as a systematic failure caused by someone and not just mere accidents or random events: "since social movements seek to remedy or alter some problematic situation or issue, it follows that directed action is contingent on identification of the source(s) of causality, blame and/or culpable agents" (Benford & Snow, 2000, p. 616). By signifying some event or situation as "unjust", a certain normative position is taken which creates an imperative for action. Justice is a social category, not a natural one and justice must be provided, which aims at agency and

responsibility. Therefore, the act of framing is an articulation which connects a responsible cause with an event and thereby creates a certain meaning (that "x is unjust").

This is related to *prognostic framing,* which "involves the articulation of a proposed solution, or at least a plan of attack, and the strategies for carrying out the plan" (Benford & Snow, 2000, p. 616). The proposed solution is directly shaped by the identified problem. It constrains the range of possible (appropriate) solutions to tackle the problem and thereby includes a certain path dependency – when something is identified as unjust (compared to unnatural or inefficient), the solution of the problem will have something to do with the category of justice. Frames become relevant for social research when their targets (policymakers) accept a frame's definition of the problem and the solution (Poletta & Kai Ho, 2008). When policymakers adopt solutions advocated by advocacy groups it means that the issue is acknowledged and their vantage point is taken for tackling a problem.

Lastly, *motivational framing* resembles the call to arms or a rationale for engaging in collective action like forming an advocacy coalition or supporting a social movement. Ideally, motivational frames offer some legitimacy and provide reasons for taking action. Motivational frames are especially relevant for gaining support and forming advocacy networks to gain strength in numbers. Policy entrepreneurs often operate in networks that allow the pooling and sharing of resources needed to lobby for new policies. It is of course not just the appeal of the frame alone that determines whether it will result in actual policy. Rather, the power structure and the connections to government officials matter (Mintrom & Norman, 2009, p. 653). The general rule of thumb is, the more support for an issue exists, the higher the chances for policy change become. Similarly, the ACF argues that networks help participants to seek allies who hold similar core beliefs (Sabatier, 2007, p. 197) and framing is the mechanism to realize this. The combination of diagnostic, prognostic and motivational framing can influence both the establishment of core policy beliefs within actors for the first time, or the activation of those core beliefs that lead to entrepreneurship or support. Issues can be framed in a way that they activate support among a target audience that already holds similar core policy beliefs but did not yet realize it. Therefore, framing is a necessary part in the formation of advocacy groups in the first place.

Some frames are more powerful than others. A *master frame* is wide in scope, which means it has a high degree of inclusivity. According to Watson (Watson, 2011), master frames operate according to a certain grammar – they lift aspects into a new (legal) context, into new operational (policy-) fields or subsystems. Watson argues that *security is a master frame*, which is based on the framework of securitization (Buzan et al., 1997).

Security speech acts aim at shifting responsibility for problem-solving in policy fields to security actors (military, police). In other words, they represent *turf-battles* or disputes between (governmental) organizations about responsibilities and resources in policy fields. This is especially relevant for this project, which wants to analyze policy change regarding the Internet. The Internet was first framed as a matter of telecommunication and computer security and then later became a matter of national security, which marks a decisive shift in the operational field. Master frames often correlate with the hegemony of policy paradigms. Securitization scholars have repeatedly shown the reference to "security" is a common feature of political discourse, because redefines what counts as authoritative knowledge and who is in a position to speak. Dunn-Cavelty develops the notion of *threat frames* "whereby particular agents develop specific interpretative schemata about what counts as threat or risk, how to respond to this threat and who is responsible for it" (Dunn Cavelty, 2007, p. 30). Security frames in this sense work as marginalization devices which exclude civil actors from the discourse while promoting security actors. They also create a logic of exceptionalism and state of emergency (Watson, 2011, p. 289). Frames as exclusion mechanisms point to the fact that not every speaker has authority to claim something and that not all societal actors can influence policy changes equally.

This final section discusses the influence of frames and what characteristics they should have in order to become dominant. Which frame becomes the dominant one is a question of a frame's credibility and its salience within the target community. *Credibility* is a function of consistency with a paradigm's ideas and norms. A frame should be congruent with the ideas of a paradigm and should not include logical contradictions (internal validity). It also must match reality to some degree (external validity). Benford and Snow argue that a frame must not necessarily be true, rather must be readable as real (Benford & Snow, 2000, p. 620). *External credibility* is also a function of the speaker who must possess a certain authority to speak on behalf of the issue. This is where status and prestige matter. Whether a frame is accepted by a target population is function of centrality, commensurability and narrative fidelity. *Centrality* indicates a hierarchy of beliefs and values (as mentioned before with core policy beliefs). The more a frame is in line with core policy beliefs, the higher the chances that it will be accepted. For that it must be *commensurable*, meaning that a frame must be congruent with a person's horizon and cultural understanding. If a frame is to abstract, it might not get salience. Hansen and Nissenbaum for example argue that the discourse on data privacy and data security is a highly technical issue which is really abstract therefore quite incommensurable which explains the failure of digital activists to mobilize large numbers of support (Hansen &

Nissenbaum, 2009). Lastly, *narrative fidelity* often is important. If frames resonate with cultural narratives (for example the idea of the American frontier or the American dream), chances of success increase.

For my analysis, the focus on rhetorical framing is relevant because frames are the visible end-points of policy paradigms. Because they rely on language and images, frames can be perceived as the materialized condensate of normative beliefs which underlie every policy paradigm. The underlying assumption is that there is a direct connection between the components of a policy paradigm (core policy, principled beliefs, causal beliefs) and framing (diagnosis, prognosis, motivation). In sum, the main function of discourses and framing attempts is change. Discourses and frames attempt not only to change the meaning of a social situation or a technical artifact, they also aim at a change of norms. How change works and what conditions must be met for change is the topic of the next chapter.

2.2.3 Degrees of Change

Now that it is clear what paradigms are and by what actors they are carried, we need to analyze the notion of change. How do paradigms change internally, how do new ideas and norms develop that in turn might influence policies? This chapter also addresses external change: how can paradigms get replaced by others?

Peter Hall theorized *three orders of policy paradigm change*. The basic mechanism is what he calls social learning: the adjustment of "goals or techniques of policy in response to past experience and new information" (Hall, 1993, pp. 278-279). Actors are in continuous dialogue with their environment and are exposed to new phenomena. New problem recognitions might arise that create urgency and a need for adaptation, for example when a new technology is invented. *First order policy change* is based on alteration of the levels or settings of basic policy instruments, whereas the overall goal of a policy and the instruments themselves stay the same. This resembles the normal mode of politics where policy instruments (for example the rate of the income tax or the degree of child benefits) are slightly adjusted in the light of new situations (for example to compensate inflation). This is also called incremental change and is rather the norm than the exception (Eckstein, 1988). *Second order policy change* goes deeper. The hierarchy of goals stays the same, whereas the policy instruments to achieve these goals are changed. This depends on the perception of dysfunctionalities or anomalies. Hall shows in his famous study how Britain adopted a new financial policy of monetary control in 1971, where the neoliberal paradigm of Thatcherism replaced the social-democratic paradigm of Keynesianism (Hall, 1993, p. 281). The more severe the impact of an external event is

perceived, the more likely becomes an overall policy change. Finally, *third order change* alters the goals of a policy and with them the instruments and their settings. It happens mainly within a paradigm. The result could be a new goal and instrument adjustment of a policy field. Most likely, the underlying problem definitions also change. As a result, the content of a paradigm changes. But this change does not necessarily lead to one paradigm replacing another one as dominant. The hegemonic paradigm can stay hegemonic if it manages to implement the newly reconfigured meaning in the overall discourse, which will be discussed in the next chapter (see chap. 2.2.4 Explaining Change).

In contrast to the previous degrees of change, an external dimension of policy change is *regime change.* Within political science, the most obvious way how policies and their underlying paradigms change is when a new government comes into office, especially from another political party. New officials often adhere to alternate deep core policy beliefs and thus are likely to adopt new legislation. Of course, this is dependent on the type of political system, which serves as an intervening variable. A change in the dominant ideas of political actors creates new policies and norms. Change in this regard is not just social learning (as Peter Hall would argue), but also a matter of power, because policy belief systems are tied to advocacy groups. These are transporting this belief system and defend it in political discourse within a policy field. When a new party gains power it has greater possibilities to communicate its belief system to a wider audience.

Within the Advocacy Coalition Framework there are several intervening variables that shape policy outcomes. *Stable factors* like basic attributes or the problem (for example verification issues for cyber-weapons which are a result of the technology itself), the distribution of natural resources, fundamental sociocultural values and the the basic constitutional structure (Sabatier, 1998, p. 102). Norm research also argues that in more static political systems, or even in autocracies where there is almost no influence from the civil society, policy change and norm diffusion depends on the social learning of political decision-makers themselves (top-down diffusion) (Checkel, 1999, p. 90). Similarly, Cortell and Davies argue that the adoption of a norm is influenced by the organization of decision-making authority (central vs. decentral), the state-societal relations (close vs. distant) (Cortell & Davis, 1996, p. 453). More *dynamic factors* are changes in socioeconomic conditions (inflation for example), changes in governing coalitions and spill-over from other policy subsystems (Sabatier, 2007, p. 193). Sabatier argues that stable factors rarely change in decades and thus are of little importance for policy change in contrast to dynamic factors, which are a necessary condition for change (Sabatier, 1988, p. 102).

The most drastic version of change is a *revolution* or a *paradigm change* as described by Kuhn. Paradigm change is a social process that has a revolutionary character – one dominant paradigm gets replaced by another. *Scientific revolutions*:

> "necessitated the community's rejection of one time-honored scientific theory in favor of another incompatible with it. Each produced a consequent shift in the problems available for scientific scrutiny and in the standards by which the profession determined what should count as an admissible problem or as a legitimate problem-solution" (Kuhn, 1970, p. 6).

Scientific revolutions are not just about the change of ideas but also of scientific practices and norms. Such radical paradigm shifts produce a *Gestalt-switch* (a major change in meaning or how things are perceived) and with it a *normative change* (how we should act based on this new knowledge). These revolutions lead to the dismantling of old paradigms and their norms and the reconstruction of a new paradigm from the scratch.

So how do these revolutions work? It starts "with the awareness of anomaly, i.e., with the recognition that nature has somehow violated the paradigm-induced expectations that govern normal science" (Kuhn, 1970, p. 52). Anomalies basically are puzzles and problems that cannot be solved with current instruments or are inconceivable by the dominant paradigm. Some anomalies are so disruptive for a paradigm that they lead scientists to question their own practices and methodologies. Over time, core assumptions of the dominant paradigm become questioned – an anomaly turns into a crisis for the paradigm. A crisis is not just destructive, but also the necessity for novel theories because scientists begin to follow new tracks of research besides already established ones. During these crises we can witness a turn to epistemology and philosophical or metaphysical inquiry about the nature of things (Kuhn, 1970, pp. 73-88). This implies that there is a discussion going on about the nature of things and about the nature of that anomaly. Out of this effort, an alternative set of new problem-solving techniques based on new ideas, new premises can arise. Scientists normally are aware that "more than one theoretical construction can always be placed upon a given collection of data" (Kuhn, 1970, p. 73) and they build a new theoretical construct to deal with the puzzle – an alternative paradigm.

A *viable alternative paradigm* is a necessary condition for paradigm change. Ideally, the new paradigm is better in problem-solving than the old one and it must have some explanatory power to gather followers. In addition, because the new theoretical construct is often based on completely new premises, it requires a modification of tools, methods and the practice of science in general, hence it establishes new norms. A paradigm change is not a cumulative process,

> "rather it is a reconstruction of the field from new fundamentals, a reconstruction that changes some of the field's most elementary theoretical generalizations as well as many of its paradigm methods and applications" (Kuhn, 1970, p. 85).

Because everything is rebuilt, old and new paradigms are often incommensurable with each other. They cannot talk to each other, because even though they use the same vocabulary (like force, light etc.) they have different *meaning* (for example light understood as a particle or as a wave). This is the reason why (in the natural sciences) inter-paradigm debates cannot be resolved by proof and truth alone (Kuhn, 1970, p. 184). This has also to do with the social dimension within science, with the men and women in power positions who tend to defend their paradigm (Kuhn, 1970, p. 62). Professionalization and functional differentiation of science restricts the scientist's vision and leads to resistance. The paradigm will be modified in an ad hoc manner and try to counter its crisis. Kuhn quotes Max Planck: "a new scientific truth does not triumph by convincing its opponents and making them see the light, but rather because its opponents eventually die, and a new generation grows up that is familiar with it" (Kuhn, 1970, p. 151). This means that scientific revolution takes time, often a generation and that there is an overlapping period when old and new paradigms coexist in the population of practitioners. During this time, textbooks are revised and a new generation of scientists becomes educated with the new paradigm, slowly replacing the advocates of the old paradigm.

This does not imply that counter-discourses and alternative paradigms have vanished. They still exist, but their influence is limited. When I speak of paradigm change, I stress the notion of *hegemony-change* – paradigms becoming hegemonic while others get excluded. A hegemonic paradigm has greater chances to influence further norm development compared to non-hegemonic paradigms. If a new paradigm becomes hegemonic, the old paradigm is not abandoned (like old scientific paradigms) but simply loses its social influence (Meyers, 1990). Hall for example argues that the neoliberal paradigm of Thatcherism replaced the more social democratic Keynesianism in the United Kingdom in the 1970s, but the latter still co-exists (Hall, 1993). Ultimately, it is a question of power, also understood in institutional terms. There are privileged positions within a discourse that make it more probable that a certain meaning is heard by an audience. The social construction via the fixation of meaning is always a process of exclusion of alternative meanings. In this view, norm internalization is understood as accepting and adopting normative instructions of a new paradigm, which means silencing alternative

paradigms and their norms (Krook & True, 2012, p. 108). In this case, contingency is forgotten, because some meanings become stable while others are silenced.

This chapter explained the different degrees of change or to what extent change can happen. The next chapter introduces causal factors that help to explain when and why change happens.

2.2.4 Explaining Change

So far I have discussed what paradigms are, how they change and what different degrees of change we can differentiate. The question remains, *when* do they change? How can the theory explain normative change? Especially in longitudinal studies, one needs to look at temporal variables. Pierson argues that most works in political science have a "snap-shot" perspective on political processes. They analyze how variables work by ripping them out of their temporal context, assuming that they can magically travel beyond a unique configuration of time and place (Pierson, 2000, pp. 72-73). However, analyzing policy or paradigm change requires time, which implies a perspective of a decade or even more (Sabatier, 1998, p. 98). This chapter introduces several temporal and conditional elements that are relevant in analyzing norm and technology change.

A common way in IR to analyze change is to rely on a distinction between *normal times* like the normal problem-solving policy process described earlier (see chap. 2.2 Paradigms and Norm-Change) and *junctures*, "where movement along a particular trajectory is initiated, and the "mechanisms of reproduction" through which movement in a certain direction is perpetuated over time" (Thelen inRast, 2009, p. 395). Junctures are sudden changes in ideas, policies or norms. This can have the character of forking-paths. For example, during a crisis advocates of a paradigm can become disenfranchised with the paradigm or the supporting social group and therefore fork out, creating their own version or derivate of the core premises of the previous paradigm. The general argument is that decisions of the past influence decisions in the future, creating something that is called *path-dependency*. In a more narrow sense, path-dependency is based on positive feedback – an "early movement in a particular direction becomes self enforcing [and] increases the cost of switching to some previously viable alternative, discouraging exit" (Rast, 2009, p. 395). For example, a politician can be become "locked-in" by making a controversial decision from which he/she cannot back off. The premise of such arguments is that "early stages in a sequence can place particular aspects of political systems onto distinct tracks, which are then reinforced through time" (Pierson, 2000, p. 75). This effect can also be observed in discourse and language – new events always must be described with an

established vocabulary which creates a pre-structuration of new events within the cognitive frames of the old. This can be applied to paradigms as well.

Once a paradigm is shared by many (becomes hegemonic), it becomes the status quo or a representation of normality. Once something is perceived as normal, it is hard to change, because abandoning an already working paradigm is often perceived as risky. The burden of proof that the new is actually "better" than the established lies with the new paradigm. Baumgartner calls this the *power of the status quo*:

> "If the status quo policy is working reasonably well, and there are more pressing problems facing the country, it may well not be worth the risk. On the other hand, if a consensus emerges that the status quo is unacceptable, then suddenly the "risky scheme" argument may suddenly collapse" (Baumgartner, 2013, p. 252).

The power of the status quo is especially important in the policy-change literature, but has also been recognized in the field of International Relations. The longer a paradigm goes unchallenged, the more it tends to solidify, because repeated iteration strengthens behavioral patterns, thus increasing the cost for change (Kowert & Legro, 1996, p. 470). The costs for change might simply be too high, ambivalence about the outcomes may hinder progress or even the fear of social ostracism for challenging group beliefs can be relevant factors.

How can the power of the status quo be broken? In IR, wars, crisis, economic depression and revolutions are decisive junctures and thus moments for change. John Ikenberry argues that:

> "The importance of crisis stems from the intransigence of political institutions and relations. Politicians and administrators are continuously engaged in coping with socio-economic challenges; responses are channeled through existing institutions. At particular moments, however, these challenges call into question existing rules of the game and the repertories of state action" (Ikenberry, Lake, & Mastanduno, 1988, p. 234).

Dramatic events call into question the constitutive rules of the game, the standard appropriate procedures and practices (Florini, 1996, p. 378). In Kuhn’s words, an anomaly turns into a crisis of the problem-solving capacity of an established paradigm. The tools, techniques and modes of explaining and framing reality become incompatible with the unfolding events. This allows alternative paradigms to question the explanatory power of the status quo. "Crises are depicted as a type of collective electroshock therapy that jolts societies out of the extend modes of thought and gives them new ways of dealing with the world [...]" (Legro, 2000, p. 263). For example, Thomas Berger argues the pre-World War

2 paradigm of Prussian militarism became contested after the horrors of World War 2 and led to the norm of anti-militarism in post-war Germany (Berger, 1996). Shocks produce norms that aim to include the formula "action X should not be repeated" or prevented. Another example is the taboo to use nuclear weapons (Tannenwald, 1999). Shocks can help to "reset" cultural systems of meaning by creating large negative externalities. They change the conditions for social behavior by rendering once socially "accepted" behavior unacceptable and thus opening a space for new behavioral standards. Crises and sudden shocks produce incentives to reevaluate standard procedures and thereby create the *window of opportunity* (Kingdon, 2010) for new paradigms to replace the old, dysfunctional paradigm.

Similarly, Legro (Legro, 2000, pp. 263-266) argues that the *collapse of an idea-system* is shaped by two factors. First, the fit between social expectations and the shock event (a paradigm's explanatory power so to speak) and second, whether the subsequent outcome is socially desirable (or not). What Legro calls expectations resembles the procedure of problem solving of a paradigm based on deep core beliefs. If a paradigm did not conceive the cause of a shock because it had a blind spot, there is a clear mismatch between a paradigm's expectation and reality. This questions the problem-solving legitimacy of a paradigm. The new *shock-event must have certain characteristics*: if the event produced a favorable or desirable outcome (sometimes called luck), there is no need for change. If the shock produces negative effects, like a rise in unemployment or human suffering, chances are that this discredits the paradigm. From social movements research we know that movements form around perceived grievances like relative deprivation, alienation or bad life conditions of minorities (Snow et al., 1986, p. 465). A facilitating condition for this process is the *severeness of the perceived problem*. Non-existential problems will be much harder to mobilize, whereas substantial issues that attract/affect many people are easier to mobilize. What is important is the congruence between the type of shock (like a natural disaster), the domain where the shock happens and the features of the paradigm to deal with the event. A prime example is the reversal of Germany's nuclear exit strategy. Initially, the grand coalition wanted to continue to use nuclear energy, thus reversing the nuclear exit initiated by the previous social-democrat/green coalition. The Fukushima shock called the conservative idea of continuous use of nuclear energy into question because it initially framed nuclear energy as safe. The successful mobilization and counter-framing of the Green party forced the grand-coalition to abandon the continuation plans. This means that there will be events which a paradigm cannot explain and this

failure can disrupt the dominant meaning horizon. In sum, a crisis of a paradigm is the reversal of closure.

As a result, a new dominant meaning horizon can be reconstructed and new meaning generated, often from the very ground. Policy-entrepreneurs/advocacy coalitions engage in practices of contestation and shaming of prevalent practices in order to break open the status quo, to challenge the established paradigm (Finnemore & Sikkink, 1998, p. 897). It is important to note that shocks are not independent from the social world. A shock is not an objective entity, but socially constructed knowledge. In other words, the *framing of the shock matters*. While an earthquake is indeed shocking and horrific in our cultural understanding, in other contexts it might be perceived differently, for example as God's justified wrath that cleanses the earth from sin. There will be an extensive discursive trail during shocks when competing advocacy coalitions try to frame the event in their terms. Advocates of an alternative paradigm will seize the window of opportunity to challenge the status quo and establish their alternative set of meanings and norms as dominant.

Thus, for change to happen, a *viable alternative* must exist*,* a competing paradigm and a suitable advocacy coalition supporting it (Legro, 2000, p. 254). Key is plausibility and internal consistency of the new paradigm, as well as a strong supporting base (advocacy coalition) for it. Another factor is *prominence.* A paradigm and its norms must be famous enough in order to reach a wider cultural audience (Florini, 1996, p. 374). The more influential the entrepreneur, the more likely it is that the norm will receive prominence. If powerful actors, for example the president himself, follow a norm, they have more possibilities to promote them actively and chances are that less powerful actors start to emulate the norms. That is why hegemonic paradigms have greater chances to diffuse their normative assumptions. Furthermore, the new paradigm should fit (match) the desires of a target population. It must offer visible benefits or at least appear to be better. Kuhn would say it must be better at problem solving. Coming from agenda-setting theory, which tries to answer the question of how and when issues are propelled onto the agenda, Kingdon argues that within policy subsystems there is a "policy primeval soup" of ideas and from time to time some ideas are selected in the form of proposals to float on top (Kingdon, 2003, pp. 116-144). In other words, within a political system a set of already made policies or preliminary policy ideas exist, which are taken out of the drawer when a new situation arises. Kingdon argues that new ideas need a problem (event) to propel them to the status of agenda items. They rely on background participants to the political process (specialists, lobbyists, academics) which have to be brought to the attention of official

policymakers. Critical junctures allow an opening of a *window of opportunity*, lift issues out of the primeval policy soup and bring new problems to the attention of officials.

This explains why some shocks sometimes do not lead to policy change.[12] If no new paradigm is established, sometimes we can witness a rebounce-effect whereby the old paradigm survives and gets modified (internal change). Lastly, in the social world there is, at least theoretically, the possibility of rebouncing of core ideas of a paradigm. This concept could be called a renaissance of thought (which is rather seldom in the scientific world). Some key ideas of a previous paradigm (for example Franklin D. Roosevelts social policy "New Deal") might become popular again and can become implemented in present day politics.

In sum, paradigm change is a function of, 1) the failure of a paradigm, 2) the social construction of the shock in discourse and 3) the presence of a competing paradigm. Only if an event’s consequences do not match with a paradigm's expectations, it produces pressure for collective reflection, especially if the failure is unexpected. Based on social psychology, Legro argues that unexpected failure is likely to produce paradigmatic innovation because "people are more sensitive to losing something they expect than gaining something they did not expect" (Legro, 2000, p. 263). This could be observed during the financial crisis of 2007/2008 were a crisis (event) that was not (completely) expected by the dominant paradigm (mismatch between expectation and event) led to the adoption of new banking regulating laws. Interestingly, the crisis was not severe enough to seriously call into question the logic of neoliberal capitalism itself. Reversely, unexpected gain does not draw critical attention because nothing bad happened. If failure is expected by a paradigm, meaning expectations and the actual event match, paradigm change is unlikely because defenders of the dominant orthodoxy will reframe the event in their favor.

2.2.5 Norm Regression and Dark Norms

This chapter is meant to address the initial critique of norm-research and to add a final piece of the theoretical puzzle before the theoretical mechanism for norm and paradigm change is presented. The question is how do we address norms that prescribe standards of appropriate behavior, but which are not necessarily morally good or deontological. Finnemore and Sikkink (Finnemore & Sikkink, 2001, p. 404) argue in their assessment of constructivism that past discourse on nationalism, xenophobia or slavery constructed and reified different identities and norms (white master versus black slave) and defined

[12] Shocks may be necessary but not sufficient to change. A shock can be a trigger event, for change but a trigger might not necessarily be a shock. While shocks can "reset" cultural meaning systems, mere trigger events only lead to the adaption or reconfiguration of existing systems of meaning.

appropriate behavior for these identities. It was appropriate for the master to possess humans, to give orders and to punish them if they were disobedient or simply for masochistic pleasure. Constructivist scholars would argue that both actor categories had internalized the norms of their respective social class, as well as the class-structure itself. It was taken for granted. Since the middle-ages, the concept of serfdom had been the norm and had been legitimized in discourse on the divine rights of kings (dei grazia). It was thus a norm that many monarchies of that time shared. The question is: how do we deal with these kinds of norms?

Critical norm scholars formulate this critique and try to theorize so-called "bad" or "dark norms" (Heller et al., 2012) as well as negative norm dynamics which they call norm regression or decay (McKeown, 2009; Engelkamp et al., 2012; Deibert & Crete-Nishihata, 2012; Heller et al., 2012; Heller & Kahl, 2013). These are not ontologically different from "nice" norms, but stand in opposition to and actively contest them. The dark norm of serfdom contests the notion of individual autonomy, which is a norm in liberal societies. It can be argued that they have no deontological dimension in the sense of a moral obligation. Rather, they contest the very moral oughtness of nice norms. The re-emergence of torture within the Global War on Terror (GWOT) is one prominent example (Liese, 2009; McKeown, 2009; Sanders, 2012; Williams, 2011). Torture norms are legitimized on the ground that in the name of national security there must be an exception from the norm that prohibits torture. If more and more states challenge well-established global norms and engage in contestation practices (Wiener, 2007), a practice effect could kick in that delegitimizes anti-torture norms globally. In recent years, there has been a lively debate about how to conceptualize this "reverse norm dynamic, whereby deeply entrenched norms, particularly those related to civil and political rights, are challenged and discursively put under pressure" (Heller & Kahl, 2013, p. 415). The general argument is that there is not just positive norm diffusion, the global spread of human rights, but also a reverse process of *normative regression* (Deibert & Crete-Nishihata, 2012, p. 343) or *normative decay*.

According to McKeown, the norm-life-cycle must be completed to include the death of a norm (McKeown, 2009). It begins by questioning the assumption that internalization is the end point of Finnemore and Sikkink's norm life-cycle (Finnemore & Sikkink, 1998). Internalization is no determinism that leads in a single direction (the internalization of a norm), because contestation is always possible (as discourse theory assumes). As I have shown, shocks and trigger moments can initiate the re-contestation of hegemonic norms and practices. During these moments, actors who have not internalized the norms of the

dominant paradigms (norm-challengers) begin to question the hegemony or normality of a paradigm. First, this process is likely to happen internally within the context of a contesting paradigm, but over time this is likely to spill over into public discourse. If this creates enough public *resonance*, the dominant norm can lose salience, first domestically but possibly over time also internationally. McKeown does not go into great detail here, but I would argue that the conditional factors for norm-change, outlined in a previous chapter (see chap. 2.2.4 Explaining Change) also work in the opposite direction. They do not just explain how a norm can become dominant, but also why other norms fail. This could trigger a *reverse*, or *negative norm-cascade,* if enough global actors emulate this practice. This effect is especially powerful if former proponents of human rights norms (norm entrepreneurs or leaders) question the very norms they promote or act inconsistently with them. This will legitimize norm-breaking behavior by other states, creating a legitimacy crisis of a norm (Reus-Smit, 2007) which can lead to its death.

The discovery of bad or dark norms is crucial for this thesis. As has been shown, many studies of dark norms focus on torture and the reversal of human rights norms (for example refugee and asylum norms). One particular norm that is understudied by IR is the norm of mass surveillance that also is an offspring of the war on terror. The idea of dark norms and norm-regression is also important because it is compatible with the idea of norm-clusters. As I have argued before (see chap. 2.2.1 Discursive Struggles between Paradigms), norms should not be understood in isolation or without context. Instead we should focus on norm clusters supporting a norm, and opposing norm clusters from other paradigms. This holistic perspective allows us to have a more complete picture since the rise of one norm (dominance) at the same time often coincides with the regression, marginalization or exclusion of another one. Just as one paradigm gets replaced by another one, norms replace each other. For this purpose the paradigm concept is well suited, since I focus not only on one advocacy group with one norm, as many studies do, but on multiple advocacy coalitions and norms (and their supporting ideas) at once.

How this combined process of norm and paradigm change works will be depicted in the following chapter, which summarizes the theoretical mechanism presented thus far.

2.2.6 Summary of the Theoretical Mechanism

This chapter introduced a wide array of causal factors that are useful to analyze norm change and to address the aforementioned critiques and shortcomings of norm-research (see chap. 2.1.3 Critique of Diffusion Models). The purpose of this chapter is to fuse the

diverse factors together in order to create a theoretical mechanism that can be used for process-tracing.

I have argued that norm research has some problems *explaining norm-emergence*. Emergence often is a domestic process (Checkel, 1998). In my terms, norm emergence happens within social groups that I have called advocacy coalitions. Norms emerge out of repeated problem-solving activities of policy advocates. Problem-solving is the core function of paradigms that includes the recognition and definition of problems as a first step. The perception or framing of problems matters because paradigms perceive problems through their unique lens, from a specific ideational vantage point. The metaphor "If you have a hammer, every problem looks like a nail" fits nicely. Problem recognition depends on a paradigm's deep-core beliefs like epistemological and ontological ideas about what the world is about, what nature is and so forth. In a theoretical sense, problem definitions are also ideas that pre-structure action. This necessarily implies blind spots of unrecognized ideas.

After problems are recognized (or not, if they represent a blind spot), the process of defining the problem follows. *Problem definitions* are ideas that frame the *definition of goals* (what to achieve) and the *definition of appropriate techniques or instruments* (means to solve the problems). In the policy field, *instruments* to solve a problem often include new policies, but new technologies can serve the same function (as will be shown in the next chapter, see chap. 2.3 Technological and Normative Change). The key insight is that the *modalities of problem solving define a paradigm*. Thus, problems are solved by relying on more or less the same tool kit. For example, a military paradigm will try to solve most issues by military means. Over time, this repeated problem-solving practice of paradigm leads to the creation of standards of appropriate problem solving, which translates into *norms*. Theoretically, it is hard to determine the order of causation: whether norms influence the definition of problems, goals and thus policy or whether the repeated practice of problem-solving leads to new norms. This is not unexpected when adopting a discoursive perspective. Krook and True recognize that *norms are works–in–progress* and that process rather than stability is the default condition (Krook & True, 2012, p. 104). There is a relationship between norms and ideas and often it is difficult to separate them. Probably it is a circular process (Jepperson et al., 1996). The modalities of problem solving, over a longer time frame, become internalized and thus unquestioned standards of behavior for paradigm advocates. These norms are tightly woven together with the ideas of a paradigm. *Paradigms are idea- and norm-clusters.*

Paradigms also include a social process. The social component is quite important because paradigms require social actors and advocates. At first, these norms of a paradigm are only valid or *meaningful for the advocates* or carriers of the paradigm. Norms and ideas are transported, carried or reified by actors that become socialized into norm followers. The *socialization* of new advocates that follow the paradigm is quite crucial. In science, this includes the process of university education and degrees. In the social world, this includes institutions and career-tracks or even party-politics. This implies that paradigms can become *institutionalized* in organizations and social institutions like political parties, bureaucracies, the military, user-groups of technology and any kind of advocacy coalition aiming for political change (like NGOs or transnational networks). Norm-research calls these "hub-platforms" or arenas (Keck & Sikkink, 1994). Institutionalization is quite important to stabilize norms and to objectify them. Institutionalization implies the creation of *carrier texts* that transport the ideas of a paradigm. Textbooks in science and political documents like doctrines or manifestos can serve this function. This is in line with Kowert and Legro who argue that norm emergence results from the patterned interaction of actors and their environment, and social processes in groups such as common heritage, language or network structure which might increase chances for norm diffusion in smaller groups (Kowert & Legro, 1996, p. 470).

The important insight is that it makes no sense to observe paradigms in isolation. Paradigms and their advocates are assumed to stand in *competition* with each other. Kuhn argued that paradigms are often incommensurable, meaning they perceive the same social reality in completely different ways, thus identify different problems and adhere to different ideas and norms. A material object or a social phenomenon like a policy or shock event means completely different things for the paradigms, because their idea and norm-network produces different meanings. At the same time, paradigm advocates engage in the constant process of meaning construction. The assumed goal of this inter-paradigmatic struggle is the *hegemony of meaning:* the ideas and norms of one particular paradigm should become the general meaning horizon for everyone. Paradigm advocates, especially within the political sphere, try to alter discourse and to produce change. Their aim is to reach discursive dominance or hegemony. This inter-paradigm dynamic is important for *norm-diffusion* both domestically, but also globally.

I assume three different ways how paradigm advocates try to make meaning dominant: by the *construction of paradigm-infused policies,* via rhetorical *framing and argumentation in discourses* and via *technological artifacts* (which will be introduced in the next chapter). These are often interrelated processes. I have described in high detail how the problem-,

goal- and instrument-definitions infuse policies which, especially in the political sphere, are accompanied by framing efforts to legitimize policies. I argue that we can expect a congruence between a paradigms ideas and norms, its policies and the technological artifacts it engages with.

Whether the construction of social meaning and norm-diffusion are successful depends on a series of *conditional factors* such as the credibility, centrality, commensurability, narrative fidelity and hegemonic nature of *frames* and discursive articulations. Other factors are the nature of the policy subsystem in which this struggle takes place, whether it is pre-structured or not and whether norm-advocates are in a power position or not. I argued that paradigm advocates are not just transnational human rights networks but can be found at all level of politics, from presidents to military generals. The closer they are to the center of power, the higher the chances for successful norm diffusion. Other factors like timing and *windows of opportunity* also should be considered. I have argued that once a paradigm is in a dominant or hegemonic position, the power of the status quo and path-dependency might further stabilize it. Path-dependency also implies an early-mover advantage because new issue fields and nascent policy-subsystems are fertile grounds for new paradigms because there are no structuration or lock-in effects (no standards of appropriate behavior, so to speak).

If a paradigm reaches discursive *hegemony*, closure kicks in. This means that the meaning articulation and contestation stops and a temporary common-sense is achieved. Most, but probably not all of society perceive issues through the lens of the dominant paradigm. The general discourse will adopt frames, problem definitions and norms of the particular paradigm. The language of the overall discourse and that of a paradigm are in congruence. The ideas of a paradigm become a general frame of reference, *naturalized and objectified***,** as if they were not contingent anymore. This implies power, because all alternative meanings and frames of reference become excluded or marginalized. Once closure kicks in, it is hard to change.

Trigger events are often important conditions to introduce change. I have introduced different *degrees of change,* from internal or incremental change where the components of a paradigm are altered to different degrees to match new social reality. The adjustment of policy goals and their settings is a rather normal and constant mode of change in politics. With these degrees of change, the dominant paradigm can maintain its hegemonic position. Another normal mode of paradigm and norm change happens when a new government enters office that promotes a competing paradigm. Of course, changes of dominant ideas and norms happens over longer periods of time with some temporal lag and not just in time

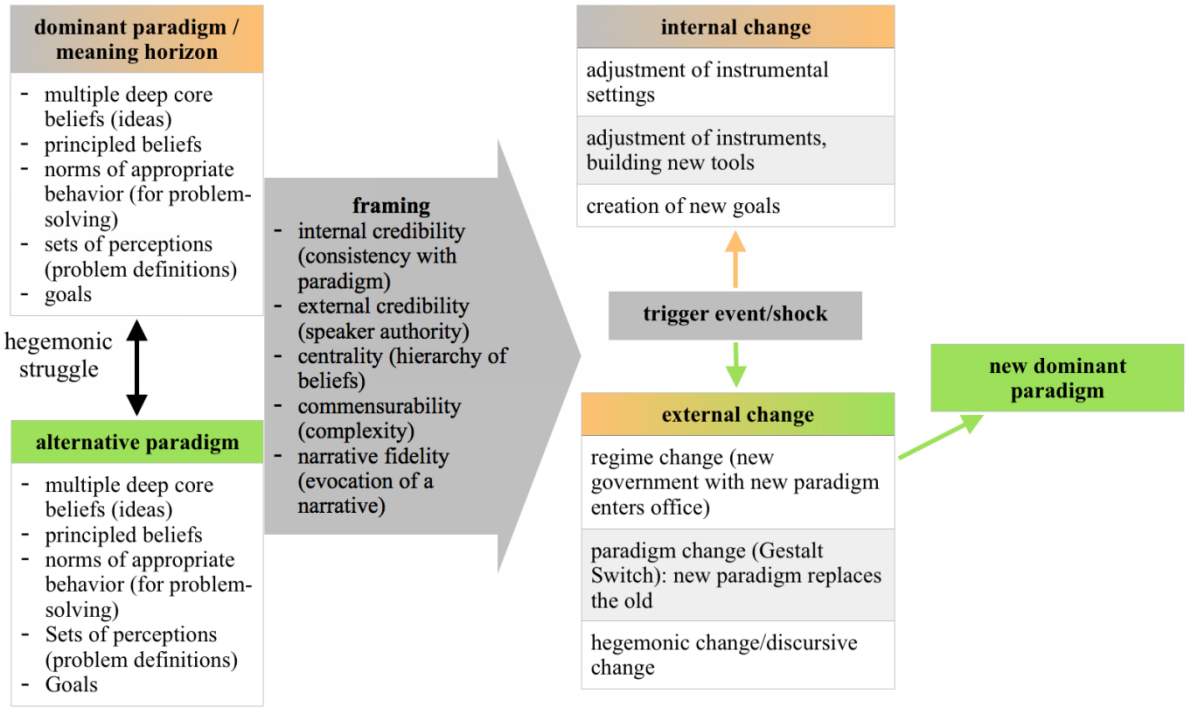
with the regime change. Due to the narrative description of change the reader might get the impression that idea, norm or paradigm change happens quickly, immediately after shocks for example. In empirical reality, ideas and paradigms change slowly and it often takes decades to realize this (Jacobs, 2014, p. 57).

But from time to time, social phenomena appear that present themselves as an *anomaly for a paradigm***.** Certain social phenomena irritate it because they do not fit to its expectations and are incongruent with its ideas and norms. I called these severe events *shocks* and they must have certain characteristics to induce paradigm change. The shock must call into question the core premises and problem-solving modalities of a paradigm. This is the case whether the problematic event developed out of blind spots (and thus its advocates could not anticipate it). There must be a *mismatch of expectations* between a paradigm and the features of this shock. If these events call into question the core premises, they can become an existential *crisis* for a paradigm. If this is the case, we can expect to see an inner-paradigmatic discourse about how to deal with this new reality, which might include ontological and epistemological debates.

Another important condition is the existence of an *alternative paradigm* that can challenge the dominant one. If the alternative can mobilize support and frame the event accordingly, it can replace the old one. This would be an instance of paradigm change. Hegemonic change, i.e. the change of ideas and norms in a political discourse normally is a slower process that often follows a paradigm change. The important premise of this thesis is that a paradigm change represents an instance of norm-change but of course norms can also change without the change of dominant paradigms.

The following graphic summarizes the process depicted in this chapter.

Figure 4. Paradigm change (own diagram)



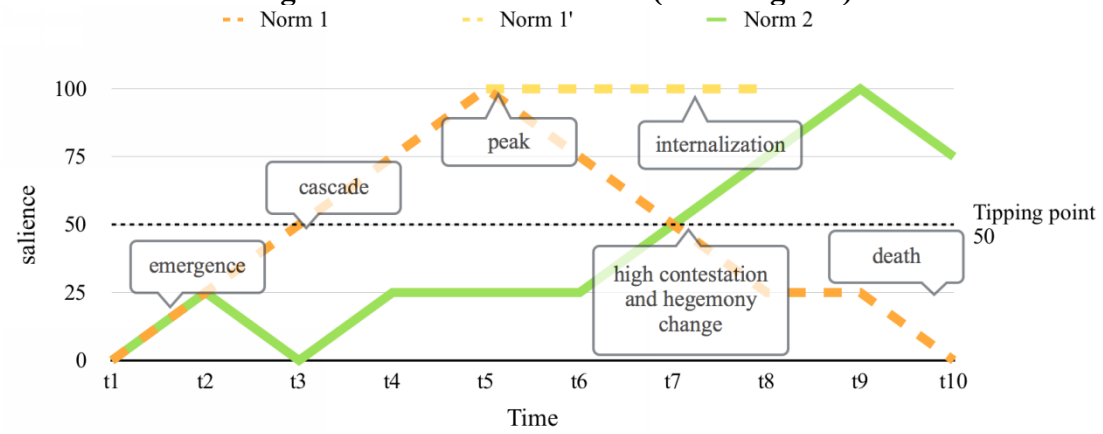
The figure should be read like a flow-chart from left to right. On the left, we see the discursive struggle between different paradigms, indicated by different colors, which engage in framing of a trigger event (or any social phenomenon). If a shock occurs, there are two possible causal pathways. In one instance, the orange paradigm adapts to the trigger event which leads to incremental change. The orange paradigm remains the dominant one (indicated by the color). If the shock represents an anomaly for the orange paradigm, and the green one uses the window of opportunity, it can induce external change. The green one replaces the orange paradigm, indicated by the color transition. Note that I will use a similar color coding through the entire thesis. Color transitions always mean the change of paradigm, ideas or norms.

If a challenger paradigm replaces an old one, an instance of *norm-decay or regression* might be observed. The norms promoted by the old paradigm can die out if they are not maintained and advocated anymore. Thus, the norm life-cycle only make sense if we broaden the scope to analyze the dynamics of competing norms promoted by competing paradigms.

This ideal-typical process plays out over time and is discursive from beginning to end. There are of course feedback loops that alter core paradigmatic beliefs. It is not necessarily a linear process. This process only becomes visible if one extends the analysis period beyond snap-shot studies and opens the analysis for competing norms and paradigms, which stand in opposition. The following graphic visualizes the process of

norm and paradigm diffusion (which I use interchangeably for now) I have described in this chapter by amending the life-cycle.

Figure 5. Diffusion of Norms (own diagram)



It describes the life-paths of two competing norms that are carried by two competing paradigms. It shows the salience or the adaptation of a norm by several actors. During the emergence stage, a norm has a low salience (of only a few actors in one advocacy group) until it reaches a tipping point of followers. The process leading to this point is discursive and can be explained with the concepts I have introduced. If successful, this leads to a self-reinforcing feedback loop (like in path dependency), resulting in a peak: the maximum diffusion is reached. This need not represent a 100% of all actors or state adopting a norm. Because different norms stand in opposition, the success of norm 1 results in the loss of appeal for norm 2. As long as some degree of support remains, norm 2 will not die out. It is simply not dominant or influential, which might change over time.

Now, traditional norm-life-cycles assume that norm 1 is internalized after the peak (turning into norm 1'), maintaining a high salience but becoming taken for granted. But as McKeown and others argue this is just one possible path not a determined process. Norms are neither static nor stable. Shock moments or gradual degradation might lead to a norm erosion (the reduction of followers). If the shock moment is in line with the expectation of norm 2 but unexpected for norm 1, the latter might lose salience. This is a window of opportunity for norm 2 advocates to contest norm 1, to establish its chain of significance as dominant. During this juncture at t7, there is the possibility for a hegemonic change. If this change is successful, norm 1 is replaced and there is the possibility of norm death. However, norm 2 is never stable and there might be another contester on the horizon.

The next chapter will introduce concepts that allow for the theorization of norms and technical artifacts. Since this thesis is about norm diffusion concerning a socio-technical

system, the Internet, it is necessary to introduce concepts from Science and Technology studies to IR. These help us to further refine the theories presented thus far.

2.3 Technological and Normative Change

"Every object tells a story if you know how to read it."
Henry Ford

While the previous chapter talked about the social construction of social norms, it is now necessary to talk about the construction of matter. Anthropologists and archeologists understand better than political scientists that technological artifacts are carriers of culture, ideas and norms. A *technological artifacts* is "a discrete material object, consciously produced or transformed by human activity, under the influence of the physical and/or cultural environment" (Suchman, 2003, p. 98). It can be argued that artifacts and culture can be examined with the same theoretical frameworks (Scott, 2008, p. 84). The aim of the overall chapter is to analyze the relationship between technology and social behavior, meaning and the development of social norms. This is done by arguing that technology is not separated from the social world bur rather embedded in it. The relationship of technology and the social world is one of reciprocal influence. What technology is and how we perceive it is a matter of meaning construction in discourses. I argue that the mechanism for social construction of norms and identity is similar to the development of technological construction. Additionally, already existing norms have an influence on the goal orientation that underlies technological construction. The paradigms of the inventors matter in creating technology. Their paradigms become embedded in technological artifacts and thus become mediated by them. As a result, the use of technology recreates the embedded norms, but sometimes also creates new ones.

2.3.1 Theorizing Technology: Traditional Approaches

Most people hold a *commonsensical definition or narrative of technology* that sees technological development as a linear reaction to human need (Häußling, 2014, p. 115). In this narrative, the necessity to survive against hostile nature drives technological invention of better tools. Nature and the artificial (technology) are seen as oppositional concepts. Technology is essentially seen as *neutral* and *instrumental* to human conduct. Artifacts are desocialized, which means that the social side (like power components, norms) is reduced to its (more or less) obvious function (Pfaffenberger, 1992b, pp. 494-497). Instrumentalists often claim that technology is *value-free* or neutral. An example is the argument "guns don't kill people, but people do". Human agency gives technology its determination (to kill) and thus is the main driver for social change. A hammer can be a means of construction or a means of warfare, depending on the usage. Likewise, disasters or accidents "result from faulty design or control, or from faulty operation, not from anything

inherent in the technology itself" (Tiles & Oberdiek, 1995, p. 16). Technology is seen as something distinct from the social world. Instrumentalists, too, decontextualize and dehistoricize artifacts which obstruct studying the historical development and their social embeddedness.

After screening the most important IR literature, Herrera argues that technology is either overlooked and treated as an "ad hoc exogenous variable – an unseen force" (Herrera, 2003, p. 566) or, especially in theories with a materialist ontology and rationalist epistemology (IR realism and neo-liberal institutionalist theories), treated as a deterministic force. For example, Kenneth Waltz argued in his "Theory of International Politics" that new military technologies increase military power of actors in the international system (Waltz, 1979, pp. 127-128). Technological development generates (external) pressures, because it alters the distribution of power and thus forces other states to adapt. If state A develops intercontinental ballistic missiles, state B has to develop a similar technology to catch up and to adapt to the new situation (arms race & security dilemma).[13] *Technological determinist* theories argue that technology is the *independent variable* that causally effects the social world in terms of security, global order or the nature of warfare. Especially in IR-realism we often find a *pessimistic* version of determinism that states that technology is out of human control and that it produces *negative (and often unintended) effects* in the social world, for example alienation, enslavement or security dilemmas. Technology is seen as something outside the social world, out of control of human agency. Once the genie is out of the bottle – nuclear technology as the prime example – it will spread and determine world order. For example it is often agued that the strategy of mutually assured destruction (that dominated the Cold War and held whole populations as hostages), is a direct result of the structural logic of nuclear ballistic missiles (Potter, 1978).

The opposite of pessimism is *technological optimism*, as can be seen with Robert Keohane, who argues that interdependence between actors increases with the emergence of new information technology (Keohane, 1979, pp. 85-109). Technological optimists assume that technology causes positive changes within the social world. Advances in medicine increase life expectancy and so forth. An extreme version of this can be called *utopism*, where technology alters human conduct to the better, like for example in Star Trek.

[13] Sociologists call this "technological push" and it is assumed that technological change is based on supply and not on demand for technology, which normally emerges later (Häußling, 2010, p. 626). The opposite concept is "demand pull", where customer articulate demands for a problem solution and mobile development efforts.

In optimist and pessimist versions of determinism, technological development is seen as a succession of steps that serve a single rationale (McCarthy, 2013, p. 473). The endogenous rationale of a technology determines the social world. In this perspective, nuclear weapons include a certain rationale (an essence or a metaphorical ghost in the machine) which automatically leads to specific social outcomes, for example the logic of nuclear deterrence. There is an implicit *teleological* assumption included. Technology seems to develop in a single linear, incremental process, from bows, to canons, to rifles, to nuclear missiles and so forth – a certain development will result in a distinct outcome, either instantaneously or over time. At the core of the teleological argument is a *logic of reflexive technization* – problems created by technology (or humans) are believed to be solved by more and better technology (Weyer, 2008, pp. 11-14). For example, a new weapon (missiles) might be countered with a new defensive (missile shield). This creates technological pushes and thereby an infinite progress. The role of human agency is negligible. "It is all about the object […]" which is the reason why this school of thought is sometimes called "anti-humanist" (Matthewman, 2011, p. 15).

Both determinism and instrumentalism assume that technology exists independent of any social context, and therefore is free from any social predisposition. Based on this perspective, technology is *discovered*. It is like finding an uninhabited island that was there all along, we just did not see it yet. A technological discovery just "pops" into existence. Innovations are independent from social relations and historical context. This is a somewhat pre-Kuhnian understanding of science and technology (McCarthy, 2013, p. 474). Both determinists and instrumentalists fail to recognize that technology is embedded in social structures which influence its development and use. Technologies are *developed* with a usage scenario in mind and are not just *discovered*. Some types of guns are designed for *more efficient* killing. The social shaping of technology during *development*, *usage* in different contexts and *discourse* is relevant and needs to be considered (Williams & Edge, 1996).

I will argue for a *social shaping perspective* that is compatible with IR constructivism. Here, it is argued that technology and the social world cannot be separated – technology is social through and through and not exogenous. Social determinism reverses the causal argument – the social determination shapes the design and use of the technology and thereby can control its effects. This perspective assumes neither an autonomy of technological development nor an existence independent from the social world. From this perspective, technology is always value laden and therefore cannot be neutral at all. Additionally, some technology intentionally was developed with power

projection and social exclusion in mind. Jeremy Bentham's circular prison (panopticon), as theorized by Michel Foucault, was intentionally designed as an automated power-projection apparatus that acted on those it sheltered (Foucault, 1979, pp. 195-231). The inmates in this circular prison are under constant surveillance, which aims at altering their behavior to automated norm-following.

Material artifacts and architecture are not just social, they are political and can express or even act out power. It is important to study not just the technical artifact, but also the designer and the design process. *Constructivists* claim to open the black-box of technical development to analyze the construction process that is socially determined by the intentions, paradigms, biases and norms of the inventors, which is why this is a more humanist perspective with a focus on human agency (Matthewman, 2011, p. 15). Social norms play a role during construction usage and discourses on technology, which is why this is compatible with the theories presented so far. However, on the extreme end, *social determinism* can tend to forget the technical artifact altogether because it focuses only on the social construction of technology. In some studies, materiality is a residue and all that matters is the form of an artifact. Bruno Latour argues against this perspective because it forgets the "things of things" (Latour, 2000, p. 112). This needs to be avoided. A social constructivist perspective on technology often operates with a special definition of technology, which is introduced in the next chapter.

2.3.2 Defining Technology

In order to grasp the social dynamic of technology we need a wide definition that recognizes that technology operates at multiple levels – it is not just the technical artifact and its material components, but also *design*, *use* by different actors and general relationship with the socio-economic *context* and *discourse* it is embedded in.[14] Hughes' study on Thomas Edison shows that several factors (economic, political, social, scientific and technical) must create a seamless web for technological invention like the electrical light bulb to be successful (Hughes, 1987). The competition between Thomas Edison's and Nikola Teslas's paradigms of electricity and thus competing designs of electrical systems, called the "war of the currents" (Alternating Current vs. Direct Current), shows the range of options and choices of alternative pathways a technology can take (McPherson, 2012). Science and Technology Studies deal with this complexity by adopting a systemic

[14] An alternative would be a *limited definition* of technology that focuses only on physical objects or artifacts. One of the drawbacks of this limited version is that many technologies now become digital and virtual and therefore loose their material features (also bio- or nano-technology) (Matthewman, 2011, pp. 9-12).

perspective, not just focusing on individual artifacts but on *socio-technical systems* – the interplay of social and material factors. I will work with this definition in this thesis.

A focus on socio-technical systems is to argue against the thesis of necessity of invention, because these systems are not inevitable in the sense that they are the only or best solution to a problem. These systems are sociogenic[15] and should be treated according to the logic of survival of the fittest – some are successful while other development paths die out. This perspective abandons the neutrality thesis of technology, which isolates technology from its social context thus claims that it is value free or without politics (Winner, 1993). It is also an argument against reductionist arguments like "nuclear weapons are neither moral nor immoral – they are just piles of chemicals, metals and junk" (Williams, 1984, p. 100).[16] While technically true, this is an intentional reduction of reality. *Reductionism* tries to artificially (and ideologically) separate technology from its usage context and how, why and where it developed in the first place. It is a version of hegemonic articulations. Politicians often use this rhetorical frame to justify the use of an ambivalent technology like nuclear weapons (Tannenwald, 2005, p. 11) or arms exports, although it is absolutely clear that nuclear weapons were developed in an enormous war effort to effectively kill thousands of people in a single strike.

The the relationship between the social and the artifact plays out during different stages, which will be central for this analysis: First, during the construction and the design process of the artifact, where the intentions, norms, values and paradigms of the inventor(s) are crucial. Most technologies are built for a reason, while others are solutions for unknown problems that, through reframing, become adapted in totally unintended ways and contexts. Other inventions are accidents that represent blind spots by the designers. Therefore, we to need include the social context of construction. Critics of the social shaping perspective argue rightfully that it is not enough to focus just on the construction because power is exercised while using a technology (Winner, 1993).

Second, the social use of a material object varies. It depends on who uses it, why an agent uses it, when and where it is used. Most technologies are *dual-use,* which means that they can be used for different purposes. The technologies for Uranium-enrichment can be used for building nuclear weapons or for civil energy. More so, not every agent can use every technology. Some technologies (such as the Large-Hadron Collider at CERN)

[15] Sociogenic means that something is caused by social influences.

[16] "Reductionism ignores the intentions, values and social understanding of those who design, develop, market and control technology; it also overlooks the understanding of users, consumers, beneficiaries, victims, and those deeply affected by technology whether they are aware of this or not. Finally, this reductionist temptation has a corollary that only the users of technology are responsible for harm, since all technologies are inherently without value" (Tiles & Oberdiek, 1995, p. 55).

require experts while others can be used intuitively by almost everyone. As such, human agents have different skills for using technology, which can be increased via learning. This means that there is an exclusion mechanism. The note that different actor (-coalitions) engage differently with technology is quite important when it is diffuses globally. Additionally, there are different points in time to consider. When a product becomes mainstream, its usage might vary from its first prototype, because a wider audience uses the object in creative and unforeseen manners. The development of usage scenarios are a matter of cultural norms and habits because they charge technical artifacts with collective significance, with meaning. As such, technology encourages the development of norms and is influenced by them as well, because of its social side. The technological object "automobile" led to the socio-technical system of "traffic" which includes not only cars and roads but a whole set of social rules, like driving on the right side of the road, stopping at certain road signs, using a seat belt while driving or even in terms of unregulated cooperation. When the "right of way" is unclear at a cross-road, drivers engage in sign language communication to determine who goes first. In these cases social behavior is coordinated without any rules or sanctions involved. Whoever has driven a car in the the United Kingdom stumbled upon the problem of driving on the left side of the road, which represents a major perturbation of appropriate behavior for continental Europeans. Clearly there are norms at work here. These norms are either included in technological design but are learned by practice of use.

Third, discourse and talking about technology frames its meaning (Weyer, 2008, p. 40). How a technology is represented and understood in discourse by competing advocacy coalitions matters. This can be grasped with the theories introduced before. The post-structuralist theorizing in the chapters before has shown that artifacts get their meaning in relation to other artifacts and that there is a discourse in place in which meaning is negotiated. The next step will be to shed a little light on the question how technology has been theorized by the social sciences before in order to provide the theoretical background for non-science and technology scholars.

2.3.3 The Politics of Technology Debate

Within Science and Technology Studies it is a conventional wisdom that technological artifacts have a social or political dimension. This and the following chapters deal with the question how to conceptualize the relationship between technology and the social.

Langdon Winner started this debate in the 1980s with his famous study "Do Artifacts have politics?" about the bridge design in New York during the 1930s (Winner, 1980).

Winner argues that the architect intentionally designed the bridges to prevent lower-class people, who relied on busses which could not pass underneath them, to enter certain parts of town. The bridge design acts out politics of exclusion (Joerges, 1997, p. 4). Winner seems to argue that the technological and social world are distinct entities and that there is a correspondence between the two (Hutchby, 2001, p. 443). This somewhat positivist notion assumes that with the help of scientific means, we can discover the true power essence of the technological artifacts and compare it with an observed outcome. That is why Grint and Woolgar call Winner's perspective *technological essentialism* (Grint & Woolgar, 1997).[17]

The critique is that intentionality is hard to prove because it requires a clear-cut causation between an actor's *intention* (i.e. the will for social discrimination), a technological *design* (a way to covertly achieve discrimination) and intended *outcome* (that this technology actually does what it is supposed to do to the target group). Disjunctures between intent and outcome exist because technologies almost always have multiple effects depending on the context in which they are used (Matthewman, 2011, p. 79). Even if we agree that Robert Moses' bridge design was intentionally discriminatory, it does not follow that this meaning is shared by the target audience (the people of New York). One can see a low bridge design as discriminatory, as the result of a cost-benefit calculus (lower bridge with less material = cheaper), erroneous architecture (like the Pisa tower) or carelessness or as a combination of all of these. Which interpretation is more true and which was the intent of the designer? Constructivism argues that perception of technologies is location-based, depending on different cognitive paradigms, a phenomenon called *interpretative flexibility*:

> "[…] associated with the design and interpretation (use) of technological artifacts; there is no unique (necessary) way of designing (or interpreting and using) technology; designs and interpretations (uses) vary across time and between different groups and cultures" (Woolgar, 1991, p. 30).

The assumption behind interpretative flexibility is that there are by nature different competing meanings about technology, but only a few become dominant ones. In terms of

[17] "The invocation of a causal factor implies that it is possible adequately to describe the key features and characteristics of the entity in question. But this runs counter to the principle of interpretive flexibility associated with the social shaping of technology. The construal of a technology as a causal factor seems to imply that there are definitive, identifiable features and characteristics of that technology, whereas the central thrust of social shaping is to suggest that such features and characteristics are contingent, that any such features we would wish to attribute to a technology are the temporary upshot of a series of complex social (definitional) processes, largely due to the efforts of particular social agencies (groups)" (Grint & Woolgar, 1997, p. 31).

discourse theory, interpretative flexibility refers to the field of discursivity. This is why the social shaping perspective is compatible with the IR-constructivist theories outlined in previous chapters.

This critique leads to the important reconceptualization of *technologies as texts* (Woolgar, 1991) that can be written and interpreted. The social side of technology, like all social phenomena, can be studied as if it were a text, introducing all the problems and possibilities of hermeneutics into Science and Technology Studies:

> "[…] technologies should be treated as 'texts' which are 'written' (i.e. configured) in certain ways by their developers, producers and marketers, and have to be 'read' (i.e. interpreted) by their users or consumers. The writers of these technology-texts may seek to impose particular meanings on the artifact, and to constrain the range of possible interpretations open to users" (Hutchby, 2001, p. 445).

The author of a text can try to put a certain meaning in the text, but whether the reader recognizes this and in fact is being discriminated against, is a different question. The agency of actor coalitions who engage in discursive struggle about the initial shaping and later interpretation of technology are of special interest. That means that technology is never free of meaning but always embedded in a net of prior knowledge. In sum, the material and the social side of an artifact cannot be separated but rather, they are one single thing as the figure shows:

Figure 6. Technical Artifact (own diagram)

technical artifact	
material dimension	**social dimension**
- entity, matter	- being, esse form, signifier
- design and shape - material used - complexity - affordances - software code	- norms - preferred meaning - usage context modalities - constructed subjectivities (users, admins, providers)

The material dimension means that the entity has a certain design and shape and is made out of matter that has certain affordances (physical properties). The software code that underpins software or Internet protocols is also a somewhat material category, although it blurs the distinction a bit (see chap. 2.3.7 Digital Technology: Software and Code). The social side, the *form* or *being* is interpreted. It includes preferred meanings that have been established during the construction, social norms of usage and usage context as

well as subject positions. The next chapter will explain how this social dimension works exactly.

2.3.4 The Social Construction of Technology and its Critique

As I have shown, IR has an incomplete understanding of technology and particularly IR-constructivism, with its focus on language, discourse and norms tends to neglect the material side of world politics. Therefore, I will introduce insights from Science and Technology studies to complement the IR-constructivist program.

Social Construction of Technology (SCOT) is a hybrid of social constructivism and sociology of knowledge. It argues that technology is social through and through (Bijker, Hughes, & Trevor, 1987). SCOT is a reaction to a strong technological determinist treatment of technology and claims to open the black box of technology, which means a closer look at the construction of artifacts within certain social contexts. In contrast to other approaches, it is highly compatible with the theoretical elements I have introduced so far.[18] It helps us understand how norms and technology are intertwined and how paradigms shape the perception, construction and reconfiguration of artifacts and their socio-technical systems over time. It also helps us study the diffusion of technology and norms embedded in them. However, due to legitimate critique on the SCOT program, I will amend this very framework.

SCOT rejects many basic and commonsensical assumptions about technology, for example that its development is a linear process driven by an internal (necessity) or external logic (demand-pull or technological push). SCOT is highly influenced by Thomas Kuhn's work on paradigms. The history of technology creates the illusion of a linear development because forking paths and dead-ends do not make it into history books. Pinch and Bijker argue with Kuhn that technology should be the *explanandum* and not the explanans which is taken for granted (Bijker et al., 1987, p. 24). Technology is conceptualized, planned and innovated by an interplay of competing human agents and not simply discovered. What technology is and what it means is the result of a discursive

[18] For readers coming from an IR background, Häußling (Häußling, 2014) gives a splendid introduction to various research programs within STS. Technic-determinist approaches (Jaques Ellul) are incompatible with the constructivist underpinnings of this thesis. Other viable approaches would have been a system-theory inspired perspective (Niklas Luhmann), which was not chosen due to its internal complexity and empirical challenges. Cultural studies (Lewis Mumford) offer valuable insights, but have a different macro-focus. Finally, there is Bruno Latour's Actor Network Theory (Latour, 2005b). Although I agree with many of ANT's insights, for example that technology acts as an actant or the rejection of linear development models, epistemologically this social theory is not really compatible with the frameworks I have offered so far. ANT is (in)famous for abandoning major concepts of sociology like the micro-macro or agent-structure dichotomy (Latour, 1996). Also, ANT is challenging methodologically, focusing on meaning construction in process, which is not possible for past inventions or places with access restrictions (Latour, 2005a).

struggle of different actors with diverging sets of meanings and expectations (paradigms) which help agents to "make sense of the artifact and the particular problems they face with it" (Bijker et al., 1987, p. 37). Because of interpretative flexibility, social groups have different interpretations about the meaning of technology and "the meanings given by a relevant social group actually *constitute[s]* the artifact" (Bijker, 1995, p. 77).

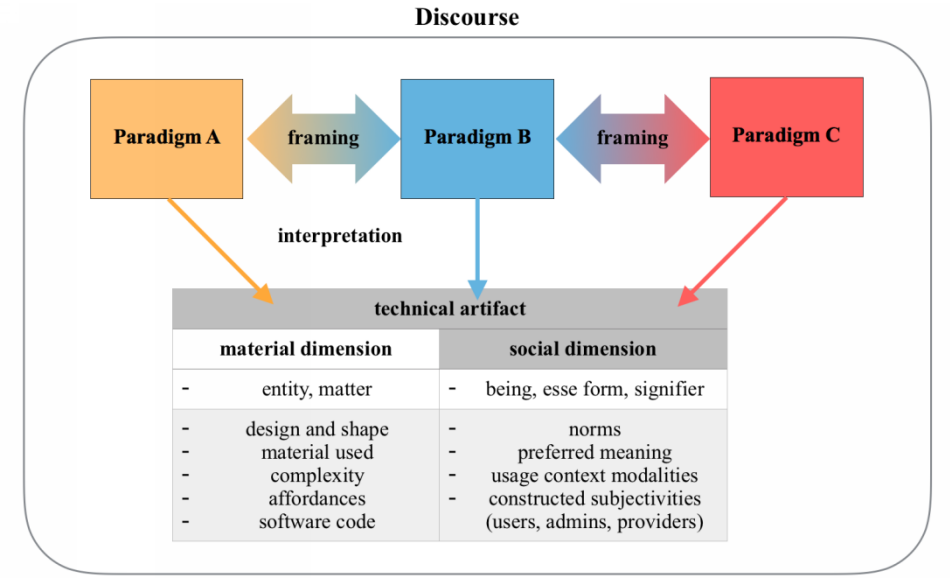
Pinch and Bijker illustrate this process of social construction in their study on the different developing paths of the modern bicycle. They ask how the dominant design of bicycles changed from large front-wheelers (called Penny-farthing) to a design with equal-sized, air-pressured tires (which is much safer and more comfortable). Between 1818, when the first two-wheel Draisienne was patented, and 1870 two competing designs were developed, which initiated a discourse on bicycles. The Penny-farthing was predominantly used and advocated by upper-class males ("dandies") to show off their skills in public parks as a form of entertainment. It could be argued that their use was similar to modern-day skateboards. The competing design was the equal-size bicycle which was more useful in a working-class context (transport) and could be used by women as well. Large front-wheelers were incompatible with the female dress-code of the time. The Penny-farthing excluded women because of its technological design and influenced norms that it was inappropriate for "ladies" to ride a bicycle (Bijker et al., 1987, pp. 17-50). Because it had several advantages and could be used by more diverse user groups, the air-pressure design became hegemonic in discourse and reached *closure*, so hegemonic in fact that this design of the bike is still dominant today. Closure in STS means that interpretative flexibility ends and a technological artifact gets a stable identity, a dominant design and usage modality. A *dominant design* refers to a kind of production standard, a way to produce things. While in the early stages of technological development, often there is no standard and experimentation by competing manufacturers goes on and over time one design will become dominant. A certain development path gets *locked-in.*

For SCOT, social equals technical construction. Different social groups (engineers, sport-enthusiasts, dandies, workers, women) engage in articulatory practices that aim to reduce interpretative flexibility of artifacts by fixing the meaning of technology. At the same time, the artifact constitutes or reimburses social identity, for example that of upper-class dandies or that of women as fragile as well as norms guiding the appropriate behavior of these identities. Pinch and Bijker explain the process of stabilization of meaning with the concept of *technological frames* that define problems, problem-solving strategies, theories, tacit knowledge, testing procedures, design methods, user practices, and exemplary artifacts (Matthewman, 2011, pp. 95-96).

> "A technological frame structures the interactions among the members of a relevant social group and shapes their thinking and acting. It is similar to Kuhn's concept of "paradigm" with one important difference: "technological frame" is a concept to be applied to all kinds of relevant social groups, while "paradigm" was exclusively intended for scientific communities. A technological frame is built up when interaction "around" an artifact begins. In this way, the existing practices does guide future practice, though without logical determination. The cyclical movement thus becomes artifact → technological frame → relevant social group → new artifact → new technological frame → new relevant social group → etc" (Bijker, 2008, p. 685).

Here, we can see similarities between the theoretical debates of advocacy coalitions and their competing paradigms within STS. Technological and political frames share the same logic and the same function, but deal with different problems. If technologies are treated as text, we can adopt all the theories that have been discussed so far. Furthermore, it can be assumed that the logic of paradigm change works according to the same parameters. Thus the argument is that different advocacy coalitions hold different paradigms that shape their interpretation of a technology (technological frame). Paradigms are in a discursive struggle, trying to attach their preferred meaning to an artifact by trying to convince their competitors in discourse with help of the social framing strategies discussed earlier (see chap. 2.2.1 Discursive Struggles between Paradigms).

Figure 7. Social Construction of Technology (own diagram)



According to SCOT, this means that there is no essence, no ghost in the machine that makes some artifacts automatically and objectively political. Rather, technological artifacts can *become politicized* in certain contexts, depending on cultural and societal elements. A

simple shoe for example does not seem to be that political in Western countries. However, it can become political in the Middle East when it is thrown at political leaders. This points us to the idea that the political qualities of technical artifacts are a function of several elements: *the goal oriented construction* and the values underlying the invention, the *technical realization of the product* (problem solving), the *meaning construction and discourse* around the object and the *intended and actual use by users in certain contexts and practices.* All these elements will be analyzed in the following chapters and also structure the empirical part of this thesis.

Constructivism is not without its critics. One of the big problems of the concept of interpretative flexibility is to decide when it stops. Even though the bicycle is a relatively stable, locked-in concept now (with two rubber wheels and a metal frame), the design is still contested by bike-enthusiasts because there have been further developments (new materials, new braking systems, new suspension forks etc.) or even new bike-designs (like recumbent bicycles). It is always somewhat arbitrary to set a point in time and declare a meaning and a technological design is temporally fixed and taken for granted. This problem is increased with digital technologies, which will be introduced a little bit later (see chap. 2.3.7 Digital Technology: Software and Code). Digital artifacts have no fixed material structure because they can be updated and modified relatively easily. There is no apparent solution to this problem and therefore the researcher is responsible to make his/her decision about closure moments as transparent as possible.

Geoffrey Herrera argues that constructivist approaches focus only on the emergence of technologies, but not on their effects or political implications after they have left the workshop (Herrera, 2003, p. 573). Similarly, Langdon Winner criticizes SCOT by saying it neglects the marginalizing and power effects that technology can have (Winner, 1993). This criticism is valid and I am sympathetic towards it, but it is not a critique of the constructivist logic and epistemology per se, but rather of its political implications. The problem can be solved easily with modified research designs, not just by looking at technological emergence, but also use and diffusion, as I will outline in the next chapter. In IR, critical constructivists already addressed this issue by pointing to power effects of social constructions, aiming to deconstruct taken-for-granted meanings in order to emancipate (Collective, 2006).

A general critique against constructivism is the *relativism* argument claiming that anything goes, as long as it is socially constructed (Herrera, 2003). In this view, a nuclear weapon can have any meaning, from being peacemaker to a weapon of mass destruction. I have addressed this critique earlier (see chap. 2.2.1 Discursive Struggles between

Paradigms). A similar critique is offered by proponents of the Actor-Network-Theory which argue that there is an *overdetermination of the social* and neglect of the "thingness of things" (Latour, 2000, p. 112). SCOT tends to favor the social over the hard material of artifacts.

> "At the extreme end of social constructionism (what we could call social determinism) material artifacts are forgotten altogether. Everything focuses on the social. The functionality and physicality of technologies disappears. Materiality is relegated to a residual category. Technologies are merely social constructions. This means that they exert no agency of their own, they have no effects. Their significance is only symbolic" (Matthewman, 2011, p. 18).

We should take Latour's criticism seriously and avoid the extreme notions of social-determinism and focus on the "thingness of things", the material artifact itself. The material structure of artifacts has some influence on the possibilities of *meaning construction in discourse*, as well on norms that develop out of using that technology. Some artifacts simply cannot be used for certain things because of their material properties. A hammer simply cannot have the function of an electron-microscope. This means that artifacts have different probabilities for meaning attachment. The artifact itself limits the interpretative flexibility. This means that in contrast to social determinism, the causality can go in both directions – the social determines the technical but in that process, there is a feedback loop from the technical to the social.[19] Verbeek calls this *co-shaping* between the social and technology: "What humans are and what their world is receive their form by artifactual mediation. Mediation does not simply take place *between* a subject and an object, but rather *co-shapes* subjectivity and objectivity" (Verbeek, 2005, p. 130). The invention of the railroad illustrates the cognitive shaping capacity. Verbeek argues that train traveling altered the perception of the landscape (distance itself) and also time, because suddenly it was possible to bridge long distances in short time which had never been possible before. Suddenly, time became more important, because trains needed precise schedules and standardized times. This co-shaping perspective is important because it assumes that new ideas, norms or paradigms develop out of using a new technology. Thus, paradigms do not always determine the interpretation of a technology but technology often leads to new paradigms. Galilei's invention of a new telescope for example provided,

[19] This problem is similar to the structure-agency debate in IR (Wendt, 1987) and sociology (Emirbayer & Mische, 1998). Anthony Gidden's concept of structuration also is helpful because he theorized the bi-directional nature of the structure and agency (Giddens, 1984). The advantage of STS is that it deals with tangible things like material culture. Whereas constructivism in IR often deals with ideational things that cannot be touched and thus, theoretically are more open to interpretation. This means that IR does not only benefit from imports from STS, but also vice versa.

for the first time, the empirical data to validate the heliocentric paradigm proposed by Copernicus.

To study the probability of certain interpretations, Gibson imported the socio-psychological concept of *affordances* to STS, which is used to describe the limitation of interpretative flexibility (Gibson, 1979). Affordances are defined as "functional and relational aspects which frame, while not determining, the possibilities for agent action in relation to an object" (Hutchby, 2001, p. 444). Affordances are a perceived property of a technical artifact that gives clues towards its use. This means that in the case of constructed matter, technological artifacts have a preferred reading built into them. This is not to be confused with determinism or essentialism, but rather a matter of probability which is affected by an objects' material features. Affordances do not change relative to the position of the observer. The edibility of a substance does not depend on hunger. Eating the wrong fruit can kill a human, independent of social constructions. Thus, Hutchby argues that there are some material effects that cannot be talked away: "the fact that a bullet fired from a gun has effects on flesh and bone that are intrinsic to the gun and bullet, and cannot be altered by social constructions" (Hutchby, 2001, p. 447). A bullet-firing mechanism has destructive properties per design and therefore it is very likely that humans will interpret a gun as killing device rather than a means of telecommunication (although a sound-based signal system is conceivable). If this was not the case, archeologists would not be able to determine the probable use of material artifacts they dig out. This does not mean that this is the only possible interpretation.

Another element that reduces interpretative flexibility is the *concept of utility*. Artifacts are designed to do things more efficiently and better. They might aim at maximizing utility. It is theoretically possible that I can use a fork to eat soup, but it is highly inefficient. A spoon does a better job. Therefore, it is more likely that a spoon is used for eating soup (which is a result of its design). Design delimits possibilities of action and interpretative flexibility. Interestingly, the word derives from the latin "designare" which means to signify, which is in line with Saussurean linguistics introduced earlier (see chap. 2.2.1 Discursive Struggles between Paradigms). I use the Oxford english dictionary definition of *design*: "A plan or drawing produced to show the look and function or workings of a building, garment, or other object before it is made" (Oxford English Dictionary, 2017). Design is not understood as the way something looks, but rather how it works. It refers to functionality as well. But the design process is just the first step. The second step is made by the user. According to Hutchby, this works similar to *conventionally paired actions* like invitations and responses: a practice demanding a

reciprocal action (Hutchby, 2001). He criticizes that the SCOT approach falsely inverts this relationship – technologies are seen as formless first moves in the sequence and that the second move, the interpretation defines what the technology is. Rather, we need to look at both, material properties and the realm of possible readings.

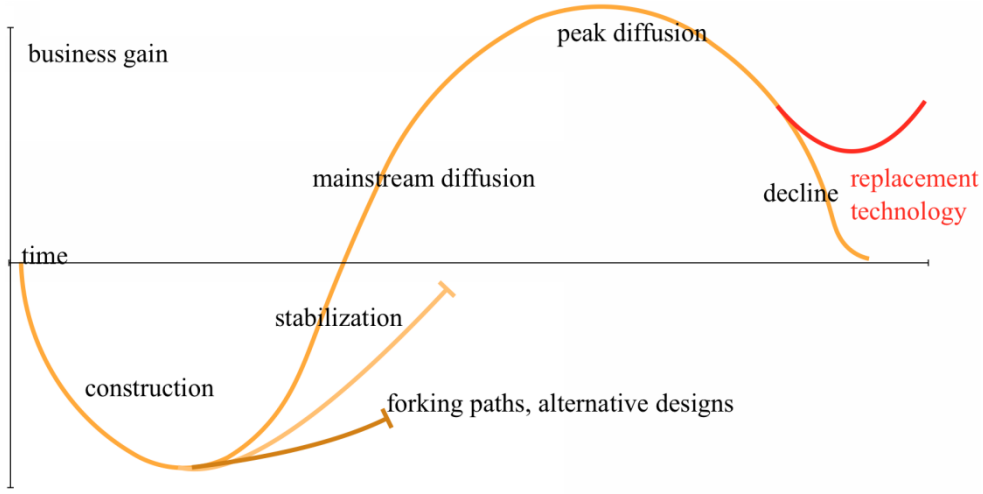
This discussion implicates that it is not enough to look at the process of construction alone, but do adopt a holistic perspective on technology that includes usage and discourse as well. We also need to consider the possibility of co-shaping of artifacts while they are in use. The next chapter introduces a temporal model that accounts for this.

2.3.5 Phase Model of Technological Diffusion

We have already established that technology does not pop into existence out of thin air, it is not exogenous to social development and it is not teleologically determined. Rather it is a process where different social, economic, political and technological factors come together which shape the socio-technological system.

Weyer proposed a multi-tiered model of technological diffusion – from invention to mainstream diffusion a technology (Weyer et al., 1997, p. 31).

Figure 8. Phase Model of Technology (own diagram)



This model helps to explain who influences a technology, when and how, both technically and socially. The construction is carried out over time by changing actors which have competing visions (paradigms) about technology and who are in a discursive struggle over dominant technical designs and social meanings. Whereas the SCOT approach mostly analyzes the first closure moment of technology, this model allows us to theorize later points in time (the effects of a technology). The model assumes three development periods: 1) emergence/construction, 2) stabilization of a design and a prototype and 3) diffusion to

the mainstream (market diffusion). At the end of each phase, there is some kind of closure that has path-dependency effects towards the next phase. Technology diffusion is no automatic process but social. The model adopts neither social nor technological determinism (Weyer et al., 1997, p. 34).

The model is based on the investment-cost S-curve[20] and includes designers, marketers and users of a technology. It argues that these matter during the different stages of technical and social construction. In the early stages, the influence of the designers on the social meaning construction is higher, but as soon as a technology reaches a mass-market, the users engage in the construction of meaning and social norms as well. While in the beginning, there naturally is a limited coalition of users who speak about the artifact, over time, as mainstream diffusion kicks in, more users will engage with the technology. This opens up the discursive space and more and different actors will negotiate the meaning of the artifact and also might establish new usage-scenarios.

It is important to note that during each juncture there is the possibility of failure: a visionary idea might not be developed. A finished prototype might not make it to the market because of insufficient start-up capital or socio-economic factors that prevent success. With each juncture, alternative technical solutions to social problems are evaluated and a certain design is favored over others. Design A might be adopted and sold at the market, whereas alternative design B is abandoned or re-modified and re-introduced in a different context. This is called a *forking path* of technological design. An alternative design can become a spin-off project initiating an individual path trajectory. Historically, the alternative forks are often forgotten (Zeppelins for example are a "forgotten" fork on the pathway of aviation). Forks are like railroad switches, that changes the direction of the train (Rueschmeyer, 2008, p. 234). The aforementioned war of the currents between Nikola Tesla and Thomas Edison is such an example of closure: Edison had the greater resources and the better support network (including political access) to make (the inferior) DC-electrical current a standard during the early days of electricity in the United States. Edison also engaged in the social meaning construction by framing the competitor as an evil technology that can kill people, utilizing AC to power the first electric chair (King, 2011). The direct current mass-diffused through the market and established a dominant pathway. DC became the dominant design for electrical currents in the US: Tesla's AC current forked and developed on a different path, becoming more dominant in Europe.

[20] It means that before a technology becomes profitable, it requires initial investment. At some point, diffusion kicks off and a product becomes profitable. Over time, the product reaches peak diffusion and then sales decline, until the product disappears, often because it becomes replaced by a successor technology.

Within the social context of climate change and the need to preserve energy, the AC current finally replaced DC current, even in the US.

2.3.5.1 Emergence/Construction

This chapter aims to highlight the construction/emergence and design process of technology and what role paradigms play therein. The first step in technological life-cycles is the process of invention where the influence of the designer to shape the artifact is at its highest. An act of construction is never neutral or value free but rather resembles the cultural features of the context and the personal biases and paradigms of the inventors that often become embedded in technological artifacts. So why are technologies invented and constructed in the first place?

Technology often deals with the realization of certain goals (called *goal-oriented construction*). Technological devices are designed to perform a function that helps to solve problems, like survival in a hostile environment. The goals could be manifold, for example making processes more efficient, more reliable, more precise or even to realize something in the first place, like flying or traveling to the Moon (Häußling, 2010, p. 624). This need not always be rational. Some technologies, like toys, self-deactivating machines or sculptures are invented for no obvious necessity reasons. Many inventions are *solutions looking for problems*, meaning that the inventor does not yet know what practical implications an invention will have and whether it has any commercial potential. This sometimes only becomes obvious during the stabilization or diffusion phase.

The *invention or construction phase* is not a straightforward process from goal to design, to a working prototype, to market diffusion. Chance is an important factor in every innovation process and many inventions, like Penicillin, were made by *accident*. A design seldom falls from the sky like Isaac Newton's apple. Rather, often a trial and error process leads to a design (deductive tinkering). During this conceptual phase, important decisions are made. What is the nature of the problem (cause) to be solved? Where does it occur, is there a pattern? The norms and ideas of the designer and the context of invention pre-structure goal-formation and the appropriate solution strategies to solve the problem, as was shown before (see chap. 2.2.3 Degrees of Change). Remember that a problem is defined as such only when there is a social group for which it constitutes a "problem" (Bijker et al., 1987, p. 30). What actually constitutes a problem worth solving depends on the inventor's socialization and world view (or paradigms).

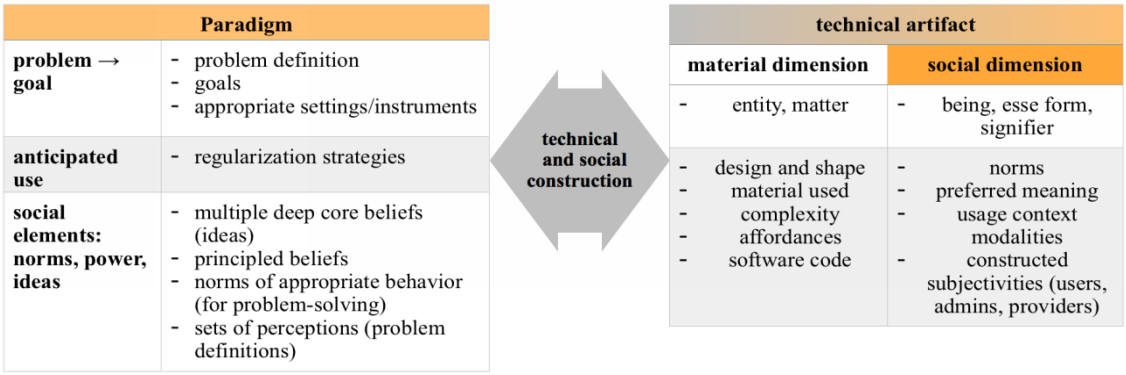
> "Just as artists naturally express their artistic values in their art, so do the makers of technologies. If, for instance, price is more important than safety in the minds of the manufacturers, their products will undoubtedly embody that trade-off" (Tiles & Oberdiek, 1995, p. 46).

Organizational cultures and the structural context of innovation also matter. It makes a difference whether a technology developed within a military or a civil context. The result is a *core invention, a central idea* that represents the identity of the artifact but is not yet the prototype. According to Weyer, this core consists of two elements, a technical configuration like a construction principle and a social configuration (Weyer et al., 1997, p. 37). This is where norms come in.

The technical-instrumental configuration can be called a design or construction principle that often is only known by the inventors of a product. Therefore, their voice is important in researching this goal. A design principle could be to make a system as reliable or as easy to use as possible. To speak in a metaphor – the intention and subjective beliefs of the initial designer are engraved into his invention; he puts the ghost into the machine by shaping the object. This is where the technological bias or affordance for certain practices and values comes from. Of course there are alternative ways of solving the same problem (again, think AC and DC currents). This means that a design decision always is the reduction of possibilities, the exclusion of alternative designs. This is similar to discursive articulations and one might even argue that design is a discursive act. For example, most tools are developed for right-handed humans, and exclude "lefties". More so, a design decision shares the characteristics of an articulation in discourse theory.

The second component is the social configuration or an anticipated arrangement of relevant actors (both creators and users). Often it is not just one inventor but a social network of supporters. This means that group dynamics should be researched as well. The designer(s) anticipate(s) both usage scenarios and potential users as well as the appropriate roles for the users, as the Penny-farthing example showed (see chap. 2.3.4 The Social Construction of Technology and its Critique). This is where power components and norms come in. The design implicates that a technology should be used in a certain way, implicating norms of practice. Here it becomes clear that during the process of construction, different actors matter at different points in time. The construction process according to an integrated functionalist and social constructivist argument looks like the following figure, which combines insights from the previous theory chapters:

Figure 9. Relationship of Paradigms and Artifacts (own diagram)



The designer holds a certain pattern of ideas and norms which I have called paradigms and which outline the problem an artifact is designed to solve, the technical solution to the problem (which becomes the design) and the anticipated usage modalities (user subjectivities) as well as the preferred meaning. During the construction process, this paradigm becomes embedded into the artifact, more precisely in its social dimension (matching orange color). The artifact temporally means what the designer intended and includes the norms he/she envisioned. Often this is a bidirectional process. The artifact can influence the paradigm, especially because during the next phase, stabilization, where new ideas are developed.

2.3.5.2 Stabilization

Stabilization is the process from experimentation and tinkering with ideas towards a working prototype. To be successful, an artifact's usage context must be widened and therefore, it must be transferred and translated from the workshop to a market of customers. Inventors often have no business or marketing experience and therefore, much depends on establishing the right connections to the industry. This is often realized by cooperation or partnerships, which connects inventors and strategic actors. During the stabilization phase, the loose and informal inventor network is expanded and often other actors come in (politics, military, corporations and hardware suppliers), which results in a recombination of relevant actors and their social structure surrounding the artifact (Weyer et al., 1997, pp. 40-46).

Resource exchange and bargaining processes between the actors further influences the design process. Different interested actors debate about the vision and the artifact itself, which means that there is a discourse within the network about the design and its meaning, norms and target social context. For example, an artifact that was initially intended for the consumer market might be interesting for the military, which then demands ruggedization of the design, making it more robust in combat. This might alter the design and function of

the artifact again. At some point, central design features are chosen. Although the identity of the socio-technical core remains the same, certain adaptions and refinements happen in this stage in order to allow a marketization of a product.

For a successful stabilization several conditional factors matter: 1) the technological design of a product must be good enough to reach a wider audience. If it is buggy or unintuitive, it will most likely fail because users will not adopt it. 2) The entrepreneurship of the company or funders matters. It is a quite complex endeavor to bring a product to mass production and to distribute it worldwide. There are production, transportation and marketing costs involved, which often are too high for small start-up companies. Therefore, their product must convince potential donors as well as a target audience, which might not be the same. Thus, the initial design of a product comes under scrutiny during this phase, because if a potential donor demands changes, it alters the technology. 3) The mainstream must be receptive for a new technology. Sometimes the time is not "ripe", so timing matters as well as the cultural technological background context. The crucial test is to see if a product works outside laboratory conditions. Lots of projects never reach the end of the stabilization phase because of incomplete innovation. If the social network can successful stabilize the socio-technological core, its stabilization leads to marketing success and the diffusion to the mainstream begins (Weyer et al., 1997, pp. 40-46).

2.3.5.3 Diffusion to the Mainstream

Diffusion of technology aims at finding or creating a market for the artifact, thus initiating a demand-pull and a self-sustaining user demand for the new artifact (see chap. 2.3.2 Defining Technology). The problem most technology face is that most users are conservative: they do not adopt a technology just because it is new. Users need to be convinced that the technology is useful and better than alternatives. This is often the function of marketing and discursive framing of a technology. The creation of a usage vision, narrative and new usage scenarios is key here (Weyer et al., 1997, p. 47). This is often done with pilot studies or public presentations. This is also a *de-contextualization*: the new artifact must be successfully embedded in new usage contexts outside the workshop and the place of invention. Without a new usage context, technology is less likely to successfully diffuse. Weyer gives the example of satellites, which were developed and stabilized in the context of NASA and the military but became adopted by the television industry which drove the mainstream adoption. The transmission of television was a new usage context (Weyer et al., 1997, p. 47). This opens up the possibility for the

creation of new norms as well. The key challenge is that the new artifact must fit to new contexts and users.

Social embeddedness is a key condition for an artifact's success. It means that the technology must be compatible with the demand of new impact constituencies, i.e. users. Another term could be resonance. This is a two-fold process: the technology must offer new usage scenarios that resonate with a target audience while at the same time being open for feedback and change based on the user's input. This means that technology must be open enough to "listen" to its users in the sense that its design cannot be too radical that potential users do not know how to use it. This is done by making technology simpler in use or by framing it in terms of older but familiar technology.[21] However, it is often the case that society adapts to a technology and not vice versa (Weyer et al., 1997, pp. 50-52).

If a technology diffuses successfully it has the chance to become a dominant design or a quasi-standard. If this is the case, a technology becomes a template for other artifacts that begin to mimic its functionality, look and feel (isomorphism). How this occurs is hard to predict by theory. A whole field of innovation studies deals with this question which cannot be answered in this thesis (Fagerberg, Mowery, & Nelson, 2006).

What can be stated is that when technology is used in the real world, different unforeseen things can happen because of *deviant or unintended use*, which can be the source of new innovation. The wider the audience, the more possible usage scenarios emerge and the higher the chance for usage variation and deviant use – a criminal will use a smartphone for his purposes and an academic will use it to enhance his research. This means that *deviant usage scenarios* produce new external effects such as threats that emerge when a large variety of users engages with a product. It can be hypothesized that the more negatively the impact of a technology is perceived, the more likely a political reaction becomes. The threat of cyber-crime only became possible because the usage practices of the average user produce systemic insecurities of computer systems (see chap. 4.4.1 Background: Growing Awareness of Computer Insecurity (1967 - 2011)). This will bring new players like security experts, the police and the military to the discourse. These new actors will try to alter the course of the technology according to their paradigms and working logics. Different new advocacy groups like different political parties, economic actors or security actors such as the military are likely to influence the course of development. Politicians will adopt new laws aiming to steer or to regulate the development of this new technology, shaping the social impact it might have. Therefore,

[21] The term "horsepower" for example frames the capability of a motor car in reference to the technology it replaced, i.e. horses.

we have to include the advocacy coalition framework and the influence of politics at this stage. I have already outlined how to conceptualize techno-political paradigms and policies.

2.3.6 Combining the Frameworks

Let's take a closer look at how the diffusion process adds politics and norms to an artifact and how these social dynamics between different actors during different stages works. I will incorporate ideas from Pfaffenberger, who dealt with the normative implications of technology from an anthropological perspective (Pfaffenberger, 1992a). The advantage of this theory is that it incorporates the usage dimension of technology as well as the role norms and discourse play therein. Also, he shares many premises outlined so far, for example that designers, either intentionally or unintentionally, embed norms in their artifacts (Pfaffenberger, 1992a, p. 283). Construction for him is both technical and social. It is not just a technical process but also a discursive one, since these technical features are discursively legitimized. He gives the example of Ford's assembly line which:

> "[…] was not only a novel and efficient method of assembling automobiles; by taking control away from the worker and centralizing it in management's hands, it also protected American society from the potentially chaotic and disruptive work force of Southern and Eastern European immigrants by forcing them to accept a work life of regimented, disciplined docility" (Pfaffenberger, 1992a, p. 283).

He calls this interaction of the technical and the social a "technological drama […] a discourse of technological "statements" and "counterstatements" (Pfaffenberger, 1992a, p. 283). This is not a strait linear process but includes three different steps of acts: technological regularization, technological adjustment, and technological re-constitution.

Technological *regularization* refers to the design process. During the goal-oriented construction a *design constituency* (the designer or a group of them) "creates, appropriates, or modifies a technological production process, artifact, user activity, or system in such a way that some of its technical features embody a political aim that is, an intention to alter the allocation of power, prestige, or wealth in a social formation" (Pfaffenberger, 1992a, p. 285). In other words, technical construction is a *bi-directional process* in which both norms and the design alter each other. This socio-technical construction creates subject identities, the social-configuration, vis-à-vis the object (the user, the administrator, the dandy etc.) who have different possibilities of influence. It constructs the appropriate usage modalities of different actors, for example their degree of autonomy. Pfaffenberger

theorizes a list of different strategies for regularization of which I can name only a few (Pfaffenberger, 1992a, pp. 291-294).

For example *exclusion*, where access to the technology and its social context is denied to persons who are of a certain race, class, gender, or fit into certain achievement categories (women and the Penny-farthing). *Differential incorporation*, where technology is designed in a way that social categories, like stratification, are incorporated (for example the Volksempfänger radio). Similar is *polarization*, which means that a spin-off artifact is created to incorporate class, gender or other categories (think pink guns, marketed for women). *Segregation*, where access to an artifact is restricted, for example with a pay-wall so that poorer users cannot afford all functions and *centralization*, where user autonomy is limited by some central administrator or access to artifacts is centralized (like the early mainframe computers at universities, see chap. 4.2.1 Background: the practice of computing in the 1950s). *Marginalization* is a technique where persons of a subordinate class get inferior versions of an artifact to reinforce status distinctions. In slave societies, servants often were not allowed to have cushions on their chairs (Pfaffenberger, 1992b, p. 503). With *delegation*, a technical feature of an artifact is deliberately designed to make up for presumed moral deficiencies in its users and is actively projected into the social contexts of use (Pfaffenberger, 1992a, pp. 291-294). Delegators are technical features that enforce norm compliance and appropriate behavior. The engine of modern cars often does not start if the seatbelt is not buckled-in.

Pfaffenberger argues that the technological design is not enough to create normative or power effects, but that these technical features must be "discursively regulated by surrounding it with symbolic media that mystify and therefore constitute the political aims […] the function of which is to regulate social behavior so that the artifact's political intentions come to life" (Pfaffenberger, 1992a, p. 294). In other words, there must be a discourse or a narrative that legitimizes why these delegators are in place and this is what creates the politics of artifacts. Here, Pfaffenberger comes close to discourse theory (see chap. 2.2.1 Discursive Struggles between Paradigms). The power-relationship between those actors and technology is established by what Laclau and Mouffe would call a hegemonic technology discourse, which excludes alternative meanings and exercises a certain type of discursive power. Such a technology discourse establishes a dominant way of understanding artifacts. The social side of artifacts, including their norms of appropriate use, must be activated, our acted out in discourse. The idea is that social context enacts the *power potential of technology* is an anti-essentialist statement – the power essence is not in the artifact, but results of the interplay of artifact and social context. Norms or power

intentions might be embedded in artifacts, but they only exist as power potentials and as such belong to the field of discursivity and are a matter of interpretative flexibility. The intention of the designer might have been discrimination, but if this discrimination is actually perceived by *impact constituencies* (the actual users of technology), is a matter of context and discourse.

The second phase of the technological drama is called *technological adjustment* which represents compensating strategies by the impact constituencies that use a technology (after or during market diffusion). Adjustment aims at making the implications of regularization either bearable or to get rid of them. Pfaffenberger theorizes three variants of adjustment: counter-signification, counter-appropriation and counter-delegation. All these can be seen as counter-articulations, directed at altering the hegemonic paradigm to different degrees.

Counter signification can be seen as a normal mode of discursive struggle about establishing a different meaning. "Counter signification decomposes and rehistoricizes the meanings embodied in artifact" (Pfaffenberger, 1992a, p. 300). Basically it is substituting one discourse for another by establishing a different fixation of meanings. One strategy can be to undermine moral authority of an artifact, which resembles the idea of injustice frames from frame-research (see chap. 2.2.2 Framing). Other strategies can include framing, highlighting contradictions and ambiguities within the hegemonic frame of the designers. The aim is to unmask the power relations. Pfaffenberger calls these little acts of subversion *counterstatements* and they aim to alter the social context that regularization creates (Pfaffenberger, 1992a, p. 285). Generally speaking they try to contest the hegemonic discourse (like the efficiency of Ford's assembly lines) with counter evidence and reframing (inhuman work conditions). As a result of such strategies, a new technical frame can emerge, which leads to new problem definitions and solution possibilities. Counter statements articulate different ideas and normative ideas and bring them together in networks of meaning. Therefore, counter signification often is the first step in the establishment of *counter-paradigms* which reinterpret how technology should be used and what it means. If social organization is successful, a user network adhering to a certain paradigm can be the result. Other strategies could include gaining access to the artifact or system from which they have been excluded and thereby trying to reshape it. Counter signification stays at the level of text and discourse.

Counter appropriation often includes socio-spatial strategies to gain access to a technology which is prevented by exclusion strategies. The strategy "involves a reinterpretation of the dominant discourse in such a way that their access to the technology

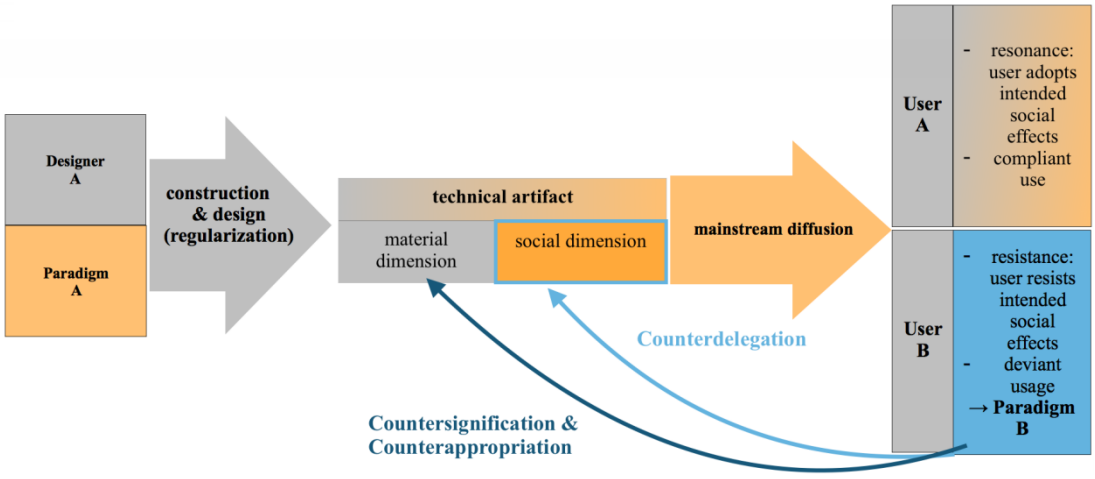
is morally legitimated. It may also involve attempts to acquire and to operate the artifacts" (Pfaffenberger, 1992a, p. 302). The 1830s "Swing Riots" and acts of political sabotage could represent hostile attempts of counter appropriaton.[22]

Counter delegation is particularly interesting for this dissertation because it happens on the material dimension; it changes the technical design of an artifact to alter regularization strategies. It includes tricking the aforementioned delegator techniques. In the digital world, hacking, understood in its original sense as someone who opens up technology to see and learn how it works, resembles counter delegation. (see chap. 4.2.1 Background: Hacker-ethic and Technical Optimism (1960s)).

Regularization effects normally require some time to become visible. Adjustment happens when dissatisfaction with a technological artifact occurs, for example if it does not work how it should or if its malfunction is so severe that it has a social impact (like accidents). Therefore, adjustment strategies require problem recognition by impact constituencies, i.e. the users of a technology. The framing literature has shown that problem recognition depends on the severeness of the problem (see chap. 2.2.2 Framing). As such, we can discern two possible outcomes of market-diffusion (see following figure): either users do not perceive a negative impact from regularization and as such they follow the usage modalities and intentions that have been laid out in the design. In that case they act according to the inventor's logic (they enact the paradigm, depicted in orange) and in this case, nothing happens. The alternative case is more interesting because it can lead to technological change. Counter articulations are put forward by *impact constituencies*, i.e. *deviant users* of a technology who resist the regularization embedded in artifacts for various reasons. Here, the social side and actor perspective becomes central again. It is not just the designer that has visions about how a technology should be used and what its functions should be. Users have something to say, too.

[22] Pfaffenberger offers the example of women in aviation. The dominant paradigm during the early days of aviation was male-dominated. It was only appropriate for men to fly and the pilot identity was constructed as some kind of noble daredevil or "aces" with a certain moral code including bravery and chivalry. This is because early pilots often came from the nobility (think Baron von Richthofen). When women like Amelia Earhart started to challenge this, they reframed the discourse of high-risk aviation to something that is safe enough that women can do it (Pfaffenberger, 1992a, p. 302).

Figure 10. Technical Adjustment Process (own diagram)



The figure shows the impact of a technology on its users. If users simply adopt the artifacts as intended by the designers, they often adapt to the preferred meaning (indicated in orange). In other words, the norms and ideas embedded in the artifact potentially resonate with the user. The user affirms, internalizes and potentially reifies these norms. If this is the case, norm diffusion through technology can be successful.

If a design does not fit the expectations of those who use it (because it is badly executed) then they will resist the regularization (indicated blue). Thus, *deviant users* become a relevant category for analysis. Sometimes they feel patronized by technology, sometimes they think they can execute functions better than the artifact lets them or they simply have a certain experimental attitude towards technology. More so, often impact constituencies of course hold their own paradigms and expectations and there can be incompatibilities with the hegemonic one. Alternatively, the impact of regularization can lead to the establishment of a whole new paradigm that is a reaction towards the hegemonic one, a counter discourse which can result in a social-movement.

Adjustment is a feedback mechanism that aims at reconstituting the technical artifact, but primarily its social side (its form or signifiers) and not primarily its technological design (although this is possible). Counter articulations that aim at the technological side are called *technological reconstitution*:

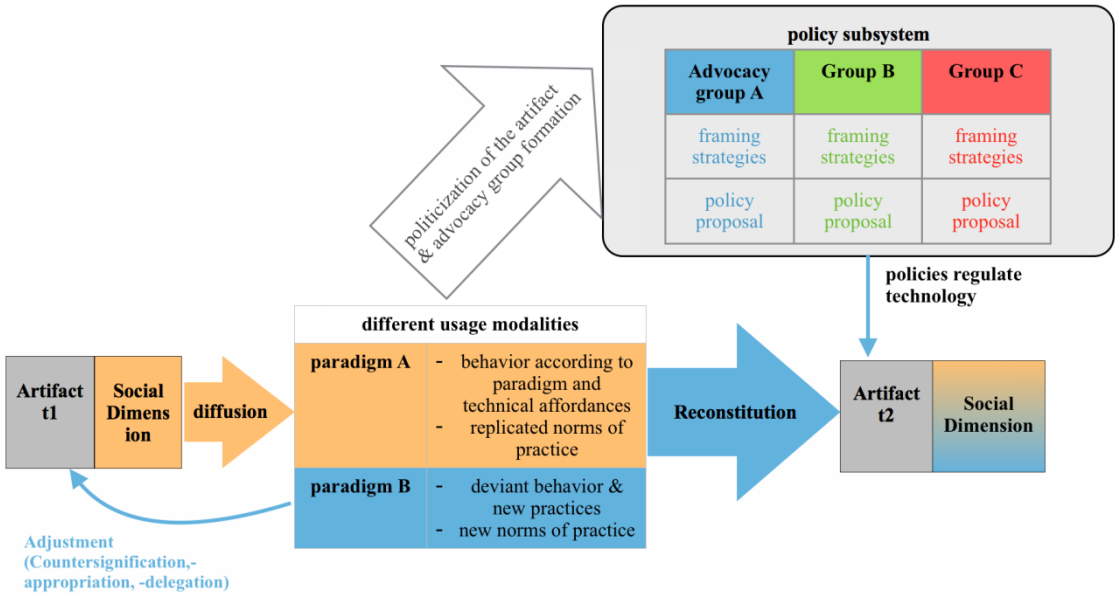
> "In technological reconstitution, impact constituencies actively reshape technological production processes or artifacts guided by a self-consciously "revolutionary" ideology, producing what I call counter artifacts. This ideology is produced by means of a symbolic inversion called antisignification" (Pfaffenberger, 1992a, p. 304).

It resembles the category of the other that challenges the design-paradigm, which is at the same time the very reason why the counter paradigm exists. Several elements come together here.

Loose networks of deviant users come together to form advocacy coalitions and engage in a variety of technological changes. One can be the *establishment of counter-contexts* of artifact use. As we have seen, designers intend a usage context but it happens that a device becomes placed into a new context. Another can be the creation of *counter-artifacts* or the severe modification of dominant designs. Here the technological cycle begins from the start. A counter-artifact is a new instance of goal oriented construction. The counter artifact's design compensates the regularization effects from the previous one. This is the very idea of technological development. Counter-artifacts and counter-contexts also tend to produce new actor categories and subject identities which form in relation to context and artifact. More so, new actors in different contexts are also the fertile ground for the development of new ideas, norms and even paradigms. This in turn influences the discourse, which also evolves. With new artifacts, new regularization strategies and the reshaping of discourse begin. The new artifact, if it succeeds, has opportunities to become hegemonic itself. This is the very instance of a change of dominant technological paradigms and, at the same time, a change of the dominant design. Paradigm change produces change in technology, which is the very core argument of this dissertation.

The following figure shows that with the impact of an artifact on the market (mainstream diffusion), new usage modalities begin to emerge. There are those who follow the logic of the inventor's paradigm (orange) and those who do not (blue). Deviant users are important, because they engage in contestation practices in terms of discursive adjustment, but also in terms of re-constitution, the creation of counter-artifacts (artifact 2). These counter-artifacts include the perceived problems the group has with the dominant artifacts and thus resembles their norms and values. Pfaffenberger reminds us that the reconstitution of an artifact itself is a new form of regularization. Not only is a new technology constructed, but also new usage visions and power potentials get implemented in the new technical design, which are inspired by the new paradigm. A new usage context and new subject positions are constructed at the same time. Also, political values, norms and technology co-shape during this reconstruction.

Figure 11. Technical & Political Reconstitution (own diagram)



At the same time, the reconstituted artifact often includes elements of the old one as well (indicated by the orange/blue color transition). The same steps of the goal-orientation process and paradigm formation can be seen here. If all goes well, the new artifact can reach mainstream diffusion and can itself have an impact on its users. This creates a forking development from the original paradigm, an alternative development path for a technology.

In the figure, I have also included the findings from the previous chapters (see chap. 2.2.1 Policy Paradigms). If an artifact reaches mainstream diffusion, often political actors begin to engage with a technology as well. The struggle between different technical communities often gets politicized, too, especially when an artifact has political impacts or if policies try to regulate the technology market. This means that there can be a correspondence between technical paradigms and political paradigms, or even an entire assimilation, for example when technical developers or companies engage in the political process, like forming technical advocacy groups or when technology companies begin lobbying efforts. So during mainstream diffusion, it is not just designers and users who engage in the meaning adjustment and technical reconstitution, but also politicians and political advocacy coalitions. Policy thus could be a fourth way to change the course of a technology. This will become clearer with software code and law.

2.3.7 Digital Technology: Software and Code

The aim of this chapter is to add the *digital component,* which is the very basis for understanding normative change of the object of study: the Internet. It offers, for now, a basic introduction to what the Internet is. A more detailed description will follow in the

case study (see chap. 4.1 Engineering the Internet). For now it is sufficient to understand the Internet technology as a multilayered entity consisting of material and digital or software elements.

Digital technology transcends dichotomy of matter and form and overcomes many of the limitations of the material artifacts. Software can be copied and cloned without quality loss. It can be distributed quickly, constantly changes its form and can get new possibilities with updates. Furthermore, all these theoretical elements I have discussed so far culminate in software, as this chapter will make clear. Software programming is also the best example for why we can treat technical artifacts as texts. Software code is *written* in a programming language that has its own grammar and syntax. Software is basically text that does something (act) and what it does is determined by the code. In computer science, *code* is generally understood as a set of instructions or commands that can be executed by a computer and that is written by a programmer in a programming language (such as Java, C or C++). Code tells the computer what it should do and how it should use its available resources in order to produce a result. The result of code can be manifold, but we see the outcomes on our computer screens, from operating systems to programs, video-games, software for managing electricity grids, finance or even cyber-attacks. Code limits the range of possibilities for human interaction with a digital technology and pre-structures agency. The Internet itself is built on a series of different code elements which govern how information (for example E-mails) is handled and transmitted around the globe with the help of physical hardware such as routers and fiber optic cables. In sum, code delimits the range of possibilities of what humans can do with computers and as such it has various degrees of power over us, directly and indirectly. This is relevant because code is written, or man-made by other humans and as such it is never neutral.

Lawrence Lessig was one among the first scholars who theorized about the relevance of code. In his influential book "Code: And Other Laws of Cyberspace" he argues that:

> "Code codifies values, and yet, oddly, most people speak as if code were just a question of engineering. Or as if code is best left to the market. Or best left unaddressed by government" (Lessig, 2006, p. 79).

Code is an invisible hand governing the workings of computers and cyberspace, which is a man-made system of interconnected computers. The arrangements of codes, sometimes called *architecture*, define how something works and what can be done with it. For Lessig, "code is a regulator in cyberspace because it defines the terms upon which cyberspace is offered" and that the people who live on the Internet are subject to that regulation (Lessig,

2006, p. 84). But it is not just about regulation but also about values and norms, which are developed and implemented (and in fact written) in code.[23]

Lessig gives two (historical) examples of competing software architectures for networking that represent and enact completely different paradigms and norms through programming code. The *Chicago Model* is a *network architecture* that does not have any entry barriers in order to connect. You simply login and you are connected to the worldwide Internet. No password or registration is required. Access is free and communication within the network anonymous (that means no data is stored about a computer's web surfing history), because it was decided to be this way by the administrators of the network. Lessig argues that the Chicago network architecture intentionally reflected the norms of the first amendment and that of a liberal policy paradigm. The architecture allows anonymity and freedom of information because of an intentional a policy decision of the universities dean (Lessig, 2006, p. 33). Paradigm-inspired network policies shaped network architecture and the norms of usage. The free and open Chicago model, with its respect for the first amendment, was the norm of Internet networking during the early 1990s, when this technology began to spread worldwide. It was the default setting how to run a network.

On the other end of the spectrum is the network architecture of Harvard university:

> "At Harvard, the rules are different. If you plug your machine into an Ethernet jack at the Harvard Law School, you will not gain access to the Net. You cannot connect your machine to the Net at Harvard unless the machine is registered—licensed, approved, verified. Only members of the university community can register their machines. Once registered, all interactions with the network are monitored and identified to a particular machine. To join the network, users have to "sign" a user agreement. The agreement acknowledges this pervasive practice of monitoring. Anonymous speech on this network is not permitted—it is against the rules. Access can be controlled based on who you are, and interactions can be traced based on what you did" (Lessig, 2006, p. 34).

[23] There is *open code* (open source) where everyone can access it and read and change it, and there is closed code (proprietary) which is not accessible. Open code is one of the powerful ideas of the open-source movement with its General Public License which guarantees users of software "the freedoms to use, study, share (copy), and modify the software" (Stallman, 1985). One benefit is that hidden power structures, for example malware embedded in programs or secret key-loggers that monitor and save everything that is typed on a keyboard, becomes visible if we can look at the code realizing these features. This also means that this limits the risk of backdoors in software, where a third party (say Russian hackers or the NSA) could gain access. As a result, open code supports the idea of democratization of government: everyone can access and read it and therefore can check whether control, espionage or surveillance is built into a software. Winner would say, and many open-source advocates would agree that open source is democratic software whereas *closed source* is, at least in tendency, authoritarian because one company (or the state) controls what the software does.

Hierarchical control, observation and other panoptic elements (Foucault, 1979) are parts of the core design principles of how the Harvard network architecture works. It makes human behavior within the network highly controllable and regulable, often without their knowing. Code can exercise various types of power over the users because it forces them to do something they would not have to do in the Chicago model. If you refuse, you cannot continue the login-process and therefore cannot use the service. Thus, code can represent a regularization or exclusion strategy.

Code regulates or controls both access to a system but also its usage or operative dimension. This is particularly interesting because usage and practice also create norms. If a meaningful behavior is repeated over time by enough people, it can become a standard of appropriate behavior. Code clearly can realize politics in Winner's terms (Winner, 1980). For example, network architectures can install Firewall-software on the router-hardware that prohibits access to certain websites and thus acts as a delegator. Political or social censorship can be an intentional design feature of a network architecture, as the Chinese Internet architecture shows (MacKinnon, 2009). Users will get used to this and develop new norms, for example new types of type-language (Emoji) as a counterappropriation strategy to bypass censorship, which can be observed in China.

Code can *discriminate* against users, for example by increasing the connection speed for those who pay a premium fee or by limiting speed for those who don't pay (segregation). Political, social or economical inequality can be intentionally built into network architecture. In order to do that, the network must be able to determine who someone is on a network, what he/she is doing and from where he/she is doing this (Lessig, 2006, pp. 45-54). The Chicago model does not provide this information, whereas the Harvard model does. Thus, it reflects a completely different set of *norms* and its design supports certain political paradigms of surveillance and control. From a libertarian paradigm, the features of the Chicago model like the lack of identification of users and the lack of content control are standards of appropriateness, but from a law-enforcement perspective this is dangerous. Because of the lack of control, everybody could do everything on the Chicago net, from watching pornography, gambling to recruiting radical Islamists for terrorist attacks. Banning certain types of information on the network with the help of firewalls like in the Harvard Model is more attractive to law-enforcement, intelligence agencies or even companies who earn money with gathered user-data from the network. What these examples tell us is that power, control and norms in cyberspace is a matter of network architecture design. This leads Lessig to the idea that code and its

architecture is a kind of law (Lessig, 2006, p. 77), because how something is build and the logic it is based on determine what can be done with it.

Software code is not only man-made but also highly changeable and amendable. Lessig adopts a hybrid position between technological determinism and social determinism that is highly compatible with the theoretical framework explained in this dissertation. Digital technology can be political because it can reflect political values (control vs. libertarianism) in its architectural design. This architecture can exercise power over humans because it acts as a constraining structure for behavior. But Lessig adds another important insight: if code is law, than control of code is power.

> "How the code regulates, who the code writers are, and who controls the code writers—these are questions on which any practice of justice must focus in the age of cyberspace. The answers reveal how cyberspace is regulated. My claim in this part of the book is that cyberspace is regulated by its code, and that the code is changing. Its regulation is its code, and its code is changing" (Lessig, 2006, p. 79).

Exercising *control over the code* and the programming of the code becomes a means of power in the digital age. Programmers, as the main inventors and engineers of digital technology deserve special attention in this regard because "code writers enact—the instructions imbedded in the software and hardware that make cyberspace work (Lessig, 2006, p. 72). They can reshape the programming code in order to reflect a different set of norms and values, which in turn will affect how this software works and can be used. A current example is the encryption debate that I have analyzed elsewhere (Schulze, 2017). In 2014, smartphone manufacturer Applemactivated (with a code update) the device encryption of its 1 billion iPhones currently in use. With a flick of a switch advocated for a norm that devices should be encrypted to prevent illegal third party access from hackers, but also from law-enforcement.

This examples show the magnitude of code change and the importance to closely watch the change of code on platforms and services that have a huge public reach. One change of code can make a difference between most fundamental values. Lessig therefore argues that *regulating code* itself becomes a political issue in the 21st century. Politics and policies can influence code design for example with laws, demanding certain standards or government access (Moore & Rid, 2016). Governments can force companies, by legal means, to implement certain code and design decisions, for example by planting so-called "*backdoors"*, intentional security vulnerabilities into a system to allow law-enforcement access. The militarization of cyberspace thesis translates into a national-security driven policy that is shaping code (Deibert, 2003).

2.3.8 Summary

In this chapter it was argued that technology can be analyzed with the same tools as norms because technology is part of the social world. IR-scholarship only offered a limited, biased perspective. I differentiated two perspectives on how technology is treated by IR and the social sciences, called technological determinism (with both optimistic and pessimistic flavors) and social determinism. I argued that we need the logical aspects of both branches and combine them in an approach that came to be known as the study of socio-technical systems, which analyzes technological artifacts within their social structure. This perspective also resolved the politics of technology debate ignited by Winner in 1980. Technology has not one essence that can be discovered, but rather what technology means (interpretative flexibility), how it is used and if it produces a power-effect is a matter of social context. Therefore, it is necessary to perceive technology similar to texts that can be read and studied. This SCOT perspective is compatible with the rest of my analytical framework presented so far and allows for bridge-building between the disciplines. The essence of this line of thought is that what technology is and how it is constructed is defined by the technological frames which constitute the object. Every technical artifact has two sides – its material dimension and its social side, which is not fixed, but a matter of discourse. The same technology can mean a variety of things depending on the social structure it is embedded in. SCOT analyzes not only the physical construction of the object but also the social construction of the meaning. The mechanism is similar to what I said about discursive power in the first theoretical chapter.

But there is more, as critiques of SCOT point out. The risk of SCOT is social overdetermination, which must be avoided. The material shape of an object matters and it is not true that "anything goes", as relativist research logic might suggest. Not all artifacts can get every meaning. Therefore, it is important to look at the outer corners of the realm of social construction and reconsider the physical object. For that, the concepts of design and affordances were introduced. These limit the range of probable interpretations and thus interpretative flexibility. Technological design often is a very intentional process and the designer actively chooses how an object is built, thereby actively limiting interpretative flexibility. The construction aspect matters and must be considered during analysis. Another reason for the importance of initial design is path dependency and the co-shaping of social structure – once established, a technology cannot be abandoned and exercise social power. I take the critique of the SCOT approach seriously and argue that a critical constructivist perspective that focuses on a technology's power relations is necessary. This

is because socio technological systems are built upon social norms and create them as well. One way to disentangle this interwoven relationship is to compartmentalize technological systems in two steps.

First, *goal oriented constructions* means that one should analyze the background of the design process and the designer at the initial stages of the construction process. The designer matters because his ideational paradigms shape the construction of the material object, his norms and ideas define what problem a device shall resolve, what intended usage functions it has and how it works. Power effects can be introduced at this stage, but whether they are realized depends on the usage context and its operative dimension. Second, the *operative dimension*, which often is neglected by SCOT. To compensate this deficiency, I included Pfaffenberger's framework that explicitly deals with normative and power-effects technologies can have. Power is pursued via technological means, it must be acted out in social contexts. Power and norms embedded in technology leave a discursive trail of framing strategies that legitimize regularization processes such as exclusion, compartmentalization and so forth. These must be studied as well. One key element of the technical drama discourse is that the fixation of meaning of technology is not a linear process but also has to face resistance, as most discursive power relations. What a user does with a technological artifact is very important because resistance and deviation tactics can be deployed in order to circumvent the power relations. Technological discourses are situations where power relations are exercised and they also alter the general structure of the technological system and its macro development over a longer period of time.

To grasp this long term evolution, the phase model of technological emergence based on the works of Weyer was introduced (Weyer et al., 1997). This model maps the diffusion of a technological system in different development steps. Within each step, socio-technical drama discourses happen at the micro level and conclude with temporary closure moments, when both a technical design and a social meaning of that designed are fixed or locked-in. This closure serves as the fundament for the next development step and thereby combines elements of path dependency and social construction without falling into the trap of overdetermination. It also includes the possibilities of counter-artifacts creating forking-paths.

For this analysis, the construction and the mainstream diffusion stage are the most important. I argue that during the mainstream phase the different theoretical concepts I have outlined in this paper can be combined into one coherent framework for analysis. The mainstream diffusion includes the politicization of an artifact, which initiates the political struggle of advocacy coalitions that have been outlined before (see chap. 2.2 Paradigms

and Norm-Change). During the mainstream stage, political actors are likely to enter the stage of the drama and will aim to alter the course of the technology according to party or organizational logics. The military for example is likely to see potential in a technology if its physical affordances allow it to be used in warfare. Other actors like economic interests will also discover the new technology and will try to generate profit with it or create new markets, which in turn can alter the development. Policies are a way to influence technological design as well, which is often overlooked by STS. Lessig made the point that the governance of a technology shapes its usage modalities and it norms, by giving the example of different network architectures that incorporate surveillance or censorship. Regulating software code is a means of power in the 21st century because defines how users engage with the technology and what norms can develop.

3. Methodology & Research Design

To analyze the question why norms of Internet control, mass surveillance technology and offensive cyber-war capabilities spread, the study uses causal process-tracing (CPT), sometimes also called explaining-outcome process-tracing (Beach & Pedersen, 2012, p. 19). I follow the methodology as outlined by Blatter and Haverland (Blatter & Haverland, 2012) but will include elements of Beach and Pedersen (Beach & Pedersen, 2012) and Bennett and Checkel (Bennett & Checkel, 2014).[24]

Process-tracing is a type of *within-case inference* that is particularly suited to explain how an outcome (dominance of the norm of Internet control in policy discourse) came into being. Thus, it is a Y-centered perspective, explaining variance in the outcome. In my case this is a norm change from utopian to cyber-realist norms (in contrast to X-centered co-variational or comparative approaches). The aim is to gain a comprehensive understanding of the case and a minimal sufficient explanation of the outcome (Beach & Pedersen, 2012, p. 18). "Minimal sufficiency is defined as an explanation that accounts for an outcome, with no redundant part" (Beach & Pedersen, 2012, p. 63).

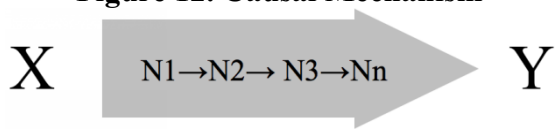
One of the epistemological assumptions of process-tracing is that of *configurational causality*, meaning that multiple factors work together to create an outcome. Many social phenomena have not one, but several causes (Ragin, 2008). The combination of factors leads to outcomes. Therefore, a wide array of theories can and should be used in CPT studies, which explains why I introduced a relatively wide set of potential causal factors in the previous chapter (see chap. 2. Explaining Normative Change). In contrast to co-variational approaches, the ambition is not to theory-test any individual theory or hypothesis, but to use the outlined causal factors in the theories heuristically as parts of the explanation in a causal mechanism (Beach & Pedersen, 2012, p. 13). This is in line with the goals of this work, which is to learn more about the case, i.e. the norm-change in the US and not that much about theory. Process-tracing is perfect for building bridges between different theoretical and disciplinary camps (IR, policy analysis, sociology, STS), but also between structure-centric or agency-oriented theories, which is one of the ambitions of this project (Bennett & Checkel, 2014, p. 23). CPT studies often do not set out clear hypotheses in the beginningy, but rather at the end of the empirical study. Theory and case-work is a much more iterative or abductive process, in contrast to more deductive co-variational case studies (Blatter, Janning, & Wagemann, 2007, p. 169). This is because of another assumption of CPT: the same outcome can be produced by different causal configurations

[24] I recognize Bennett's and Checkel's contribution, especially Jacbob's chapter on idea change (Jacobs, 2014), however the book came out with the majority of the research design already drafted.

(*equifinality*) and the effects of the same causal factors can be different in heterogeneous contexts. As such, any CPT-study must pay attention to potential, case-centric factors explaining an outcome inductively. It is unlikely that theory can predict every minute detail in a case and as such, inductive factors will matter in the empirical study that can be used for theory building (Blatter & Haverland, 2012, p. 81).

Additionally, an epistemological assumption is that *causality plays out in space and time*, sometimes even decades. CPT operates with a mechanistic understanding of causality. The central concept is that of a *causal mechanism: "*a set of interacting parts – an assembly of elements producing an effect not inherent in any one of them. A mechanism is not so much about 'nuts and bolts' as about 'cogs and wheels' – the wheelwork or agency by which an effect is produced" (Hernes, 1998).

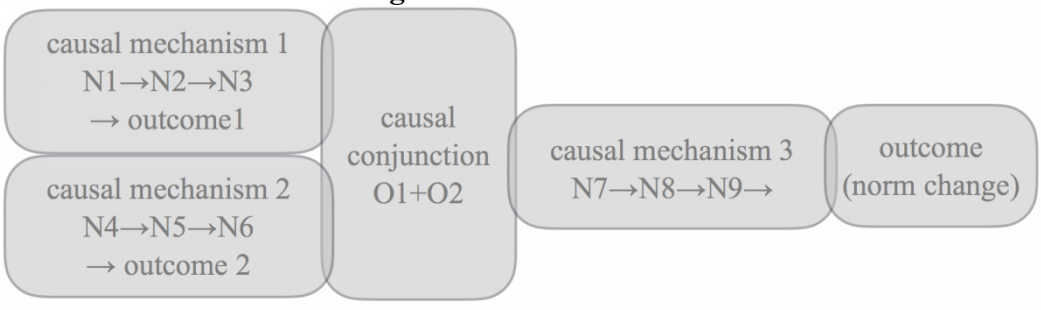
Figure 12. Causal Mechanism



A causal mechanism links the cause (X) with the outcome (Y). The cogs and wheels (Nn) transmit causal force often over longer time periods. Causal mechanisms can include material factors, such as technological change but also ideational ones like the transformation of ideas and norms that structure reality, which this thesis is about (Beach & Pedersen, 2012, p. 53). It includes the possibility to study large time-frames in a longitudinal fashion and thus is well-suited for the study of norm-emergence and diffusion. The notion of *path-dependency*, a causal factor initiated in the past producing effects in the future, is central to CPT (see chap. 2.2.4 Explaining Change). Path-dependency implies that either a specific temporal order of causal factors is crucial for an outcome Y, or causal conditions have to be present at a certain point in time to create an effect. These long time-frames make it necessary to divide the empirical section into different parts. A useful analogy is that of a *causal chain*: "in which specific causal conditions form the necessary and (usually together with other conditions) sufficient preconditions for triggering other necessary and sufficient causal conditions or configurations at a later point in time, and this causal chain leads at the end of the process to the outcome of interest" (Blatter & Haverland, 2012, p. 94).

A causal chain represents the combination of different causal mechanisms in a temporal sequence (N1-N3 and N4-N6) and create sequence outcomes (O1, O2) that can be combined at different junctures (equifinality), which then in term create a new causal mechanism, leading to other conjunctions until the outcome appears.

Figure 13. Causal chain



Thus, the above graphic presents the combination or fusion of different causal mechanisms into one long-term causal chain. Therefore, a few chapters will describe the long-term sequences (storylines) of macro-events leading to certain critical junctures or causal conjunctions, in which "multiple causal conditions work together […] at a specific point in time or over a short period of time to produce the outcome of interest" (Blatter & Haverland, 2012, p. 94). These junctures often lead to a change of the causal pathway. For example, in the graphic, two causal pathways are fused together in an additive fashion at causal conjunction. These junctures are then analyzed in more detail considering perceptions and motivations of actors.

It is important to note that these *junctures* can widely differ from each other, incorporating diverse causal factors, actors and contextual conditions (case-specific causal factors). Blatter and Haverland argue that causal factors can operate at different levels (macro or micro) and interact with each other (Blatter & Haverland, 2012, p. 97). In one juncture individual decisions might determine an outcome while in another structural constraints might be more important. This means that during each juncture, the analytical focus might change and therefore different types of evidence might be used. Therefore, the logical step is to zoom into these junctures and analyze the motivations and perceptions of actors (confessions), looking for smoking-gun evidence that confirms the existence of parts in the causal mechanism as outlined in the theory.

The analysis of causal factors does not resemble variable-scoring (or so-called data-set observations as in large-N and covariational studies), but tries to determine necessary and sufficient conditions of individual causal factors and the parts of the chain. Therefore, every element within the chain must be tested whether it is a necessary or sufficient form of causation.[25] The test includes the question whether Y would have occurred without X, thus i.e. applies counterfactual reasoning.

[25] In formal logic, sufficient conditions are those in which a causal factor X (rain) is a necessary condition for Y (wet street) to happen. If X (rain) happens, Y (wet street) occurs, every time. However, X must not be the only cause for Y which means that Y (wet street) can occur without X, for example by another cause Z (street

CPT has a drawback that needs to be discussed. The CPT approach does not strive to for statistical *generalization* as most quantitative studies understand it. Causal mechanisms that produce an outcome are most likely context dependent or case-specific, meaning that even if the same mechanism could be found in another country or case, the outcome effects might be different. That means that generalization of findings to a population of similar cases with similar outcomes is not possible in the strict sense. However, CPT can be used for possibilistic generalization, which means that the conditions producing an outcome might be generalizable (Blatter and Haverland 2012, 31f.). In other words, the causal mechanism in its totality might not be generalizable, but elements of the causal arguments might be further used for theory building. The value of CPT lies within theory generation and the development of a wide range of potential causal mechanisms that might be used, if adapted, in other cases. This generating of hypothesis will be done in the conclusion of the thesis (see chap. 5. Conclusion).

The next step is to introduce the research design and to address the questions, of how this process-tracing analysis proceeds exactly and what steps are taken to increase intersubjective verifiability. Process-tracing often does not represent a linear-research design. Instead, in process-tracing studies theory-screening and empirical work often is not separated but done in parallel. The researcher starts with theories that can potentially explain the outcome but also gains familiarity with the empirical case, which often reveals the need for further theorizing. This is sometimes called "soaking and soaking" (Bennett & Checkel, 2014, p. 18) and is what I have done in this thesis (see chap. 2. Explaining Normative Change). Out of this process I developed both the concrete research question and the case selection, which often are synthesized relatively late in the research process (compared to large-N studies).

After this conceptual work and case selection, I determined the *macro-developments and structural factors* of the process of norm emergence and diffusion, critical junctures and turning points where the path-development changed, as well as key actors and their motivations and their perceptions (Blatter & Haverland, 2012, p. 112). I did this first for the general history of the Internet, consulting historical documents and the written histories of other researchers (Abbate, 2000; Burman, 2003; Hafner & Lyon, 1998; Mosco, 2004; Naughton, 1999). I traced the origins of thinking about digital technologies to Norbert

---

cleaner). X is sufficient for Y, which is formally expressed as X→Y. Necessary conditions are those in which if X (the raven is black) is the case, then Y (the bird is a raven) is true as well. Y always occurs if X exists. Which means X (black) is a characteristic of Y (being a raven), but not the only characteristic, because other black birds must not be ravens. So the opposite must not be the case. This is expressed as Y→X which means Y is implied with X (or X is necessary for Y) (Gabriel, 2006).

Wiener in the late 1940s (see chap. 4.1.1 Background: Cybernetics). It was logical to start an analysis of different "cyber" paradigms with the invention of cybernetics.

Then I determined the important milestones and *junctures* of the Internet in line with the theory of technological developments. The Internet's construction period, and thus the first juncture, happened between 1966 and 1976 and the stabilization and early use took place during the 1980s. The mass diffusion started in 1992. The 1990s represented a primary focus point of analysis because of the mass diffusion of the technology, which created new issues and problems and thus points of interaction between the paradigms. This also marked the time when political and military actors became aware of the technology and when Internet paradigms formed. Another focus is on the mid 2000s, particularly because of the increased relevance of the technology in national security contexts with the war on terror. This is where the militarization of cyberspace gained headwind and accelerated. *The analysis ends in 2013*, because the Snowden leaks represented a major juncture the long-lasting impact of which is not yet completely clear, although much indicates a further strengthening of cyber-realism (Bennett & Checkel, 2014, pp. 26-27). Admittedly, many new important developments were triggered with the Snowden leaks that might be interesting to dive into more deeply, but time and space constraints are powerful arguments to end the analysis there. The reader might ask, why such a long time frame? I follow Jacobs (Jacobs, 2014, p. 57) and Legro (Legro, 2000, pp. 256-258) who convincingly argue that idea, norm and paradigm change happens slowly and thus can only be observed adequately over longer periods of time.

Since I utilize Manjikian's initial conception of cyber-narratives, including a cyber-utopian, a cyber-liberal and a cyber-realist reading, but add the engineering perspective, I had to analyze *not just one process, but four parallel ones*. The process of norm diffusion and the diffusion of the Internet consists of (at least) four different branches or sub processes that interact at different points in time. To increase coherence and to assess the independent causal effects of ideas or paradigms on different actors, it makes sense to switch levels or units of analysis (Jacobs, 2014, p. 63). The assumption is that different actors have different exposure to ideas of paradigms. If those who do not follow a paradigm repeat its ideas nevertheless, we can infer societal dominance from this very fact. The thesis will operate with the following *levels of analysis*: it focuses first on the designers and inventors of the Internet (micro), analyzes the impact with the early users and then shifts to the level of political *and* military decision-makers to assess the political impact of the technology and the different paradigms. To complement the picture, the public opinion and overall discourses is included. I will only focus partly on the

international dimension, because the main focus is on norm emergence and diffusion inside the US.

After having outlined the overall process in a large mind-map, I began *collecting source material* for each paradigm. Kuhn argued that paradigms are transported by textbooks, journals and educational material. Thus, the *primary data selection criterion* was whether a text talked about the Internet or related technologies from a distinct paradigmatic point of view. Another criterion was how important a document was, for example if it appeared often in the literature (snowball technique). Additionally, to make sense of the process and the motivations of actors, I included interviews, memoirs and statements such as speeches of the key actors and paradigm-carriers to get some insights on perceptions (Blatter & Haverland, 2012, p. 106). Because of the diverse nature of actors, the data sources are not standardized and include a vast array of sources from ethnographic research, statistics to pop-cultural references, which is common in process-tracing studies (Blatter & Haverland, 2012, p. 106). The following table summarizes the data sources:

Table 1. Paradigm Holders and Carrier Sources

	Engineering Paradigm	Cyber-Utopianism	Cyber-Liberalism	Cyber-Realism
Advocates	- engineers/developers - computer Science community - ARPA personnell	- early Internet users - hacker culture - netizens - libertarians & counter culture	- political elites - business actors	- military actors - intelligence community - military think tanks - law enforcement (FBI)
Data & Carrier Texts	- recorded oral histories of developers - interviews - science papers & reports explaining design - Internet archives - idea exchange between the actors (request for comments)	- manifestos of the net community - recorded oral histories of key actors - interviews - utopian public literature, novels, media publications - interviews - social media posts & messages	- political agendas - policies - recorded oral histories of key actors - interviews - political speeches	- military strategies & doctrines - national Security Strategies - briefing material, handbooks - policies - interviews
Secondary sources	- written histories - other scientific publications	- written histories - other scientific publications	- written histories - other scientific publications	- written histories - other scientific publications

A complete corpus of the carrier texts for each paradigm will be presented in the appendix (see chap. Corpora).

During the next step, *the data was analyzed qualitatively* using content analysis, identifying relevant problem definitions, solutions strategies, normative components, framing strategies (in line with the theory). To streamline the analysis of the paradigms, I drafted the following guiding questions that were applied to each paradigm and that structure the table of contents.

- What does the literature say about the dominant actors in each period?
  - Who are the paradigm holders?
  - How is the paradigm generating new followers?
  - Which of these are politically active and engage in norm entrepreneurship?
- What is the historical and social configuration, i.e. the structural background, of these actors that might determine their thinking?
  - Are there any social norms guiding the social interaction?
- What are the carrier media for the paradigm?
  - What documents reflect the thought process?
- What are the dominant elements of the paradigm?
  - What is the central problem, for those actors, what solution strategies do they develop?
  - How do they perceive the technology in question?
  - How do they frame it rhetorically?
  - What are the central norms of each paradigm?
  - How does the paradigm pre-structure the interaction with the artifact?
  - Are there any blind spots of the paradigm?
- What are these actors doing? What is the outcome of this process?
  - Is it a policy, a technological artifact or discourse?
  - What are the characteristics of those?
- What paradigm contents (ideas, norms) become embedded in the policies or artifacts?
- How do paradigms change over time?
- Does the paradigm exert political influence or any discursive power, shaping public discourse?
- What are trigger events or shocks (juncture) that alter the paradigm?

I analyzed each paradigm independently, starting with the engineering paradigm, continued with cyber-realism and finally analyzed cyber-utopianism/liberalism. *I screened the source material for answers to these questions*. The questions served as a coding-scheme which I used to analyze the key documents in a qualitative fashion (Miles & Huberman, 1994, p. 55). The analysis partly relied on MaxQDA, but also consisted of traditional note-taking and highlighting. By asking these questions to the texts, I inductively created categories, for example *ideas*, were all the ideas of a paradigm where collected and summarized. For example, cyber-realist documents repeatedly spoke of something like that "the Internet transcends state-borders", which creates border-protection issues. I coded it as "death of distance problem" (see chap. 4.4.2.2 Problem Definitions of Cyber-Realism). This allowed me to draft a comprehensive list of all the elements the paradigm consisted of: ideas, norms, policies, technical artifacts and the respective changes over time. This allowed me to summarize the paradigms and to assess their overall societal impact in terms of public discourse or policies. An overview of the findings is presented in the appendix (see chap. Paradigm Summaries).

In the next step, I *checked whether these paradigm ideas corresponded with the ideas of political administrations* of Bill Clinton, George W. Bush and Barack Obama. An important question is *how I determined the influence and reach of a paradigm*. This was done by simply accounting for the number of appearances of certain ideas. The more often ideas of a certain paradigm appear in documents of a political administration, the more influential the paradigm is. For example, early National Security Strategies of the US barely included cyber-realist ideas, which dramatically increased during the mid 1990s (see chap. 4.4.2 Ideas: Formation of the Information War Doctrine (1976-2000)). Theoretically it can be assumed that during the early stages of a paradigm, only a few ideas will appear in each document and the more these ideas develop, the more they will appear in the carrier texts or even will make it to the title of policy documents.

Other good indicators are political speeches and the number of actors utilizing ideas of a certain paradigm. A paradigm is more influential if a diverse set of actors, from academia to business to policy-makers utilize its ideas.

Especially media reception is a great indicator for assessing the societal impact of a paradigm. The assumption is that if ideas of a paradigm make front-news, they are widely influential. That is why I sometimes refer to influential media publications and front-pages of newspapers (see chap. 4.3.3 Ideas: Cyber-Utopia on the Information Superhighway (1993)). Another good indicator for the relevance of the paradigm are Google Ngrams (Google, 2016), i.e. how often certain key-words appear in scanned library documents. This showed the overall relevance of paradigmatic key-concepts in public literature. For the period after the year 2000, I also utilized Google Search Trends that count how often a search-term was searched for in Google (Google Trends, 2016).

The tricky part was to assess the dominance of one paradigm, especially when two were present within one administration. To grasp this, I describe these nuances as accurately as I can (see for example 4.4.4 Politics: Turn to Realism - Critical Infrastructure Initiative (1996-1999)). Finally, I base my judgement about the relevancy of certain topics and ideas on the judgement of other scientists who studied similar issues. Thus, I try to triangulate the relevance of certain ideas and norms by cross-checking it with secondary literature and polls.

The downside of this approach is that there is *no way to quantify the findings* (as I initially intended to). I cannot accurately determine to what degree a paradigm is important but can only provide ordinal measurements based on good judgement and the heuristic of idea-appearances. It is always a bit tricky to assess the dominance of certain ideas within a

political administration that releases thousands of documents each month on a wide array of topics. There is no way to study them all.

Another issue is that the quantity of texts is not always the best indicator for the importance of an issue, especially if the issue is highly classified, like cyber-security and cyber-war. Important documents are secret and intelligence agencies extensively use deception to shield their capacities from foreign agencies. As with any process-tracing case study, the potential risk is a "omitted sources" bias, i.e. that I missed an important part of the causal mechanism or that I overlooked other important sources. This risk can never be fully avoided, due to space and time constraints.[26] Data-triangulation with other studies that deal with the different parts of this analysis (for example the history of the Internet or the evolution of cyber-warfare) were used to present a a picture as complete as possible. Another risk was "selection bias" of sources that confirm the assumed causal mechanism while ignoring those which falsify it (Beach & Pedersen, 2012, p. 124). The way I tried to solve this was by testing whether identified parts in the causal mechanism were necessary for the outcome and to check for counterfactuals: would the same have happened with another administration? Admittedly, this is always somewhat interpretative.

There is also an issue with research designs studying ideas. The paradigm perspective only allows to see positives, i.e. ideas that fit to a paradigm whereas tracking negatives like "forgotten ideas" or "blind spots" is more tricky. That is one of the reasons why use four distinct paradigmatic perspectives because they partly reflect on each other's blind spot, providing some external critique.

The analysis will begin with the paradigm held by the ARPANET inventors during the late 1960s and also will introduce the basic design features of the Internet. Since the Internet is the technical artifact this thesis is about, and whose norms are changing, it makes sense to start with the construction and the characteristics of this artifact. This provides the fundament and basis for everything else.

[26] Bennett and Checkel argue that a causal mechanism can never be complete and will always be provisional because causality cannot be observed directly (Bennett & Checkel, 2014, pp. 11-12).

4. Case Study

Now let me introduce the logic of the individual chapters of the following empirical section. To be intelligible and comparable, most chapters feature similar elements. Each chapter starts with an entry quote, a motto that highlights a certain aspect of the chapter, often deriving from the very paradigm the chapter is about. The meaning and context of the quote will become clear throughout the chapter. Since I focus on different concepts, the *headings* of the subsections matter. That is the reason why most of the chapters have a similar *naming scheme*. The naming convention highlights different parts of the theory which serves as the ordering principle. Chapters labeled with "*juncture"* offer deep insights and thick analysis of turning points in the causal pathway, while chapters labeled with "*background*" present macro-structural developments and thus comprehensive storylines (see chap. 3. Methodology & Research Design). A clear-cut separation of "thick analysis" and "comprehensive storylines" was not always feasible, so that some chapters might include both. Chapters titled with "*ideas"* will trace the evolution of ideational concepts of each paradigm. I will focus on problem definitions, the perception of the Internet technologies in positive or negative terms, and the framing, i.e. the social construction of the technology. "*Norm"* chapters will do the same with norms. "*Blind spot*" chapters offer a discussion of things not anticipated by each paradigm, which often represent a point of contestation for other paradigms. "*Artifact*" and "*policy*" chapters are treated as the outcome of the ideational process in a time period. This is based on the theoretical assumption that ideas influence technologies and politics likewise. They manifest norms and ideas. These chapters show how norms and ideas became embedded in technology. Finally, at the end of each chapter, an in-depth, *critical analysis* of the paradigms' contents follow, discussing potential biases and blind spots. Each chapter is concluded with a short *summary* of the causal mechanism that was presented. These summaries are then used for the final analysis and the depiction of the causal mechanism in the conclusion.

4.1 Engineering the Internet

"We reject kings, presidents and voting. We believe in rough consensus and running code."
Motto of the Internet developers

This almost rebellious introduction quote can be seen as the informal motto of the creators of the Internet. How the Internet was created is the topic of this chapter. Today we experience the Internet as a seamless, unitary network and invention, but in reality, it is not one thing. The Internet is a meta-infrastructure, a network[27] that consists of interconnected networks. This network of networks has three dimensions: the *physical* layer of computers, routers, switches and transmission lines (copper & fiber-optic cables, wireless), a *digital* layer consisting of software code (called protocol) that regulates digital data-transmission over this hardware and an *application or content-layer,* which represents the things we can use the Internet for, like surfing, E-mails or mobile applications (Libicki, 2009, p. 12). All these layers and elements have been invented over time. As such, the Internet neither has a primary inventor nor has it precise point in time when it was invented. The Internet was a collegial effort among an international research community. It is an evolving artifact that is co-shaped by its users and its designers.

As such there are different origin stories or multiple histories (Peter, 2004). Internet historian John Naughton discerns two interrelated development phases. First, the prototype phase (1967-1972), where the Internet's predecessor called ARPA-Network (henceforth ARPANET) was built to interconnect mainframe computer systems within the context of the US Advanced Research Projects Agency (ARPA) (Naughton, 2016). This laid out the technological groundwork for the second phase between 1973-1983, which can be called the internetworking phase. It is important to analyze both artifacts because one led to another and the latter incorporated ideas from the former. There is no clear cut between the two because the Internet inherited many design features from the ARPANET. "You can mark the birth of the Internet back to the ARPAnet", as one of the inventors argues (Crocker, 2009). The final development phase was the global diffusion of the Internet with help of the World Wide Web, an application that made the Internet more visual and easier to use.

The purpose of this analysis is to trace the evolution of norms surrounding the socio-technical system Internet and its technical and philosophical predecessor called

[27] "A *computer network* is a set of *computers* communicating by common conventions called *protocols* over communication media. Computers in a network are called *network nodes*, and those that people use directly are called *hosts*. Computer network protocols usually involve the exchange of discrete units of information called *messages* over some form of physical *medium*, such as coaxial cable, microwaves, or a twisted pair of copper wires" (Quarterman, 1989, p. 6).

ARPANET. The goal is to identify the major paradigm that defined the goals and uses for technology and therefore shaped the initial construction of this technology. The theoretical argument is that paradigms include norms that become embedded in the material affordances of technological artifacts. The questions that guide this chapter are: *what core ideas and norms became embedded in the Internet architecture, what are its technical affordances and what norms developed with its construction and usage?*

To analyze these norms and ideas I will focus mostly on the hardware and software layer, because software protocols govern how data is exchanged and thus determine the technical affordances of this technology. The term protocol refers to "any type of correct or proper behavior within a specific system of conventions" (Galloway, 2006, p. 7). It is therefore quite similar to the definition of norms as standards of appropriate behaviors, but protocol is software code that organizes how computers (the hardware) interoperate for example, how they establish connections and exchange messages (Lessig, 2006, p. 5). It is a kind of common language for different technical artifacts that also influence social behavior: "Protocols govern how specific technologies are agreed to, adopted, implemented, and ultimately used by people around the world" (Galloway, 2006, p. 7). Protocols determine functionality, technical affordances and the practice of using this technology which then can lead to new social norms. This is also the reason why an analysis of protocols is key for determining norms within the technical artifacts ARPANET and its successor, the Internet (represented through its TCP/IP protocol).

Computer scientists would analyze protocols by looking at the programming syntax, the source code. As a political scientist, I will focus on the inventors and early users, scientists and engineers of the technology and their science and engineering paradigm that shaped the goal oriented construction of these protocols. They are key actors who used the technology and realized its potential. They were the first to establish the meaning of the networking technology and thereby influenced the early norms of using this system. In other words, the engineers initiated a particular causal path-trajectory that had future implications. To trace the ideas of inventors, I will mostly rely on historical primary sources such as official documentations and reports, the preserved research note-exchanges between the inventors and their oral histories. These sources are the carrier medium of the engineering perspective on the Internet. I will also use the rich written histories by secondary authors.

The analysis proceeds according to the technical diffusion model outlined in the theory. I begin with the goal-oriented construction of the ARPANET. I will deduce the ideas that led to the construction (see chap. 4.1.2.1 Ideas) and the norms embedded in the

system (see chap. 4.1.2.2 Norms Shaping the Construction of ARPANET) by looking at the central artifact, the Network Control Program (protocol). Then I look at the early user-reception of this technology and analyze how the users of the ARPANET changed its initial meaning and function (see chap. 4.1.2.4 Co-shaping the Meaning of Networks). The same structure is replicated for TCP/IP (see chap. 4.1.3 Constructing the Internet (1972-1991)), the central protocol that governs the Internet we use today (see chap. 4.1.3.1 Artifact: Internet Protocols and Norms). The core argument is that the Internet reflected academic ideas such as the free sharing of information, collaboration and a general skepticism towards central control structures. It was intentionally build to be global and without central control. Afterwards, I will deal with the conditions for the stabilization and the mainstream diffusion of the technology by answering the question of how TCP/IP could become a dominant technology. This has two parts: the software-dimension (see chap. 4.1.3.2 The Diffusion and Dominance of the Internet) and the hardware dimension, called the Internet backbone (see chap. 4.1.3.3 The Internet Backbone). Finally, I turn to the visual Internet or the World Wide Web, a key artifact that enabled non-IT-experts to use the Internet and thus was crucial for its worldwide success (see chap. 4.1.4 Artifact: The World Wide Web (1989-present)). After this more historical part I introduce blind spots, i.e. things the inventors did not anticipate, which ultimately created the cyber-security and cyber-war problems that we have today. As such, this chapter is the crucial link to the other paradigms (see chap. 4.1.5 Development Blind Spots). Before we jump into this discussion, we need to clarify some terminology that is often used, even in the title of this thesis, but seldom reflected upon: What is this thing called *cyber* anyway?

4.1.1 Background: Cybernetics

No analysis of cyberspace or modes of thought therein – paradigms – should start without mentioning Norbert Wiener (*1894–†1964). Wiener coined the term "Cybernetics" from which other concepts such as cyber-space, cyber-war etc. derive their name. Wiener developed the concept during World War 2 while working on the "anti-aircraft problem", the problem how to shoot down modern high-speed airplanes. This problem required on the one hand, complex mathematical calculations to predict the position of the plane, and on the other hand, a feedback mechanism that aligned the position of the gun accordingly, a process way too complex for a human to calculate. This problem led Wiener to formulate a theory of Cybernetics, "the science of control and communication in the animal and the machine" (Wiener, 1965).

According to Rid's excellent history, cybernetics has three main concepts. First, *control*. A system or organism that controls or steers its environment. That is what the prefix *cyber* means, deriving from the Greek word κυβερνήτης, meaning steering, navigation or governance. Second, *feedback* or learning which predicts future behavior. Finally, the fusion of the human and machine into a *system*. For Wiener, the anti-aircraft gun and the human operator were not distinct entities but one system. Other examples of cybernetic systems would be a prosthetic hand or the cockpit of a Jet, where pilot and Jet form a *symbiosis* (Rid, 2016, pp. 69-75). These ideas together formed a *"computational metaphor*" or the argument that humans and society could be the thought of information processors or machines. This was the foundation for the term *information society* (Turner, 2006, p. 22). This thought implied a vision of *automatization*: since humans, animals and computers were all systems operating according to cybernetic principles (control and feedback), the latter could take over human functions. The idea that machines will, some day, take over control was born in 1948 with Norbert Wiener (Rid, 2016, pp. 26-63).

Wiener's widely regarded 1948 book Cybernetics (Wiener, 1965) became a hype across the sciences until the late 1970s and even infused popular culture (see chap. 4.2.4 Artifact: The WELL and the Social Construction of Cyberspace (1980-1990)). The 1950s and 1960s saw an unprecedented growth of machines taking over human work, from microwave ovens to production robots. Wiener's systemic or holistic thinking was also the basis for Talcott Parsons' and Niklas Luhmann's system theory or the idea that technical systems could serve as models for society. According to Turner, the appeal of cybernetic thinking came from the fact that it connected various disciplines: computer-science, social sciences (psychology, sociology) but even aspects of American culture (Science Fiction) and counterculture of the late 1960s (see chap. 4.2.2 Ideas: Stewart Brand and the Counter-culture (1960-1970)). Cybernetics facilitated interdisciplinary collaboration and research and provided a coherent conceptual framework to connect various networks of social actors (Turner, 2006, p. 24). It can be argued that cybernetics was a meta-theory during the early 1950s-1970s.

Interestingly, in his later work, Wiener speculated about two potential outcomes of automatization: a dystopian vision of enslavement and suppression and a utopian one of human liberation and empowerment (Rid, 2016, pp. 26-63). The dystopian vision predicted that automatization would destroy jobs and lead to unemployment. Wiener feared that at one point, computers could begin to act on their own or worse, could be utilized by power-hungry politicians as a means of social control (Turner, 2006, p. 24). The utopian vision saw the potential to realize Marx' "utopian praise of un-alienated labor, of human

flourishing through creative and self-actualizing productions" (Beebe, 2010, p. 885). This dual vision of cybernetics explains why this chapter starts with Wiener. Here, both dystopian and utopian lines of thought had already been conceived and began to branch out with different advocacy groups. Wiener is also important because various actors involved in the social construction and framing of the Internet referred to his ideas. Cybernetics in that sense is the foundation both for *cyber*-realism and its technologies of control and surveillance, but also *cyber*-utopianism. One cyber-utopian, a man named J.C.R. Licklider, is regarded by many engineers as the spiritual father of the Internet idea. Licklider shaped the organizational structure at the Advanced Research Projects Agency, the place where the Internet was invented. This will be the topic of the next chapter.

4.1.2 The Social Construction of the ARPA-Network (1966-1972)

To study socio-technical systems such as the Internet, we should consider the context of invention first (see chap. 2.3.2 Defining Technology). This is the purpose of this chapter. The Internet developed within the context of the Advanced Research Projects Agency (ARPA, later renamed to Defense Advanced Research Agency or DARPA).[28] The context of invention is important because it enabled the creation of a costly, experimental networking system that was nonproprietary and thus open to use.

ARPA was founded as a reaction to the Sputnik Shock that revealed a so-called "science gap" (Taylor, 2008, p. 9). As a reaction, President Eisenhower dramatically increased federal research & development (R&D) spending (Congressional Budget Office, 2007) and founded ARPA in 1957 to catch up with the scientific and military development of the Soviet Union. Eisenhower gave ARPA a relative *broad mandate for basic research* focusing on "high-risk and high pay-off" technologies (Lukasik, 2011, p. 13) and a large military budget, especially compared to civilian research centers such as the National Science Foundation (NSF). In the early days, ARPA was the best of both worlds: it had a large budget and a relatively free-wheeling style of management, giving program managers and research directors a relatively free hand to pursue projects without much interference or oversight, as long as they produced results that had military appliances. One of these areas was computing, which particularly benefited from the mixture of a large budget and a free hand to experiment (Hafner & Lyon, 1998, p. 22).

ARPA established an Information Processing Techniques Office (IPTO) and began funding expensive computer research around the US with the aim of creating centers of

[28] The "defense" part was added and removed repeatedly during its history so I use ARPA and DARPA interchangeably throughout the thesis.

excellence or an "intergalactic network" of elite research, as the first IPTO director J.C.R. Licklider (1962-1964) called it (Taylor, 2008, pp. 10-11).[29] This was the first notion of something like a computer network. Licklider established a very *informal management style*: "IPTO managers maintained close personal contacts with their colleagues in the computer research community, providing an informal circle that was commonly known among computer researchers as the 'ARPA community'" (Roland & Shiman, 2002, p. 22). The "ARPA-style" continued with other directors. Stephen Lukasik (director of ARPA between 1970-1975) summarized: "what distinguished the agency from other parts of government was its freewheeling style, flexibility in management and contractual arrangements, enforcement of the highest level of excellence from its contractors, and openness to technical ideas from all directions" (Lukasik, 2011, p. 6).

One general problem of computing in that era was that mainframe computers[30] were custom-built for specific applications (like ballistics calculations or graphics) and thus *highly incompatible with each other*. Hardware and software differed dramatically. A program written for one machine would not work on another and if computer scientists wanted to use particular programs, they either had to rewrite the program themselves or jump in a plane and fly to a computer site where the program could be run (Abbate, 2000, p. 1). This was expensive, often resulted in duplicated research and thus was highly cost inefficient (Hafner & Lyon, 1998, p. 40f.). For Robert Taylor, a later program manager at IPTO between 1966 and 1969, who was tasked with supervising computing research, this computer incompatibility was a cumbersome and inefficient process. Taylor used three different terminal computers to manage the computer projects at three different sites that all required different command inputs:

> "There was one other trigger that turned me to the ARPAnet. For each of these three terminals, I had three different sets of user commands. I said, oh, man, it's obvious what to do: If you have these three terminals, there ought to be one terminal that goes anywhere you want to go where you have interactive computing. That idea is the ARPAnet" (Taylor, 1999).

[29] J.C.R. Licklider (*1915-†1990) is regarded by many ARPA engineers as the origin of the Internet idea. He had read Wiener's papers and can be regarded as an early cyber-utopian. In 1960, Licklider published an influential, cybernetic-inspired paper called "Man-Computer Symbiosis", a technological optimist and cybernetic manifesto of the future Licklider outlined a utopian vision that computers had the potential to act as an extension of the human brain, that they could amplify human intelligence and transform the way we think (Licklider, 1990).

[30] "Mainframes are a types of computers that generally are known for their large size, amount of storage, processing power and high level of reliability. They are primarily used by large organizations for mission-critical applications requiring high volumes of data processing" (Technopedia, 2016).

Out of his personal annoyance with this process, he developed the *goal of the system*: money and time could be saved if these different computer centers would be connected to each other. Researchers at computer site A should be able to log into the mainframe computer at site B and execute the program there remotely, from afar. Mainframe computer A would "host" the application for B, and thus these machines were called "host-computers". This idea of sharing resources between computer centers was the primary reason for the creation of ARPANET. In the long run, it was assumed that this would bring researchers closer together and would facilitate cooperative research projects over long distances (Heart et al., 1981, pp. II-2).

Because of ARPA's free-wheeling management style, Taylor had no difficulties to convince his supervisors to provide relatively large funds to launch an experimental network, as this following smoking gun episode shows:

> "I had no proposals for the ARPANET. I just decided that we were going to build a network that would connect these interactive communities into a larger community in such a way that a user of one community could connect to a distant community as though that user were on his local system. First I went to Herzfeld [ARPA director] and said, this is what I want to do, and why. That was literally a 15 minute conversation. And he said, "You've got it." He said, "How much money do you need to get off the ground?" I think I said a million dollars or so, just to get it organized. There was no ARPA order written or anything for months, maybe even a year later" (Taylor, 1999).

What makes this noteworthy is the fact that at this time it was not even clear that a computer network would actually work. The ARPANET program had the character of a feasibility experiment and was treated as such (Kleinrock, 1990). It can be doubted that this highly uncertain endeavor would have started without the generous funding and the basic research orientation at ARPA (sufficient condition).

What should have become clear by now is that the goals of ARPANET represented scientific goals of resource and information sharing between research centers that coincided with the goal of budget efficiency of a government agency. ARPA was a military research center, but the ARPANET was dominated by civilian actors and their ideas (Segeberg, 2004). In theoretical terms, Taylor was an impact constituency unsatisfied with the status quo in the practice of computing. He engaged in a technical reconfiguration campaign altering the dominant use of computing of the time (Pfaffenberger, 1992a). A unique factor with ARPANET is that the designers of the system designed it for themselves. This allowed a constant feedback loop, which was especially supported by ARPA's management style. This special development context had an important influence

on the shape and design of the system, because it enabled particular ideas. It initiated a special pathway: the network was designed by computer scientists for computer scientists. Economical (a business model, proprietary standards or patents) or security considerations (authenticating users on the system, encrypted communication) were not important (see chap. 4.1.5 Development Blind Spots). That ARPA funded this experimental network (where no one knew whether it would in fact work), is a key condition for its success and its open design (Kleinrock, 1990). What were the key ideas and norms that only could develop in the ARPA context?

Two elements are particularly noteworthy: first, the *ideas that became embedded in the Network Control Program* that regulated data-exchange within ARPANET and second, *how these ideas were conceived and realized in a social process among graduate students* that wrote this protocol. Both factors had path-dependent implications for the future and will now be analyzed in more detail.

4.1.2.1 Ideas

In 1966, Robert Taylor hired Lawrence ("Larry") Roberts to create a computer network to allow resource sharing between ARPA-funded mainframe computer centers (Abbate, 2000, p. 44) and the invention phase began (see chap. 2.3.5.1 Emergence/Construction).[31] Roberts had to design the system from scratch because "we didn't even know what computer networks were really […]" (Cerf, 1990). Roberts wanted the system to be as open as possible for all kinds of computer hardware, reliable, quick and sufficiently large (Hafner & Lyon, 1998, pp. 104-105).

Roberts turned to computer science colleagues at different universities to overcome a central challenge: since these incompatible mainframe computers spoke different languages, each individual machine had to be reprogrammed to understand the others. This was technologically not feasible. Instead, the problem was sidestepped by building a subnetwork of cheap, identical mini-computers called Interface Message Processors (IMP) that would communicate with each other (Naughton, 1999, p. 90). Thus, the mainframe computer at each site only had to communicate with their personal IMP, which then passed the message to an IMP at another site, which then translated the message for the mainframe computer there. For the hosts, the subnetwork was invisible. They thought to be directly in touch with the other machines (Roland & Shiman, 2002, p. 18). This basic subnetwork topology was so fundamental that it still exists today: our IMPs are modems and routers.

[31] A list of key Internet milestones and security incidents can be found in the appendix.

This subnetwork of incompatible host-computers and IMPs connected over traditional phone lines was conceptualized and built over the span of three years at four computer sites: The University of California at Santa Barbara, the Stanford Research Institute (SRI), the University of California at Berkeley and the University of Utah. The physical network hardware, the IMPs, were developed by Bolt, Beranek and Newman (BBN) after IBM and other prime manufactures turned down the ARPA contract, arguing that such a network would never be economically be feasible (Naughton, 1999, p. 131).

Figure 14. ARPANET Host-Computer and IMP Subnetwork, Source: (Heart et al., 1981, pp. III-2)

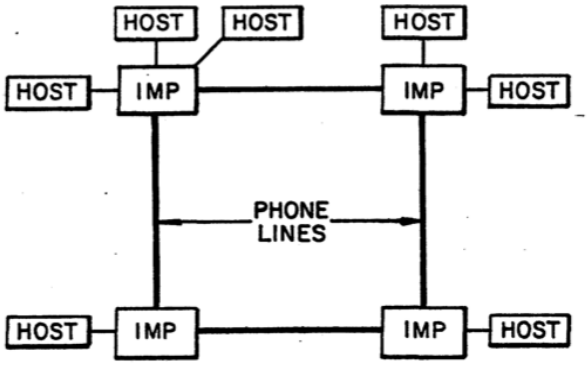


Figure 1 -- IMPs, Lines, and Hosts

The software protocol that managed the message transfer was written by graduate students at the four university sites.

For the software protocols, Roberts and his colleagues picked up theoretical ideas that had been floating in the computer science community of the time: a *distributed network topology, switching of digital packets and dynamic/adaptive routing of packets* (Kleinrock, 1961; Baran, 1964; Davies, 1965). The first idea was to use a *distributed network topology* or architecture. Roberts initially thought to create a centralized star network (Pelkey, 2014, p. chap. 2).

A post office that collects all letters that have been sent at a central location and then delivers these letters to their designation at the edges represents a star network. Roberts initial idea was that all host-computers would be connected to a central computer which would facilitate the networking functions and message exchange between all other machines (see figure).

Figure 15. Different Network Topologies outlined by Baran (Baran, 1964, p. 2)

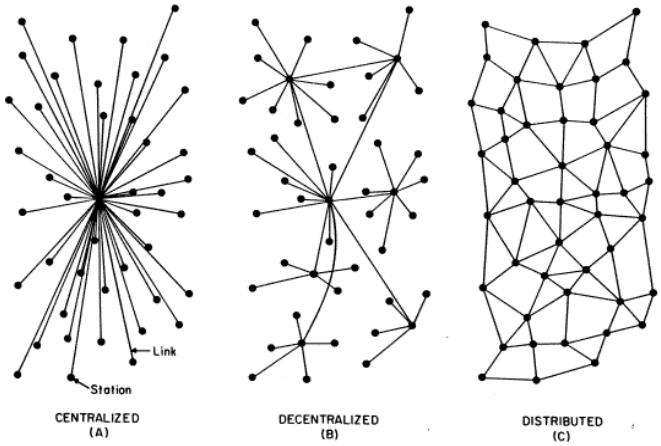


FIG. 1 — Centralized, Decentralized and Distributed Networks

This idea was met with resistance by his colleagues and particularly Robert Taylor who did not like the idea because:

> "[…] there was a strong element in the culture, in those days, mid 1960s that was reflected in me. I didn't trust large organizations. This is part of the movement of the 60s. I didn't trust large organizations. I didn't trust centralized control of anything. Small is beautiful" (Taylor, 2008, p. 44).

This episode was the first glimpse of something like a political idea or social norm influencing a design decision. Taylor essentially acted as a norm entrepreneur arguing that no single institution or organization shall be able to control the operation of the network. This was a reference to the emerging counter-culture of the 1960s (see chap. 4.2.2 Ideas: Stewart Brand and the Counter-culture (1960-1970)). The alternative would have been a decentralized system, like the phone network of the time, where a few, densely connected clusters would then be interconnected. Paul Baran worked on the same issue of network topology at RAND, but with a national security perspective. Dealing with the question of how communication could be maintained after a nuclear first strike, he argued that distributed networks would be most likely to survive.[32] The idea of a distributed network is

[32] The US-Air Force researched different solutions to the threat of a nuclear first-strike. "Survivable communications" was a buzz-word of that time. The problem Paul Baran was working on was how the US government could be able to launch a retaliatory strike if the telephone network, linking the White House with the army bases was disrupted or destroyed (the "command" aspect) and how to maintain control over its troops and authority after a first strike (control) (RAND, 1964). Creating decentralized or distributed command centers with redundant communication routes was the solution. Baran calculated that each node should at least have three other connections which provide a suitable level of redundancy in case of a nuclear attack (Baran, 1964). For RAND, a computer network served the purpose of national security and not

that each node has multiple redundant connections to its neighbors, so if one fails (or gets destroyed by a nuke), a reserve line exists. The US highway system represents a distributed network (Galloway, 2006, p. 35).

A highly decentralized or distributed system was chosen for ARPANET, but with this decision came a problem that was known from analog telephony. *Switching* is the process of establishing a phone connection between caller, (manual) operator and recipient. Analog audio signals degrade with each switch. The more switches between caller and recipient, the worse the audio quality gets. This could be witnessed with international phone calls back in the day (Hafner & Lyon, 1998, p. 57). The more distributed a network, the more switching was required and the worse the audio signal got.

Therefore, the ARPANET engineers had to use *digital data transmission*, a series of bits.[33] Digital communication was quicker, could be stored more easily and allowed for higher bandwidth (i.e. more transmissions over the same line at the same time). Whereas an analog line could carry only one phone call at the same time, several digital communications could be sent at the same time over the same cable. There was another catch. Digital communication does not flow in a constant stream of information, like analog audio, but happens in bursts. Large portions of data are sent at the same time followed by silence. Inactive lines were a waste of capacity. The problem of uneven data flow had been discovered before in the telegraphy system of the 1930s. During rush hours, more people than the line could handle wanted to send messages. The telegraphy solution to this problem was a technique called *store-and-forward switching* (Abbate, 2000, pp. 11-13). Messages were sent to the telegraphy offices (the nodes), were temporarily stored and forwarded when the lines were inactive (during night-time), which was a more economical use of available bandwidth.

This led to the idea to divide digital messages into smaller "message blocks" (Baran, 1964) or "*packets*" (Davies, 1965). The analogy would be that instead of sending an entire book in one shipment, the individual pages of the books would be glued to post cards (the packets) and then sent individually. The receiver would re-assemble the book out of the pos cards at the end-point of the transmission. This implied that the post cards would not all travel the same way. The network individually determined the path over which the packets would be sent with a routing-table. The nodes in the network would constantly

freedom of research and exchange of ideas. This more military perspective on networks shaped Baran's assumptions of how such a network should look like and operate (its protocols).

[33] A bit, or binary digit, is a unit in computing which can have two values: 1 (on) and 0 (off). Different combinations of 1s and 0s are transcoded into alphabetical letters. For example, the succession of the following 8 bits "01000001" represents the letter "A". A message block (packet) of 1024 bits therefore can store a message consisting of 128 alphabetical letters. Assuming that the average English sentence is 20 letters long, one packet carries the information of roughly 6 sentences.

check whether its neighbor nodes were active (feedback) and if not, would instead send packets in another direction (Naughton, 1999, p. 103). Thus, packets would be sent randomly over the network, depending on the free capacity of the distributed data lines, which means they travelled on a hard-to-predict path. This was called *adaptive or distributed routing.*

The sum of these ideas was called *packet-switching,* which is the core idea that both ARPANET and the later Internet share. This refers to Weyer's core invention that was described earlier (see chap. 2.3.5.1 Emergence/Construction). It means that the data flow in the network is not determined by one centralized watchtower, but by the individual nodes in the network. This network architecture allowed "to control the communication without centralizing it" (Taylor, 2008, p. 44). The network would govern itself and the end-points, i.e. the hosts, could not execute any control over the network. Thus, the control of the network was decentralized. This idea was "most critical" (Taylor, 2008, p. 57). A message sent over the network would exist only at the beginning and the end of the transmission. While in transit, it was chopped up in packets which travelled over random paths. Thus, a message could not easily be intercepted. This made traditional wiretapping and electronic surveillance more difficult. With digital transmission, it was not possible to plug into the cable with an Alligator-clip and listen to the messages. When packet-switching spread globally with the Internet in the 1990s, this became a central concern of intelligence and law enforcement agencies, which will be discussed in a later chapter (4.4.7.3 Artifacts: NSA and the Full-take Norm of Internet Control (2001 -)). For ARPA engineers, surveillance and eavesdropping was not a concern because they could not predict that an idea invented in the late 1960s would still be in use 30 years later. They chose packet switching only for pragmatic reasons: it was a feasible, robust and innovative solution to the problem of incompatible computer systems.

These theoretical ideas had to be implemented into a working software protocol that defined how packet-switching was going to work. This implementation process happened in a special social context with a special configuration of actors, which will be introduced in the next chapter.

4.1.2.2 Norms Shaping the Construction of ARPANET

The Network Control Program (or protocol), implementing the packet-switching idea was written by a set of graduate students at the four host-universities, who formed the so-called Network Working Group (NWG). According to the theoretical model (see chap. 2.3.5 Phase Model of Technological Diffusion), it is important to analyze the social

configuration, the context of invention, which is the purpose of this chapter. The ARPA developers represent the organizational platform or the key-advocates for norm-emergence (Townes, 2012, p. 51).

Steven Crocker, one of the designers, describes the situation these young computer scientists found themselves in:

> "There was no senior leadership. There were no professors. There was no adult in the room, as it were. We were all more or less in our mid-20s and self-organized. Out of that emerged ... a strong sense that we couldn't nail down everything. We had to be very ginger about what we specified and leave others to build on top of it. So we tried to focus on an architecture that had very thin layers that you could build on top of — or go around" (Crocker, 2012).

This social configuration, another instance of the freewheeling ARPA management style, imposed pragmatism on them. They had to design the protocol as open and transparent as possible to allow future modification. Thus, *openness represented the core norm* during the development process.

> "The openness in the design and the openness in the design process were driven by a strong understanding that we didn't know everything and hence needed to leave the door wide open for others to build on what we were doing. You can describe this as an academic ideal if you want, but it can just as easily be described as engineering pragmatism" (Crocker, 2015).

Being computer scientists, they invented a peer-review mechanism to collect and brainstorm ideas which they called "Request for Comments" (RFC). Originally these were "temporary, informal memos on network protocols" and the "intent was only to encourage others to chime in, but I worried we might sound as though we were making official decisions or asserting authority" (Crocker, 2009). This documented their work progress and allowed every participant in the group to suggest modifications to the protocols. The RFCs were sent to everyone by post (later by E-mail).[34] This mode of collaborative work reflected strong equality norms among peers and not competition: "Everyone was welcome to propose ideas, and if enough people liked it and used it, the design became a standard" (Crocker, 2009). In other words, it represented a *meritocracy*, similar to the hacker ethic that developed around the same time (see chap. 4.2.1 Background: Hacker-ethic and Technical Optimism (1960s)). The network protocol was a cooperational effort and thus belonged to no one. It was not proprietary intellectual property but was perceived as a commons. What they developed was for the sake of all and thus public in principle. "We did not think of protocols as finished products, and we deliberately exposed the internal

[34] They also have been digitally archived (RFC Archive, 2016).

architecture to make it easy for others to gain a foothold" (Crocker, 2009). The source code was openly published for everyone interested and could be modified by everyone in the group (because all were programmers).

Naughton summarizes the importance of these RFCs and this mode of production in the history of the Internet:

> "What these kids were inventing, of course, was not just a new way of working collaboratively, but a new way of creating software. The fundamental ethos of the Net was laid down in the deliberations of the Network Working Group. It was an ethos which assumed that nothing was secret, that problems existed to be solved collaboratively, that solutions emerged iteratively, and that everything which was produced should be in the public domain. It was, in fact, the genesis of what would become known much later as the Open Source movement" (Naughton, 1999, p. 138).

This peer-to-peer mode of production, as it was later called (Benkler, 2006), initiated a path trajectory that is fundamental for the entire history of the Internet. The same modus operandi was used when creating the Internet and it is still present in today's Internet governance structures (Hofmann, 2005) with the motto "We reject kings, presidents and voting. We believe in rough consensus and running code" (Clark, 1992).

The important condition is that the free-wheeling ARPA management style supported and actively endorsed this: "There was the culture of the funding by ARPA and the research by the principal investigators and by the graduate students that fostered the open, shared, trusted, ethical, free exchange and spirit of that period" (Kleinrock, 2015). Lawrence Roberts strongly supported this and participated in this process as well.

Having talked about the social mode of construction, the next step is to illuminate the outcome of this process, the artifact called the network control protocol (NCP).

4.1.2.3 Artifact: The Network Control Program

To realize those goals and to reflect the norm of openness, the NWG built the Network Control Program in layers. Each layer would perform only one function and would be separated from the rest. Lower layers would manage packet switching and transport of data, higher level layers would run the applications (remote access to computers). This layer model became an industry standard because each layer could be tested, checked for errors (de-bugging) and reprogrammed individually without distorting the rest of the functions, which allowed the system to be highly adaptable and scalable. Layering also reduced technical complexity of the system and allowed it to be built in a decentralized way at different host-sites at the same time.

The NWG wanted the *application layer to be as open as possible*, allowing all kinds of different applications (i.e. the stuff that could be sent over the network). "The openness of the protocol design process was motivated by wanting to promote the widest possible adoption and the widest base for future innovation" (Crocker, 2015). In other words, the designers intentionally did not prohibit what could be sent over the network, thus allowing all kinds of possible applications and usage scenarios. The network was supposed to empower users to develop new applications and therefore, the network did not care about the content being sent over it, just like the highway system does not care whether the traffic consists of business people or families going on vacation. The *network remained neutral or indifferent* in regard to the content. Later, digital natives and cyber-utopians interpreted and framed this openness as a freedom of speech norm (see chap. 4.2.8 Norms and Key Ideas of Cyber-Utopianism), but it was not explicitly conceived by the designers as such.

> "In general, we didn't view the Arpanet as having any moral issues one way or the other. It's not that we didn't think about such things, but I think the general view is that technology is a tool, and it can be used for good or evil. The tool itself is not inherently good or bad" (Crocker, 2015).

The developers clearly adopted a pragmatic, technology-as-a-tool perspective which argues that the social agent determines the technology by its use. If the designers had wanted to limit usability, they could have implemented functions that would prohibit certain applications from running but they did not because they wanted it open, flexible and adaptable. This decision would later open the door for applications in the legal gray area (like sharing of copyrighted material or computer malware).[35]

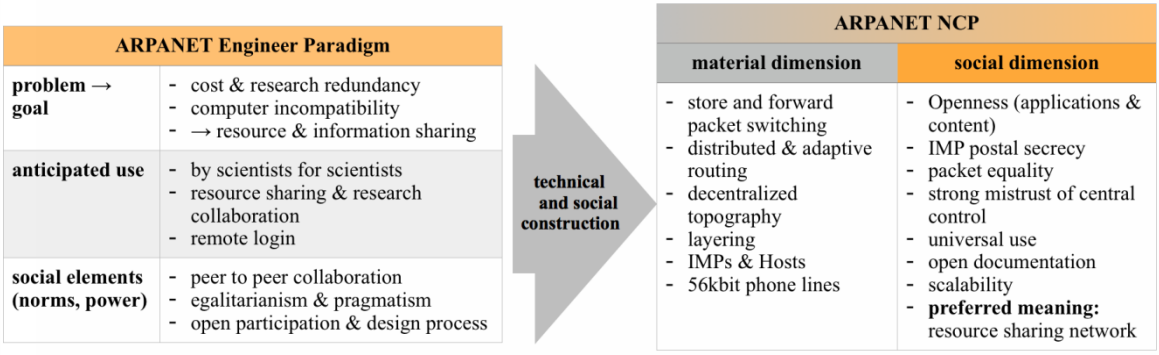
Because computers were incompatible (and sometimes did not even have the same character set of signs) another important decision was made, which still has huge implications today: the intermediary nodes, the IMPs or routers, *would only read the address of a packet,* but not the message itself. The content of a message would be readable only at the target computer, which reassembled the chopped up packets (Abbate, 2000, p. 123). This becomes clearer if we use a post card analogy (see chap. 4.1.2.1 Ideas). The IMP would only read the data required to establish communication (i.e. address field) which was written in the first 32 bits of an individual packet (the so-called header). The protocol did not care what was written on the message field of the post card (like it is

[35] The NWG itself developed a wide variety of applications that could be run on the network like file-transfers (File Transfer Protocol or FTP) and remote-login (TELNET). In fact, file-sharing was implemented quite early in the technological design of the ARPANET and was one if its earliest functions and basically a core functionality of a computer network (Abbate, 2000, pp. 106-108).

supposed to be in the post office as well). Again, cyber-utopianism later picked up this idea, interpreted and framed it as a privacy feature (see chap. 4.2.8 Norms and Key Ideas of Cyber-Utopianism). But again, this function developed out of technological feasibility, pragmatism and the goal of openness and adaptability and not necessarily for political or moral reasons.[36] If the IMP (which was running the NCP) would read all messages coming through, it would require more computing power proportional to the total size of the network. This would make them more expensive and prone to error. Therefore, it was more efficient if the IMP or router did not read every message passing through.

To sum up, ARPANET reflected academic or engineering norms: "[…] The style of design and cooperation mirrored the academic notion of information sharing as coin of the realm" (Cerf, 2015). The early protocol design of the ARPANET represented four core norms that were inspired by a scientific/engineering paradigm held by the inventors. First, *anything can be sent*. Second, no intermediary could read what was sent *(which resembles postal secrecy)*. Third, *all traffic was handled equally*. All packets were equal, no matter what their content was. Finally, the *network topology and the subnetwork idea reflected a strong mistrust of central control*: "the network could not/should not depend upon a centralized control structure, but rather on a distributed control structure that no one (or a few) parts of the network controlled the rest, but that all portions shared the control" (Kleinrock, 2015). No central authority, no corporation or state should control the entire network. It is important to stress that these norms were not embedded for political reasons, but rather because of pragmatism. They were the best technical solutions to a problem. None of the inventors could foresee the future and no one anticipated the privacy or freedom of speech issues that emerged later. The engineers can be seen as *passive norm entrepreneurs*: they shaped the social and technical dimension of the artifact ARPANET without intentionally promoting a moral agenda with their technology.

Figure 16. Engineer Paradigm influencing ARPANET Design (own diagram)



[36] "The privacy issue was not one that drove the original design, as I recall […]" (Kleinrock, 2015).

However, their mode of peer-production necessitated openness and their academic background supported the idea of free information exchange, network neutrality and mistrust in central control. In other words, social norms and academic ideas might not have been dominant during the construction, but they were there to some degree. Their pragmatic decisions pre-structured the path for later discourse. The cyber-utopian paradigm perceived these structural features as intentional moral decisions that became embedded in code (interpretative flexibility). When the first discourse about the implications of this technology developed in the 1980s, the social implications of these design decision became visible. These passive norms became signified as norms with the widespread diffusion of ARPANET's successor, the Internet, because cyber-utopian advocates framed them as such. But there is another important instance of co-shaping the meaning of technology. The early users had an impact here as well.

4.1.2.4 Co-shaping the Meaning of Networks

This chapter argues that not just the ideas of the inventors were important, but that user-feedback helped to establish the meaning, purpose and technical utility of the network. In fact, Naughton argues that the ARPANET is an interesting instance of co-shaping of technology, where the users gave the technology a concrete utility and meaning that had not been intended by the developers (Naughton, 2016, p. 9). What the ARPANET meant and what it could be used for emerged out of the practice of using it. This also led to the creation of several norms that were not anticipated by its designers. This user feedback was possible because the ARPA management style explicitly endorsed it.

The NWG finished the final specifications for the protocol in December 1970 and most of the ARPANET's initial physical infrastructure of IMPs, Hosts and telephone cables (the so-called backbone)[37] was in place by the end of 1971 and run by the Department of Defense (DoD) (Abbate, 2000, p. 78). This represents the phase where the system stabilized (see chap. 2.3.5.2 Stabilization). Robert Taylor left ARPA to Xerox in 1969 and Lawrence Roberts became head of IPTO. Since then, the technical diffusion of ARPANET across US computer research centers had begun. Roughly one computer center per month was connected to ARPANET, excluding those universities without ARPA contracts. By July 1977, 58 host-sites had been connected to ARPANET, and the first

[37] "An Internet backbone refers to one of the principal data routes between large, strategically interconnected networks and core routers on the Internet. An Internet backbone is a very high-speed data transmission line that provides networking facilities to relatively small but high-speed Internet service providers all around the world" (Technopedia, 2015).

international links to Norway and London had been created (Heart et al., 1981, pp. III-80-91).[38]

In the beginning, the ARPANET was used "primarily as a facility for experimentation with packet-switching" (David, 2001, p. 7), a solution for a problem yet to find. Besides that, there was not much to do. In the fall of 1971, it was estimated that the network carried only 2% of its intended capacity, which implied that no one really used it (Hafner & Lyon, 1998, p. 175). Particularly the feature of resource-sharing was seldom used. Roberts decided in 1971 that direct access of terminals and new emerging mini-computers to ARPANET, without the need for a host-computer, would be a good idea because it would bring more users to the net. This was a reaction to the computer-revolution that began to emerge around the same time (see chap. 4.2.3 Artifact: Democratizing Technology (1970-1980)). It led to the widespread diffusion of personal computer technology to enthusiasts and early or adopters (Abbate, 2000, p. 138). Around the time there existed around 50000 computers at universities and private companies (Rid, 2016, p. 141). This new spectrum of users articulated their demands and norms about computing: they wanted to connect their machines to ARPANET and did not want to rely on large mainframes (Heart et al., 1981, p. 117). A new actor formation and a new cyber-utopian paradigm were forming. This is an important contextual factor that was crucial for the success of ARPANET.

ARPA endorsed more users on the network. There weren't any formal rules or acceptable use policies. The only access requirement was that you had a username and password that was registered with one of the networking sites, but local administrators tended to give access out freely (Abbate, 2000, p. 85). Unauthorized users (called network randoms) were tolerated as long as they did not do any harm (because they increased traffic). This lack of security has to do with the engineering paradigm that influenced the development of the net (see chap. 4.1.5 Development Blind Spots). The *early adopters of the network formed an epistemic community of computer scientists* (initially there were few military applications) because technical access and use barriers were quite high. In order to use the ARPANET, you had to be a trained computer scientist. There was only text on the net (no images, audio or video) and "browsing" was done by typing in computer commands manually. You had to have precise knowledge about what you were looking for, where to find it and if you found it, how to use it. This remained the status quo until the invention of the graphical web browser software Mosaic in 1991 (see chap. 4.1.4

[38] One example of early military use of ARPANET was to transmit data from the NORSAR seismic array, used for detecting underground nuclear tests from the Soviet Union, from Norway to the US (Townes, 2012, p. 50).

Artifact: The World Wide Web (1989-present)). For the impact constituents, the users, the experience was so frustrating that they started to develop new applications and to engage in the design process themselves.

One episode is insightful. While running network diagnostics, an unusual amount of intra-node traffic at MIT was detected, the same place where the hacker ethic formed (see chap. 4.2.1 Background: Hacker-ethic and Technical Optimism (1960s)). BBN realized that MIT users had turned (hacked) their IMP into a hub for local-area networking, sending data and personal messages between local computers at MIT. ARPANET was designed to connect long-distance research communities. "The notion of using the IMP as a local connection was quite a surprise, to the extent that it became just common and had not been envisaged" (Heart, 1990). This discovery represents an anomaly in the Kuhnian sense: the network was used for something that the dominant engineering paradigm did not anticipate.

One of those "killer-applications" was Network E-mail, introduced in 1972 by Ray Tomlinson. Its traffic began to dominate the ARPANET, thus manifesting the dramatic desire/need for people-to-people communication. This was a "major shift" (Kleinrock, 2015). The official completion report states: E-mail "changed significantly the feel of collaborative research with remote groups" (Heart et al., 1981, pp. III-113). The service was relatively easy to use and way quicker and more affordable than telephone. Mail also became quite popular with ARPA management and Roberts began funding E-mail hosts at BBN and other locations, which gave users E-mail accounts (similar to what Mail providers nowadays do). The ARPA-director at the time, Stephen Lukasik (1970-1975), was a strong advocate of E-mail who used the ARPANET for managing internal affairs (Lukasik, 2011, p. 14). He lobbied much of ARPA's management and other agencies and departments to use this technology, acting as a norm entrepreneur (Lukasik, 1991). With E-mail also came the first newsletters and mailing lists (one-to-many or many-to-many communication) which had a huge impact on the formation of virtual communities and the development of social norms therein. ARPA itself created the ARPA Newsletter (published by SRI in 1973) which contained information on log-in sites, new hosts and new applications. Mailing lists disseminated information for all subscribers and they formed around various topics, professional as well as recreational.

In sum, what the users did was to engage in a reconstitution-process to alter the technical function and social meaning of the ARPANET (see chap. 2.3.6 Combining the Frameworks). By inventing attractive new applications such as E-mail or even games, they altered the meaning of the technology step-by-step and created standards of appropriate

behavior within the computer network. Suddenly, they were able to share their ideas and research data with help of electronic mail and file-sharing. Communicating via mailing lists became a standard of appropriate behavior within the research community. The repeated practice of thousands of users established E-mail communication as a norm of computing that changed what the network was and meant. This changed the meaning of ARPANET from being a remote sharing network into being an *information technology*, a notion that was novel at the time (McLuhan, 1964). This perception of the ARPANET diffused among educational channels and into the public.

In 1972, ARPANET was presented to the public at the International Conference on Computer Communications, which is described as a "watershed moment" (Cerf, 1990) for the ARPANET. To prepare for the conference, Roberts engaged his team and contractors to develop useful applications and usage scenarios for the ARPANET (Kleinrock, 1990, p. 25). This means that many of the usage scenarios for the network came after its construction, representing a solution in search for problems. "There were simple demonstrations of e-mail, and text editing, and file transfers, and remote log-ins, and things like that" (Cerf, 1990). User innovation such as Tomlinson's E-mail was key in making the technology interesting and demonstrated its utility to the general computer public. The ARPANET presentation of 1972 indicated a major change in the perception of networking technology and what networks actually meant and could do. It transformed the experimental and unproven concept of packet-switching networks into something *real* and tangible.

This episode aligns nicely with the theory (see chap. 2.3.5.3 Diffusion to the Mainstream). In theoretical terms, the presentation of 1972 represented a *closure* moment that reduced interpretative flexibility and changed what networking and networks actually meant. The whole presentation changed the computing discourse of that time by establishing a dominant discourse on computer networking. Terms like packet-switching, sharing, decentralization, E-mail and layering became key signifiers in computer science discourses of the time. Networking became the next big thing and "the future" as several electronics magazines stated (Electronics, 1972). The ARPANET presentation altered the meaning of networks from experimental resource sharing to factual *information sharing of social actors* (Kleinrock, 1990, pp. 24-25). E-mailing, a norm that developed out of deviant practices showed that the most "valued resources of the net were people, not computers" (Abbate, 2000, p. 111). The norm that it was appropriate to use this network for information exchange then diffused to the mainstream.

This change of meaning had several distinct outcomes. First, computer makers and developers suddenly realized that a new networking market was emerging (Abbate, 2000, p. 186) and rushed to develop their own marketable solutions. The ARPANET, with its innovative packet-switching, adaptive routing and layered protocol in fact became the dominant design for computer networking and later a de-facto standard for networking (see chap. 2.3.4 The Social Construction of Technology and its Critique). Quarterman shows how the 1972 presentation led to an international diffusion of packet-switching technology and thereby jumpstarted new developments such as local area networking (LAN). More so, the quantity of networks increased, creating new types of incompatibilities (Quarterman, 1989).

Second, the ARPANET changed the way scientists worked and what types of projects were feasible.[39] The network greatly contributed to the formation of virtual communities on message boards or online forums that later became important (see chap. 4.2.4 Artifact: The WELL and the Social Construction of Cyberspace (1980-1990)). These networks allowed information sharing for non-professionals and can be highlighted as the birthplace of the net-community with its network-citizens, netizens. Because ARPA was funding the majority of American computer science and most of these institutions got access to the ARPANET, this dominant design and the social norms of peer-to-peer collaboration quickly spread through the educational channels and were discussed in computer science textbooks and journals, representing carrier media for the paradigm (Roberts, 1988, pp. 149-151). This could only happen because the ARPANET specifications were made public in the RFC's: everyone could look them up and replicate the technology.

Third, more users became aware of the networks and wanted access, including the military. One of the early uses of the ARPANET were DARPAs seismology (for verification of nuclear tests) and climate programs. Additionally, policy-makers such as Albert Gore began to recognize this technology (see chap. 4.3.2 Politics: Bill Clinton and Albert Gore as Internet Advocates (1992-2000)). In sum, this led to an increase of users of the ARPANET and represented a beginning decontextualization of the technology from academic contexts to the business or military world. The mass diffusion of networks created a new, but also an old problem, the incompatibility of different networks. This

[39] In 1977, Paul Baran and David Farber invented a new type of research cooperation when writing one of the first research papers collaboratively over the ARPANET. They argue that packet-switching networks are going to replace the dominant communications paradigm of circuit-switching (telephony). They predicted that networks soon will be used for "mundane applications: automated hotel reservations, credit checking, real-time financial transactions, access to insurance and medical records, general information retrieval, and real-time inventory control in business" (Baran & Farber, 1977, p. 1066), which would fundamentally transform the economy.

issue played a major role in creating the Internet, which will be introduced in the next chapter.

4.1.3 Constructing the Internet (1972-1991)

The evolution of the Internet does not end with the successful ARPANET experiment, because one successful computer network does not constitute an *inter*-net. The term *inter* in Internet can mean two things. First, an inter-network connection bridging two or more computer networks and second, an inter-national connection that makes it truly global. This chapter is about how the ARPANET became the international inter-network that we still use today. To realize this, a new set of protocols had to be constructed, thus representing another instance of goal-oriented construction (see chap. 2.3.5.1 Emergence/Construction). The general argument is that the new Internet Protocol inherited many ideas and norms of ARPANET, since it was constructed in the same peer-to-peer manner and within the same organizational structure of ARPA. However, the problem of connecting different computer networks posed new challenges that required new ideas.

After Taylor left ARPA in 1969, Lawrence Roberts became head of IPTO in 1972 and hired the former BBN programmer and developer Robert Kahn to manage the different networking projects that ARPA had started after the ARPANET's success. IPTO researched new applications for networks, such as a satellite communication net (SATNET) or the ALOHANET where the goal was to connect the Hawaiian Islands with radio-waves. These other networks represented forking-path developments of packet-switching (see chap. 2.3.5 Phase Model of Technological Diffusion). Kahn was faced with different networks which, although they used packet-switching, were fundamentally incompatible because they used different data rates, different packet sizes and speeds (Cerf, 2014). Each network thought it was the only one in existence because it had not been designed to recognize others. Kahn described this *core problem* that led to the Internet in an interview:

> "Here I am sitting with the notion of multiple networks, and I'm trying to think, how would we actually do anything interesting with them if we don't connect them? Because the computers were all very big. If I have a radio net, what am I going to do with the radio net? I can maybe plug a terminal into a little interfacing computer, but I've got to get to some big machine to do anything interesting. So I had the problem of trying to figure in those nets, and I had a basic architectural approach to deal with it, which is what became the Internet" (Kahn, 2004).

In other words, a new networking protocol was needed that managed packet-handling between incompatible computer networks. Kahn followed the path outlined by his IPTO predecessors and adopted the same informal management style. He approached his old friend Vinton Cerf, with whom he had worked on the ARPANET protocol. Cerf was active chairman in the NWG, which after the 1972 presentation became international and renamed itself to International Packet Network Working Group (INWG).[40] By 1972, several competing networks were being developed in Britain, in France (project Cyclades) and at private firms such as Xerox, where Robert Metcalfe was working on another fundamental technology called Ethernet (Metcalfe, 2004). INWG was the international networking forum for idea-exchange between computer network experts and networking initiatives around the world. It maintained the informal RFC tradition (called INWG notes). Theoretically speaking, the norms and ideas that diffused through ARPANET resonated with Cerf and Kahn (see chap. 2.3.6 Combining the Frameworks) and thus they internalized and reified these norms. Out of this idea exchange between the international actors, emerged "A Protocol for Packet Network Interconnection", as Kahn's and Cerf's from 1974 paper was called.[41]

In this paper, they called this new inter-networking protocol *Transmission Control Protocol* (TCP) and named the network of networks they planned to build the "Internet". TCP/IP is the software protocol that governs how the Internet works. Between 1974 and 1979 the protocol was refined several times through the process of RFC and peer-to-peer collaboration with international scholars (Kahn, 1995, p. 14). The first successful test was in 1977 when a packet-radio network in San Francisco, the ARPANET and the SATNET, were connected and exchanged packets with each other. In 1978 researchers proposed "splitting the TCP protocol into two separate parts: a host-to-host protocol (TCP) and an internetwork protocol (IP). […] IP would simply pass individual packets between machines (from host to packet switch, or between packet switches); TCP would be responsible for ordering these packets into reliable connections between pairs of hosts" (Cohen, 1978, p. 179). Henceforth the protocol became a protocol-suite or *protocol-stack named TCP/IP*. Throughout 1979, Cerf and Kahn lobbied the DoD to make TCP/IP a defense department standard for their computer networks (Pelkey, 2014, p. Chap 9.6).

[40] Cerf: "The INWG group was about 25 people or so, which ultimately grew to, you know, a mailing list of several hundred" (Cerf, 1990). However, as Pelkey (2014, chap 6.3) remarks, the initiative to make NWG international came from European researchers after the ICCC conference: "they agreed they needed to meet again and function much like the Network Working Group, NWG, of ARPANET."

[41] According to Naughton, they tossed a coin and Cerf came out as the first author (Naughton, 1999, p. 162). Since then he is regarded by many as "the father" of the Internet. In reality, many people sponsored important ideas. Cerf and Kahn simply collected all the free-floating ideas and wrote them up. Cerf modestly mentions Louis Pouzin, Hubert Zimmerman, Robert Metcalfe as influential contributors to the design.

Additionally, they planned that the ARPANET, still based on the NCP, would be migrated to TCP/IP (to support satellite links), a process that eventually took until 1 January 1983. Cerf describes the period between 1983 and 1985 as a consolidation period for TCP/IP (Naughton, 1999, p. 168), which corresponds with its technical stabilization (see chap. 2.3.5.2 Stabilization). During this time frame, more and more actors picked up TCP/IP as a standard for their networks or built computer hardware and software to support TCP/IP.

This new version was partly a path-dependent construct that further developed ideas from ARPANET, but it also added new components which will be introduced in the next chapter. There I will explain how it worked and what its core ideas and norms were. After that follows a chapter on the spread of TCP/IP that led to the WWW in the 1990s.

4.1.3.1 Artifact: Internet Protocols and Norms

What were the new characteristics of TCP/IP? Generally, "the basic design of protocol layers and documentation and much of the upper structure was done as part of the ARPAnet and continued without much modification as the Internet came into being" (Crocker, 2009). In other words, the Internet protocol inherited many design features (on the technical side: packet switching, distribution, adaptive routing, layering) and norms (open source ethos and RFC mode of working and lack of business or security features) of the ARPANET, but because of its different scope, had to implement new design elements. This is a prime example of path-dependency.

The fundamental difference between ARPANET and the Internet is that the latter would connect multiple independent networks with heterogeneous architectures, like radio or satellite communications or networks owned by private actors, thus constituting a meta-network (Leiner et al., 2015). Therefore, it occurred to Kahn that it would require an *open architecture*, which means that the protocol would not put any constraints on the types of network or devices that it included. Openness thus is both the key design principle of the Internet (see chap. 2.3.5.1 Emergence/Construction) and also the key social norm: all networks, no matter of shape, size, function (private, military, civil) or technology (radio, satellite, wired) should be includable. An alternative interpretation of this idea is: "One of the primary norms of the Internet is that anyone can talk to anyone" (Crocker, 2015). In contrast to ARPANET, the Internet was intentionally designed to be a *communication medium* that supported communications between heterogeneous devices and networks (Cerf, 2014).

The general problem was that computer networks at the time had no language to refer to others. Each network operated like it was the only one in existence. Cerf and Kahn

could not enforce changes in individual networks to recognize others (Cerf & Kahn, 1974). What they did was to put a black box between the individual computer networks that disguised itself as a host-node in each. From the perspective of a single network, this special gateway computer looked like any other node that received packets. Packets of network A (with specialized packet sizes, bandwidths etc.) would be send to that gateway node and it would remodulate the packets to fit the general requirements of the next network B. The gateway computer performed the function of routing packets. Cerf describes the transmission of data in the network in an easy, understandable way using the post card analogy:

> "This is kinda like post cards in envelopes. So if I think of the underlying network as being a thing that carries envelopes and the addresses on the envelopes are unique to each network and I put a thing, we called a gateway, in-between the networks. When a computer generates an Internet packet we will have it stick that post card into an envelope and address that envelope in the next network's addressing structure. It goes through the network, the network has no idea that it is anything special: looks like any other packet, right? Like any other envelope. But when it gets to the destination's gateway, the gateway pulls the thing out, opens up the envelope, throws it away, and says 'what's in there?' and says 'holy-cow, it is an internet post card, what am I supposed to do with it?'. It looks in the routing table and says 'send it to this network over here' and it says 'ok, I know how to do that! I will create a new envelope for that network, stick the post card into it, seal the envelope and send it into the next net.' This thing is called encapsulation and decapsulation. And that is how we hopped the Internet protocol packets through all these different networks. It's as simple as that" (Cerf, 2014).

The intra-networks[42] handled their internal packet-switching operations and the gateways did the inter-networking part between heterogenous networks. They had to invent a system that allowed a packet from one network to find an address in a different network and this was solved with IP-addresses, which basically work like postal-addresses. Each device in the network gets an address towards which packets are sent. Each gateway acts as a decentralized post office sorting the messages for different postal areas (networks).

The encapsulation idea has important consequences: the local networks do not need to know about the location of the target host because it was the gateway's job to figure that out (Abbate, 2000, p. 129). The design of IP implicated that "no single node on the Internet knows definitively where a destination is, merely that it is 'over there.' Each node does know the exact location of every node it is connected to, and may pass its messages to

[42] Networks within the larger structure of the Internet.

whatever machine is closest to 'over there'" (Galloway, 2006, p. 44).[43] As a result, the nodes within the Internet have no idea that they actually participate in a larger meta-structure (the Internet) because they only see their neighboring nodes, but not what lies beyond. In other words, every device/computer on the Internet is potentially connected with every other device on the net without knowing it. This is the essence of *interconnectivity* that the Internet created. The Internet itself is not aware of its totality; it has no internal "awareness" or intelligence of all the individual nodes and subnetworks it consists of. The network is "stupid" (Isenberg, 1997) because it conceals its own innards (Galloway, 2006, p. 65). This technical affordance lies at the core of the so-called *attribution problem*[44] that underlies the logic of cyber-war (see chap. 4.4.2.2 Problem Definitions of Cyber-Realism) and is important to keep in mind for understanding the later chapter on the evolution of the military perspective towards the Internet, called cyber-realism. It is also an instance where Latour's "thingness of things" matters (Latour, 2000).

The lack of central intelligence was an intentional decision, but not because of normative concerns: "[…] We didn't want each computer at the edges of the nets to know how many nets you have to go through to get to the destination" (Cerf, 2014). When using the Internet, the user does not need to know that his/her data traverses a multitude of different computer networks. For the user, the Internet appears to be one network while in reality it consists of thousands of different networks. The implication of this is that when we send a message that message is chopped up in packets, repackaged and send "over there" randomly to nodes until the packet finds its destination. This may not always be the most direct route, because packets might cross multiple networks. If these networks are physically located in different countries, it happens that *packets cross different jurisdictions*, because they don't recognize borders. It can happen that it is quicker to send the packets from Berlin to Munich via networks in the US or China. The user does not normally see this process (unless he uses software called trace-route). Because everything happens in a millisecond or so, it appears as if the message was send directly from Berlin to Munich while actually it travelled two-times around the globe. This very feature is a central security issue for military-actors (see chap. 4.4.2.2 Problem Definitions of Cyber-

[43] Take for example the networks A-B-C-D-E. Gateway A only knows that it is connected to Gateway B and if it gets the task to send something to a computer in network E, it does not know were E is (Cerf 1979, in Abbate 2000). It passes the packet to its closest connection which is B. B does the same with C and D. Finally D is familiar with E and therefore delivers the packet. Theoretically, the message hops around the network until it arrives in the vicinity of the target and if it cannot find it, after a number of hops, it deletes itself and the sender retransmits. If ABCDE are gateways in different networks, at each hop a recapsulation is done.

[44] It refers to the problem that the origin of a cyber-attack seldom can be traced back to its origin. The encapsualted cyber-attack caries only information about the last gateway it passed so if it has been artificially rerouted around the globe, the origin cannot be determined.

Realism), but was framed by cyber-utopians as the erosion of state borders (see chap. 4.2.8 Norms and Key Ideas of Cyber-Utopianism). Again, this will be important later on.

Recapsulation also has important privacy implications that were discovered in the 1990s. Recapsulation conceals the content of the packet it wraps up, much like an envelope protects the content of a post card from being read by the postman while in transfer (resembling postal secrecy). It is important to stress that privacy protection was not a concern for the engineers. Who would threaten privacy in this closely-knit community of scientists anyway?[45] This privacy feature developed because it was a good and pragmatic solution to engineering problems. Privacy was a by-product but not necessarily intentionally developed. Given enough computing power, the gateways could have been designed to read the content of the decapsulated messages but this would have made the network more expensive and complex. Intelligence agencies nowadays lobby for a technology called Deep-Packet Inspection (DPI) that enables reading a packet's content when it crosses a gateway (Parsons, 2013).

More so, the Internet Protocol is actually blind to the integrity of the data it transports and the only thing that TCP does is to check whether the messages arrives in one piece (Galloway, 2006, p. 42). The only machines in the network that know the content of a message (chopped in packets) are the sender and the receiver at the outer edges of the network. This became known as the *end-to-end principle*, which is the central idea of the Internet.[46] "The motto was, don't rely on anything inside those nets" (Naughton, 1999, p. 162). The end points, not the gateways, are responsible for regulating data flow. If a packet gets lost in the network (or is garbled through radio transmission), the sender at the end would retransmit the package automatically at random time-intervals (Hafner & Lyon, 1998, p. 227). The logical alternative to this end-to-end design would be a network that had internal intelligence (Isenberg, 1997): "the hardware at each intermediate node in the network could be given the necessary capacity (data storage, applications that can react to interruptions and recreate messages, etc.) to perform this function" (Gillespie, 2006, p. 5). This alternative model became known as virtual circuit model and was implemented in the competing x.25 inter-networking standard proposed in 1976 (Abbate, 2000, pp. 148-156).

Another implication of this end-to-end design is *the norm of distributed control*: no single node in the network can control the entire network operation. There is no central

[45] As Crocker remarks: "In the early days, the use of the Arpanet was restricted to those who were working on ARPA sponsored projects. The development of TCP/IP was aimed at connecting different networks together, hence the term "Internet", with the intention of making networking available to as many people as possible" (Crocker, 2015).

[46] "The Internet's protocols themselves manifest a related principle called 'end-to-end': control [or location of network functions] lies at the ends of the network where the users are, leaving a simple network that is neutral with respect to the data it transmits, like any common carrier" (Gillespie, 2006).

watchtower that can monitor the entire network, or that distributes IP addresses (which has implications for surveillance and espionage). Additionally, there is no central routing table as in the ARPANET (Mueller, 2005, pp. 720-721). The Internet has a high degree of distribution because adaptive routing algorithms manage routing. Thus, control over the network is highly-decentralized, or distributed. Cyber-utopians later called this a self-generating mechanism (Zittrain, 2006). The Internet allows no central or hierarchical control. Therefore, it cannot be shut down from one central position. However, individual parts of the network can be shut down by severing ties (or fiber optic cables) or overloading the gateways that connect to the larger Internet.[47] Like with the ARPANET, espionage in form of simple wiretapping at one location was circumvented through of packet-switching (Abbate, 2000, p. 120). Surveilling the entire data-flow within the network was made extremely hard, which presents the key problem for intelligence agencies and law enforcement actors that want to monitor Internet communication. The idea of bulk-data collection on the Internet is a logical solution to this problem and has its origin with the idea of decentralization (see chap. 4.4.7.3 Artifacts: NSA and the Full-take Norm of Internet Control (2001 -))

These individual elements constitute another core norm which is called *net-neutrality*. Because the Internet was designed to be open, adaptable, general purpose and with distributed control, the network is neutral to the data it sends: all data packets are sent with the same speed and are treated the same, no matter if packets contain video information, text or E-mails. Everything is equal and no instance within the network can control traffic flow and data transmission speeds. All services run with the same quality (David, 2001, pp. 16-17). This technical affordance lies at the heart of the current net-neutrality debate in which commercial actors argue that a network of two speeds is desirable for different services such as video-streaming (see chap. 4.5.2 Ideas: Cyber-Utopianism under Obama and Clinton)

Finally, because of the open source ethos of the international community of developers, *TCP/IP was designed as a commons*. In a distributed network, all nodes share the responsibility for maintaining stability. Because the network would manage itself and network functions are a shared task it was not relevant who the owner of this network was. The documentation was as open as possible because everybody ought to be able to use and re-use it. Anyone could write an application that could use TCP/IP. No one had to be asked

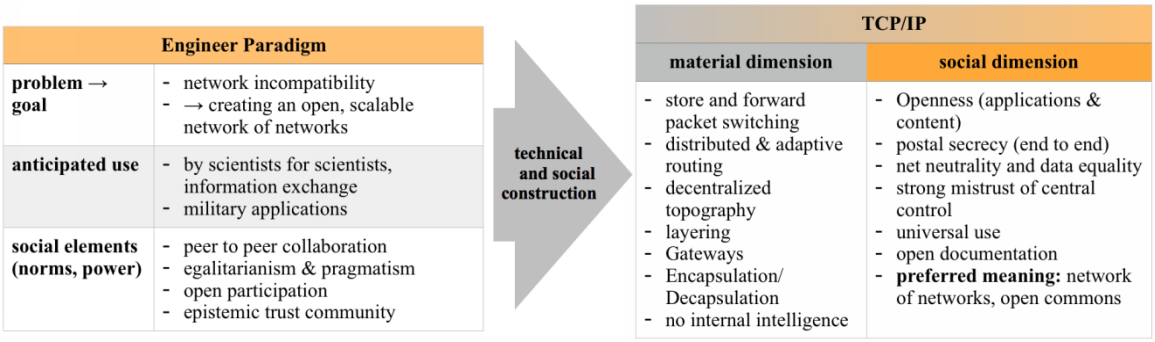
[47] Physical network shutdowns would become a political weapon used by state actors during the Arab Spring (Roberts et al., 2011) and since then feature prominently in the cyber-war arsenal of military actors (Geers, 2015).

for permission or a license. There was no limited copyright. TCP/IP was never patented and the protocols have fallen into the public domain (Mueller, 2005, p. 736). Cerf explains:

> " […] TCP-IP protocols were never patented. In fact, they were made available as widely as possible to the public as soon as possible. In fact, it's a little unusual that this happened because it was funded by the U.S. Defense Department, and normally one would have expected, not only would these have been rather close held, but they could even have been classified, except that all the work was done in the open with university researchers, principally coming from the computer science departments. The openness of those protocols and their availability was key to their adoption and widespread use" (Cerf, 2000).

This is a quite clear smoking-gun confession that the open-source norms are fundamental for the Internet. More so, the Internet was never classified either, although it developed in the context of ARPA (Townes, 2012, p. 54). The Internet actually is the manifestation of the open source idea and academic norms. In sum, the theoretical construction process looks like this:

Figure 17. Norms shaping TCP/IP (own diagram)



Galloway summarizes the key technical norms of TCP/IP: "The ultimate goal of the Internet protocols is totality. The virtues of the Internet are robustness, contingency, interoperability, flexibility, heterogeneity, pantheism. Accept everything, no matter what source, sender, or destination" (Galloway, 2006, p. 42). This openness in documentation is a key reason for the quick mainstream diffusion of TCP/IP and its becoming de facto standard.

4.1.3.2 The Diffusion and Dominance of the Internet

This chapter explains the diffusion of TCP/IP to mainstream users and traces the causal conditions for its success. TCP became operational in 1977 and the first two networks that were interconnected were ARPANET and the satellite network SATNET, which included international hosts in Norway (1973) and in 1985 Italy and Germany (Townes, 2012, p.

51). Quarterman estimated that in 1983 there were roughly 50 networks connected to the Internet. In 1989 the number grew to 500 (Quarterman, 1989, p. 282). This growth was facilitated by the 1970s digital revolution with the advent of the personal computer (see chap. Quantifying the Internet and the Digital Revolution). This dramatically changed the computer landscape: researchers and private persons started to buy smaller computers for individual use instead of relying on big university mainframes for the computing.[48]

Additionally, the Ethernet technology developed by Robert Metcalfe in 1973 – a forking-path development to accommodate packet-switching for the radio-network ALOHANET – began to spread rapidly during the 1980s. Local Area Networks (LAN or Ethernet) became standard at universities and companies[49] because they were relatively cheap to set up and dramatically increased collaborative working. It can be said that LAN is the Internet's little brother or as its inventor calls it: "The Ethernet is basically the low-level plumbing for the internet. […] every internet packet goes through a number of Ethernets before it gets from its source to its destination" (Metcalfe, 2004). Because TCP/IP was designed to be highly adaptable and scalable, it was compatible with LAN technologies and allowed the inclusion of the growing number of local area networks (in universities, private companies and even private homes) into the larger Inter-network. This collection of smaller networks gradually became called the Internet (Hafner & Lyon, 1998, p. 244). The existence of thousands of small LANs created grassroots pressure for the INWG to adhere to their very own openness idea and convinced them to modify TCP/IP to better support smaller networks. Computer users at DARPA-funded universities wanted to connect their smaller local networks to the ARPANET. Private companies wanted to connect their local business networks to larger ones. In fact, most pioneers of the Internet argue that the spread of LAN and the grassroot pressure it generated was a sufficient condition for the success of TCP/IP because, in contrast to other protocol competitors such as X.25, it supported LAN, which gave it an advantage for widespread adoption (Leiner et al., 2015).

[48] According to data from the US Census Bureau Current Population Survey (1984 and 1989), in 1984 8,2 million US households had a personal computer, while in 1989 the number almost doubled to 15 million (U.S. Census Bureau, 2005). Pelkey adds the numbers for business: " […] IDC estimated an installed base domestically of 27 million personal computers in business environments in 1987 with only 11% connected in LANs. They projected the number of personal computers in business environments to swell to 38 million by 1989 with 28% of them attached to LANs – a 65% growth rate over the 6.6 million personal computers attached to LANs in 1988" (Pelkey, 2014, p. chap. 12).

[49] According to Pelkey: "[in] 1985 there were 560,000 installed Ethernet LAN connections. Assuming five LAN connections, or computers, per network gives an estimated 100,000 Ethernet networks. In 1986, there were 650,000 Ethernet LAN connections shipped, likely doubling the number of Ethernet networks. The same would hold true for 1987 when 1,260,000 Ethernet LAN connections shipped" (Pelkey, 2014, p. chap. 12).

The other important factor for its success is openness. The TCP/IP specifications were openly available and because of DARPA's good connections to the computer science departments across the country, the design quickly spread. Thus, like Thomas Kuhn says, the knowledge of the paradigm was transferred to the next generation of scholars through textbooks and social interactions. TCP/IP was open. Everyone could reuse and re-modify it, which served the interest of the computing community. In the early 1980s, DARPA began to commercialize the technology to support commercial Internet products. As a result, the TCP/IP protocol was made available for all major computer companies and by 1990, most computers supported it. The ARPANET's old Network Control Protocol was updated to TCP/IP in 1983 and the hundreds of ARPA host-sites now supported TCP/IP (Leiner et al., 2015). DARPA started to support UC Berkeley to modify its UNIX operating system (BSD) to include TCP/IP in 1980. Before Windows, Unix was the dominant computer operating system for personal computers within the research community. This helped enormously to establish TCP/IP as de-facto-standard (Leiner et al., 2015) and indirectly influenced the emergence of grass-roots networks such as USENET (established in 1980), FIDONET (1983) or the WELL (1984), which Naughton calls the "poor man's ARPANET" (Naughton, 1999, p. 169). This is one of the key conditions for the mainstream diffusion of the Internet in the 1990s. All these systems were applications that could run on top of TCP/IP (application layer). Out of these grass-roots initiatives developed a cyber-utopian computer culture, inspired by the hacker-ethos and the fundament for cyber-utopianism (see chap. 4.2.4 Artifact: The WELL and the Social Construction of Cyberspace (1980-1990)). These cyber-utopians decontextualized the technology and thus were essential for norm-diffusion within the Internet and the concept of a cyber-*space*, a distinct space inside the computer.

This greater user base allowed TCP/IP to become the dominant technology for internetworking, although the competing X.25 protocol was proposed by powerful advocates from the telecommunications industry.[50] TCP/IP had an early-mover advantage and was already established, while X.25 was a mere theoretical and yet-to-be-proven standard (Abbate, 2000, pp. 154-155). All this indicates that the time was ripe, the market was receptive for an internet-working standard and that DARPA's entrepreneurship and advocacy played an important role during the early diffusion phase (see chap. 2.3.5.3 Diffusion to the Mainstream). The user base was an important factor, too. TCP/IP was more attractive because it allowed *all kinds of applications,* which facilitated a great

[50] Other competing network protocols were IBM's System Network Architecture, Xerox Network Services and Digital Equipment Corporations'S DECNET (Townes, 2012, p. 59).

social-embeddedness in new usage contexts. It was intentionally designed to be general purpose (and not just military): "it was not designed for just one application, but as a general infrastructure on which new applications could be conceived, as illustrated later by the emergence of the World Wide Web" (Leiner et al., 2015). Today one would use the term platform. The World Wide Web is simply one application that runs on the same TCP/IP infrastructure while E-Mail, Voice-over-IP or even the so-called "dark-net" are different applications. In other words, the Internet and the World Wide Web are not the same: the Internet (TCP/IP) represents the railroads and the WWW is what is transported over them.

Before we turn to the WWW it is necessary to illuminate changes in the physical architecture and the governance of the technology that appeared in the mid 1980s and set the foundation for global diffusion.

4.1.3.3 The Internet Backbone

ARPANET was decommissioned in 1990 because its hardware was outdated. It became replaced by the NSFNET or National Science Foundation Network launched in 1986 (Abbate, 2000, p. 194). This mode of succession corresponds with one technology replacing an older one (see chap. 2.3.5 Phase Model of Technological Diffusion). NFSNET's purpose was to physically connect NSF-funded super-computer research sites in the US, to create another network of networks. The program was directed by Dennis Jennings and represents a forking-path driven by ideas similar to ARPANET's resource sharing ideals: super-computer users should be able to remotely connect to super-computer centers to do calculations and work collaboratively (Merit Networks, 1995, pp. 16-19). The protocol running on this hardware was chosen to be TCP/IP because it was free, nonproprietary and sufficiently tested. In other words, the design of NSFNET represented similar ideas and norms developed at ARPA. Thus, it is an example of how norms diffuse with technology and resonate with new target audiences that chose to adopt these norms and thus reinforce the standards of appropriate behavior and use outlined in the design (see chap. 2.3.6 Combining the Frameworks). This reinforced the causal trajectory initiated by ARPANET and its academic norms.

Super-computers, which can process vast amounts of information, rely on high-speed hardware. In 1988, the network hardware connecting these super computers was updated to T-1 (1.544 megabits per second) connection speeds, way more powerful than ARPANET's

obsolete 56 kilobit/s telephone lines (National Science Foundation, 2016).[51] The powerful underlying physical hardware of NFSNET (high-speed lines and modernized packet switches) was called the backbone and connected thirteen regional networks in the US and later overseas (Office of Technology Assessment, 1993, p. 20). The software part, the TCP/IP protocol, remained mostly identical. The whole system became fully operational in 1988 and since then has carried a majority of the traffic of the different inter-connected networks. This is a significant transition in stewardship of the Internet. Since the 1970s, the physical nodes (Hosts and IMPs) of the Internet were in control of DARPA and thus under military stewardship. When NSFNET took over, stewardship was given to a civilian agency. Interestingly, this was only possible because of generous civil-research funding initiated by Congressman Albert Gore with the Supercomputer Network Study Act of 1986, as a later chapter will show (see chap. 4.3.2 Politics: Bill Clinton and Albert Gore as Internet Advocates (1992-2000)).

NSFNET vastly diffused Internet access to non-military, non-DARPA users. Theoretically speaking, NSFNET further decontextualized Internet use from the DARPA into a wider science context (see chap. 2.3.5.3 Diffusion to the Mainstream). The old ARPANET was an elitist club of DARPA funded universities and DoD institutions. Tensions were growing between those computer scientists who had access to the network and those who did not. The non-military public had limited access and thus a large part of the research community was excluded, which represents a somewhat unintentional exclusion strategy (see chap. 2.3.6 Combining the Frameworks). The use of services such as E-mail and community interaction were already the norm and "had greatly enhanced research productivity and had generated a strong community spirit among ARPANET sites" (Denning, Hearn, & Kern, 1983, p. 3). Those universities who could not access these services had a competitive disadvantage. The impact constituencies at these universities engaged in counter-appropriation, lobbying to gain access to the system. NSFNET gave these disconnected research centers access to the Internet and thus significantly expanded the Internet's use base. In 1985, there were roughly 2000 computers in the system and in 1993, 2 million (National Science Foundation, 2016).

A large-enough domestic and international user-base was sufficient condition for the success of the Internet because it increased the utility of the network and spawned a whole set of new services and applications (Townes, 2012, p. 58). This is sometimes called the *innovators dilemma*, resembling the chicken-egg problem. Robert Metcalfe argued that a

[51] South Korea currently has the fasted average Internet speed at 26.7 *mega*bits per second while the US scores around 12.6 mbit/s (Akamai, 2015).

computer network increases its value the more users are connected to it, which in turn attracts more users, ever increasing its value. The challenge for every new technology is to convince new users to adopt it although there is no utility yet because there are no users. This is sometimes referred to as Metcalfe's law although there is no solid mathematical proof for it (Metcalfe, 2006). However, the NSFNET provided a large enough user-base to make the Internet useful (Abbate, 2000, p. 188). Because the Internet was designed to be open for all kinds of applications, this laid the foundation for later innovations such as the World Wide Web and the creation of web-browsers (the first web-browser Mosaic was created within the context of NSF).

More users made it important to organize behavior within the net so the NSF enforced an "Acceptable Use Policy" which aimed to enforce a proper, scientific use of the NSFNET and therefore established several norms. It was acceptable to use the network for international communication and research exchange but should not be used for "for-profit activities" or "illegal or specifically unacceptable use" (National Science Foundation, 1992). Interestingly, the social configuration at ARPA that led to the informal, voluntary, open source governance style of NWG became replicated with the wider Internet community at the universities (path-dependency). The NSF community chose to mimic ARPAs organizational infrastructure that was a result of the open source development ethos, indicating path-dependency. It created the Internet Activities Board (IAB) with two subsidiary task forces Internet Engineering Taskforce (IETF) and Internet Research Task Force (IRTF) in 1986 (Abbate, 2000, p. 207). The IETF that still exists today is responsible for the short term Internet developments such as new standards. The IRTF focuses on long term issues (Kahn, 1995, p. 19). The culture of request for comments and distribution via E-mail for consensus finding is still in place today (DeNardis, 2015). Because of the decreased relevance of DARPA for the Internet, the NSF became a major player and steward in Internet governance until the technology was completely privatized in the mid 1990s.

But NSFNET also had an international impact:

> "The NSFNET backbone glued together the international networks—almost all traffic from abroad would transit the NSFNET. With that kind of connectivity available, other countries were prompted to build their own networks so they could get connected too. Many of them used NSFNET's three-tiered structure—backbone, regionals, campus networks—when they started to build their own networks" (Merit Networks, 1995, p. 34).

It set an example and provided the de-facto hardware standard for other countries to build new regional networks. Since NSFNET runs on the freely available TCP/IP, many other states opted for this example, initiating a technical norm-diffusion by emulation. Over 6000 networks were connected to NSFNET in 1992, and one third of them came from over-seas (Merit Networks, 1995, p. 35). One important over-sea connection was CERN (Conseil Européen pour la Recherche Nucléaire), where the World Wide Web was developed around the same time.

4.1.4 Artifact: The World Wide Web (1989-present)

This chapter introduces the final piece of the puzzle that shaped the meaning and usage of the Internet, the World Wide Web (WWW) or the visual Internet. It helped to diffuse TCP/IP globally and gave non-computer experts the possibility to use the Internet. The WWW is both an instance of theoretical decontextualization of a technology (see chap. 2.3.5.3 Diffusion to the Mainstream) as well as its partial reconstitution (see chap. 2.3.6 Combining the Frameworks)

The *core problem* of the Internet during the 1980s was its terrible usability. Everything was text and although the net contained a lot of interesting information, from various newsgroups, bulletin-boards and virtual communities (see chap. 4.2.4 Artifact: The WELL and the Social Construction of Cyberspace (1980-1990)) to file-sharing (of games and programs mostly), the data was hard to find. There was no search engine and you had to know where the information you were looking for was stored, then manually log onto the system and dig through the directories there. Surfing the web was basically old-fashioned command-line typing (like MS DOS) while the personal computer already got a graphical, windows-based point and click interface in 1984 with the Apple Macintosh.

This problem of information storage and retrieval struck Tim Berners-Lee (*1955), an English engineer working at the CERN nuclear research center in Geneva. CERN had a high personnel fluctuation, which created *problems* of information storage and retrieval: "The technical details of past projects are sometimes lost forever, or only recovered after a detective investigation in an emergency. Often, the information has been recorded, it just cannot be found" (Berners-Lee, 1989). In other words, CERN had no efficient institutional memory that stored what was going on within its doors. Berners-Lee's *goal* was "keeping track of relationships between all the people, experiments and machines, I wanted to access different kinds of information, such as a researcher's technical papers, the manuals for different software modules, minutes of meetings, hastily scribbled notes, and so on" (Berners-Lee, 2000, p. 15). To solve this problem, he wanted to create a shared

"*information space*" where all the researchers with their incompatible PCs could access each other's information. This was his dominant metaphor for understanding the WWW. He thought of it as a network of associations based on the scientific thought process. This thought-process is non-linear, non-hierarchical and based on association of different concepts (theories and data) with each other. Ideas in an academic paper are linked together by footnotes and references. Theoretically, one text continues in another one when the researcher jumps between references. This resembles not one insulated text, but a *hyper-text*. Hypertext, or the idea of non-sequential/non-linear text, had been conceived already with Vannevar Bush (Bush, 1945) and been picked up at ARPA-funded researchers in the 1960s, among them famous names such as Ted Nelson (see chap. 4.2.3 Artifact: Democratizing Technology (1970-1980)) and Douglas Engelbart (inventor of the mouse). The initial vision was:

> "Suppose all the information stored on computers everywhere were linked, I thought. Suppose I could program my computer to create a space in which anything could be linked to anything. All the bits of information in every computer at CERN, and on the planet, would be available to me and to anyone else. There would be a single, global information space. [...] Being able to reference anything with equal ease, a computer could represent associations between things that might seem unrelated but somehow did, in fact, share a relationship. A web of information would form" (Berners-Lee, 2000, p. 4).

But Hypertext was just one part of the story. Berners-Lee bundled it together with TCP/IP to create not just a local information space, but potentially a *global* one. From the very beginning he had not just CERN in mind, but potentially the entire research community, which all relied on different hardware and software. He chose TCP/IP for the very same reason it was invented: it allowed incompatible networks and computers to talk to each other and exchange data. Because TCP/IP was nonproprietary, he could simply use it.[52] To create this information space, Berners-Lee, together with his colleague Robert Cailiau, invented the *World Wide Web*.

Following good scientific practice, he wrote an official proposal in 1989 (Berners-Lee, 1989) with a request for comments (mimicking the INWG working procedure). In 1990 the proposal was modified and reformulated and Robert Cailliau (CERN senior management) jumped in as co-author. In their joint paper, they outlined the World Wide Web: "Texts are linked together in a way that one can go from one concept to another to find the information one wants" and this network of texts is called the Web (Berners-Lee &

[52] Following TCP/IP's footsteps, Berners-Lee released the WWW and its related technologies to the public domain in 1993, making it one of the most important open source artifacts (Berners-Lee, 2000, p. 73).

Cailliau, 1990). The information of these texts, the files so to speak, were to be stored not centrally on one machine but rather decentralized. The system was designed to link various files stored on different computers, utilizing TCP/IP.

Berners-Lee wrote a server software that would host or "serve" the information (a website) and a client software that could retrieve information (the browser). Berners-Lee and Cailliau also developed HTML (the Hypertext Markup Language), a common programing language that is relatively easy to use and allowed the indexing of media within the World Wide Web. With these tools, he created the first hypertext page (info.cern.ch) in 1990, which is still online today. This made the Internet tremendously easier to use.

More importantly, in August 1991, he made these tools available for free on this website (and thus on the Internet as a whole) and provided a documentation on how to use them. This move "exposed the Web to a very critical academic community" (Berners-Lee, 2000, p. 46). Because scientists could repurpose the system for their own needs, the reception was widely positive. Other scientists began to create own web servers to store their files and materials. This is an example of successful decontextualization and social-embeddedness: HTML resonated with a wider user community (see chap. 2.3.5.3 Diffusion to the Mainstream). Berners-Lee linked to them and created one of the first web-repositories or news hubs on the Internet. Berners-Lee tracked the activity on his server and "The rate was incredible, still doubling every three of four months, growing by a factor of ten every year, from one hundred hits a day in summer of 1991, to one thousand in the summer of 1992, to then thousand in the summer of 1993" (Berners-Lee, 2000, p. 75).

The final piece of the puzzle came in February 1993, when Marc Andreessen, working at a super computer center connected to NSFNET, wrote Mosaic, the very first graphical browser to access websites, and distributed it for free. The central appeal of Mosaic was that it was free of charge, easy to install and use and required no learning because it had a simple point-and-click interface that even allowed images, pretty much like modern-day browsers. Since the release of Mosaic, which later turned into Netscape, Internet usage skyrocketed because suddenly it was easy to use even for non-experts (see chap. Quantifying the Internet and the Digital Revolution). The Internet, being driven by text and command lines during the 1980s, suddenly became visual (Internet History Museum, 2016). Quickly, other formats such as audio and video followed.

Let’s consider the norms and Berners-Lee initial vision of the system, and the dangers it might face once more. The WWW follows the path set out by TCP/IP and the ARPANET community (path-dependency). It *shares the commitment to openness*, both technically in terms of compatibility and usability, but also in terms of the social process:

The Web was constructed in peer-to-peer fashion but was also designed for this very purpose (Berners-Lee, 2000, p. 203). Thus, the case can be made that the norms that became embedded in TCP/IP resonated with Berner's Lee who internalized them and reified them with his invention.

Berners-Lee chose a *system with minimal rules*: "I would have to create a system with common rules that would be acceptable to everyone. This meant as close as possible to no rules at all" (Berners-Lee, 2000, p. 16). Besides being minimalist, the other core property was "It had to be completely *decentralized*. That would be the only way a new person somewhere could start to use it without asking for access from anyone else. And that would be the only way the system could scale, so that as more people used it, it wouldn't get bogged down. This was good Internet-style engineering." (Berners-Lee, 2000, p. 16). Berners-Lee intentionally designed the Web without central control or a central gateway hub that had to be consulted before anyone could publish anyone. According to him, this was a philosophical, i.e. paradigmatic decision because being a scientist he *promoted the free exchange of information*: "For people to share knowledge, the Web must be a universal space across which all hypertext links can travel. […] Information must be able to cross social boundaries as well." (Berners-Lee, 2000, p. 164). There *should be no central control and no censor.* This was also a technical decision. Centralized systems can easily get congested. They do not scale and do not grow as well as decentralized ones. In sum, "there was no central computer "controlling" the Web, no simple network on which these protocols worked, not even an organization anywhere that "ran" the Web. The Web was not a physical "thing" that existed in a certain "place". It was a "space" in which information could exist" (Berners-Lee, 2000, p. 35). This hard to grasp nature of the Web creates a lot of interpretative flexibility which opens it up for endless interpretations and meanings, which is one reason for the cyber-utopianism of the 1990s (chap. 4.2.4 Artifact: The WELL and the Social Construction of Cyberspace (1980-1990)).

Berners-Lee argued reparably that the *openness* and *universality* were the key norms behind the project: everyone should be able to access the Web (regardless of computer and operating system) and everyone should be able to publish anything (and potentially modify anything, given prior authorization). But he also designed it to have a social effect:

> "When I proposed the Web in 1989, the driving force I had in mind was communication through shared knowledge, and the driving "market" for it was collaboration among people at work and at home. By building a hypertext Web, a group of people of whatever size could easily express themselves, quickly acquire and convey knowledge, overcome misunderstandings, and reduce duplication of

> effort. This would give people in a group a new power to build something together" (Berners-Lee, 2000, p. 162).

In other words, the WWW was designed to be an information space and a *tool for collaborative work and the creation of communities of interest*. It should increase creativity by linking knowledge together in a global, universal information space open for all who wish to access it. "This was the ultimate in openness in technical design and that culture of open processes was essential in enabling the Internet to grow and evolve as spectacularly as it has. In fact, we probably wouldn't have the Web without it" (Crocker, 2009). In other words, had the technology not been open but proprietary, the Internet may look quite different today.

Berners-Lee warned quite early that "the Web could splinter into various factions – some commercial, some academic, some free, some not. This would defeat the very purpose of the Web: to be a single, universal, accessible hypertext medium for sharing information" (Berners-Lee, 2000, p. 76). With the politicization and commercialization of the Internet in the late 1990s, he witnessed that it turned into a "battleground": "Many people in business, government and society at large would like to "control" the Web in some way" (Berners-Lee, 2000, p. 124). This, according to Berners-Lee is the single threat the Internet faces because it would pervert its initial logic and destroy its intended utility: the global and equal access of information. Thus, in 1996, he strictly opposed US Attempts to exert control over Internet content by censoring pornography (see chap. 4.3.5 Junctures: Policy Attempts to Control the Internet (1993-1996)). The idea that the Washington would decide what would be "indecent for everyone in the world was indeed sinister" (Berners-Lee, 2000, p. 113).

This indicates one of the central tensions that a universal information system creates: information that is regarded as harmless in one culture (say nudity or religious content) is considered indecent or amoral in another. But Berners-Lee argues that this is not a problem of the Internet itself, but of cultural sensitivities. Demanding to censor the system for every user on earth would act against the global purpose of the system. Thus, "keeping the medium and the content separate is a good rule" in political discourse (Berners-Lee, 2000, p. 130). The solution to the pornography dilemma is not to censor some information for all, but decentralize censorship to the end points: the user's computer, i.e. parental filtering software.

Even today, Berners-Lee is politically active, advocating against corporate control of the Internet, for example obstructing the principle of net-neutrality in the EU (Berners-Lee, 2016) or against pervasive Internet-surveillance of states. Thus, in contrast to most of his

ARPA colleagues, Berners-Lee is an active norm-entrepreneur arguing for free speech and open networks. His activism allowed Berners-Lee to be more sensitive to the politicization of the Internet technology and potential new developments that might affect the Internet that had not been envisioned by the designers. The next chapter will analyze the blind spots of the engineering paradigm that had political implications as the technology diffused globally.

4.1.5 Development Blind Spots

According to Kuhn, paradigms always create unanticipated blind spots. Legro argues that these are crucial to explain the demise of a paradigm, if a shock occurs (Legro, 2000). That is why I will talk about paradigm blind spots for each of the paradigms (see chap. 2.2.4 Explaining Change).

ARPANET, the Internet and the WWW were invented by computer scientists with the needs of scientists in mind. The goal was to establish connectivity, but not necessarily secure or economically feasible communications. Robert Metcalfe summarizes the blind spots as following:

> "The problem was we were grad students designing the Arpanet, and there were lots of things unimportant to us. Our goal was to get connected. We didn't care about security, because who would threaten it? We were a small family then, so we didn't really anticipate that anyone would be malicious. The other thing we left out was economics. Since we were being paid, we just didn't put any economics in the Arpanet. Eventually that was overcome in the 90s with the development of economics – like advertising for example. But still, the Internet is recovering from the lack of early attention to security and economics" (Metcalfe, 2006).

For this thesis, the *lack of security* is the most notable affordance of the technology and the prime indicator that ARPANET and TCP/IP served academic and not military purposes (Townes, 2012, p. 54). While the Internet's openness for all kinds of applications spawned millions of useful applications and services, it also enabled the malicious use of the network as well as cyber-warfare activities that disrupt, manipulate or destroy information in networks (Gartzke & Lindsay, 2015, p. 332). The problem is multi-faceted and complex so I will focus only on the most important issues.

First, the original Internet lacked a good authentication mechanism that assures that an IP address is genuine. Unlike phone numbers, IP-addresses are non-permanently assigned to users which means that the same user can have multiple IP addresses over time (which makes it complicated to attribute an IP to a user). More so, IP addresses can be spoofed easily. Thus, a malicious actor can claim to be someone he isn't. Until the invention of

SSL encryption in 1995, there was no way to make sure that a party on the Internet is indeed the party that it claims to be (Hallam-Baker, 2007). This *lack of authentication, together with the lack of network intelligence* (end-to-end principle) produces the attribution problem that makes it so hard to determine the source of a cyber-attack (see chap. 4.4.2.2 Problem Definitions of Cyber-Realism).

Second, the *Internet lacks secure or encrypted communication* that further prevent eavesdropping or surveillance. When thinking about network topographies at RAND in 1964, Paul Baran proposed to build an encryption system at the node level (Baran, 1964). Each switching node would encrypt the message blocks send forward. This would add another level of security and complexity and was indeed logical for a military-inspired network carrying classified information. Most military networks have encryption in place. [53] However, this security feature was not adopted for the ARPANET and the later Internet. IMPs would not read packet messages but they were still sent in plain-text which could be theoretically reassembled by someone who would collect all packets traversing a network. This is the reason why one should not send sensitive information over public WiFi networks. In 1967, an ARPANET engineer named Willis Ware wrote a paper on "Security and Privacy in Computer Systems" where he worried about unauthorized network intrusion, say by the Russians (Ware, 1967). As he approached Lawrence Roberts with the question of security, Roberts response was to focus on creating a working prototype first and worry about security once the experiment is a success (Kaplan, 2016, p. chap.1). Later the security question probably got forgotten. Security and network controls did not feature prominently within the engineering paradigm.

Why? ARPA Director Stephen Lukasik argues that the academics working on the projects were "too naïve and honest to conceive of REAL BAD GUYS" (Townes, 2012, p. 54). More so, restricting access or available information on the network would in fact violate the very goals of the system. ARPANET developed within the context of DARPA, but civil, not military scientists were in charge of designing the network. The peer-to-peer construction model created trust among the epistemic community of users and thus the question of security was secondary. This is an explanation for the lack of security. If the network would have been developed not peer-to-peer, but top-down by a more military orientated agency, it most likely would have been developed for clearer military purposes and thus would have stronger access and content controls in place. In other words, ARPA's

[53] MILNET, a spin-off or fork-development from ARPANET that emerged in the early 1980s added this additional security. MILNET would get re-equipped with encryption and better user access controls (in line with military norms) while the ARPANET remained open (Abbate, 2000, p. 143).

free-wheeling style was both the source of the Internet's success but also of some of its problems.

The *lack of economic considerations* is also important. A network developed by a private company, say AT&T[54] most likely would feature some element of billing, to make users pay for network use to compensate for the operating costs of such a network. Since ARPA funded the operations of ARPANET, a sustainable business model for networking was no requirement. The competing X.25 protocol, invented by the telecommunications giants allowed such a billing mechanism that tracked which sites a user would visit for how long and what content he/she was looking at (Abbate, 2000, p. 160).[55] Such a network would allow for better surveillance of users. This issue became prominent in the early 2000s, when copyright infringement because of file-sharing became a problem for copyright-holders (David, 2010). But since the Internet was developed by academics that relied on the idea of free flowing and easily accessible information, the idea of restricting certain files on the network or to limit access for certain user groups was completely incommensurable.

Lastly, Internet developers designed the network for a small epistemic community and never anticipated the world-wide diffusion. This envisioned usage scenario is important (see chap. 2.3.4 The Social Construction of Technology and its Critique). When Kahn and Cerf wrote the specification for TCP/IP in 1974, they estimated that there would be roughly 2-3 competing networks (like the ARPANET) per country. They also estimated that 4.3 billion potential IP-addresses (and thus devices on the network) would be more than enough (Cerf, 2014). At the time, the world population had not even reached four billion inhabitants and there were no smartphones and no laptops in every household. It is estimated that with the ongoing trend called the "Internet of things", by 2020, about 50 billion devices will be on the net (Cisco Systems, 2016).

4.1.6 Summary

Let's summarize the causal mechanism presented in this chapter. The goal-oriented construction of the Internet started with ARPANET, exhibited path-dependency with the TCP/IP Internet and culminated in the World Wide Web. Of course, the development is still going on, but for the thesis these first steps were the most crucial ones because they

[54] American Telephone and Telegraph Company.
[55] The X.25 protocol for internetworking was promoted by the International Telecommunications Union was built with access controls and cost-accounting in mind (Abbate, 2000, p. 160). Such a network was more centralized and could be controlled centrally by system operators. The intelligence was located at the gateway, which allowed for better monetarization because cost-accounting could be easily build in at the switch-level (Abbate, 2000, p. 160).

exerted causal influence into the future. I will summarize the causal mechanism in a narrative fashion and will present the most important parts in a summarizing table at the end.

The context of innovation at ARPA was a necessary condition for the later success and shape of the Internet. Additive causal factors are that ARPA provided *large enough funds* and through its *flexible management*, enough *academic freedom* to create an experimental network (part 1).[56] This equifinality of factors facilitated the construction of the network in the first place. It can be easily argued that without ARPA, no Internet, or at least not in the form it has nowadays. This can be proven by referring to the original inventors of packet-switching, like Paul Baran at RAND, who did not receive funding to build a prototype network because it was deemed to be unfeasible by the Defense Communications Agency (Abbate, 2000, pp. 20-21). Donald Davies, who developed the same concept, also could not convince the British Post Office (who owned the necessary transmission lines) to fund a similar network experiment in the United Kingdom (Davies, 1986).

The Internet was created by scientists for scientists and thus reflected academic or engineering key ideas and norms (Townes, 2012, p. 44), such as *openness* (in terms of participation, source code and envisioned content and use) and peer-review (RFC). These norms became embedded in the core invention called packet-switching as a by-product to pragmatic problem-solving and not because of intentional advocacy. The discussion of alternative network protocols such as X.25 has shown that had the network been developed by a private company, it would have included different billing or accounting features (see chap. 4.1.5 Development Blind Spots). In other words, the social configuration of actors, during the conjunction of construction, was a necessary condition for the design and the norms of the network (part 2). The creators of the Internet acted as passive norm entrepreneurs that put certain material affordances into the technology that became later realized and signified by the cyber-utopian users (see next chap. 4.2 The Evolution of Cyber-Utopianism). These affordances had a high interpretative flexibility but at the same time implicated a certain preferred interpretation: the fact that *everything could be sent* resembled freedom of speech *that intermediary nodes would not read packet-content* resembled postal secrecy and privacy, *net-neutrality* represented general equality and the *decentralized topography* represented mistrust in central control by states or large corporations. The social side of these artifacts was socially constructed by the users post-hoc during the mainstream diffusion, representing a conventionally paired action as

[56] A visual summary of the engineering paradigm is depicted in the appendix.

outlined in the theory (see chap. 2.3.4 The Social Construction of Technology and its Critique). The designers themselves saw the technology as neutral and did not want restrict usage scenarios or appropriate applications.

The users and early adopters played an important role in this reconstitution process (Pfaffenberger, 1992a). Because inventors at the same time were the users and because ARPA management was particularly open to user feedback, the meaning of the network was co-shaped by its users (part 3). Had ARPA not been as open and flexible, this feedback-loop would not have been possible (necessary condition). What the ARPANET meant was co-shaped by users and inventors with the practice of using the system. The impact constituencies of the system began to reconstitute the artifact by developing new applications such as file-transfer, E-mail or forums (see chap. 2.3.6 Combining the Frameworks). This established new norms of usage, for example that it is appropriate to communicate over this network instead of using remote-login. This process was enabled because the system was designed to open for new usages and ARPA leadership was supportive as well. Thus, the meaning of the ARPANET as a resource-sharing network changed into *being an information communication technology*. This meaning spread outside the ARPA community when the network became public in 1972.

Because the ARPA protocol documentation was open and non-classified, its specifications could easily spread through the research landscape and became embedded in textbooks in computer science. Thus, it became the dominant technical design for computer networks in the 1970s. The introduction of the Personal Computer had an additive causal effect that increased the user-base and spawned the creation of hundreds of new packet-switching networks. Without this user-base solving the chicken-egg dilemma of new technologies, the network would likely not have been a success. At the same time the spawning of hundreds of new incompatible networks was the necessary condition for the Internet's problem definition: how to interconnect these new, incompatible networks. To solve this problem, the TCP/IP protocol was created much in the same collaborative fashion as ARPANET. TCP/IP inherited the core features and norms of ARPANET, namely packet-switching but extended its logic. Path-dependency is a central explanation for the design of the Internet (see chap. 2.2.4 Explaining Change).

TCP/IP *maximized decentralization with the end-to-end principle*, implicating that no single node should be able to monitor or control the entire network of networks (part 4). Surveilling messages in the network was complicated because of packet switching and because the network had no internal intelligence of its operations. At the same time it interconnected every node with every other. This pragmatic technical decision allowed

great interconnectivity and scalability, but was also a necessary condition for the attribution-problem that lies at the core of cyber-war. This issue would be later become a national security problem for military actors. At the same time, cyber-utopians perceived this lack of internal intelligence as a privacy feature that created anonymity, which represents an example of how the same technical affordance creates different social meanings for actors adhering to different world views or paradigms. This will be further illuminated in later chapters (see chap. 4.2.8 Norms and Key Ideas of Cyber-Utopianism).

TCP/IP could successfully mass-diffuse through the market because it was open-source, scalable and adaptable to incorporate new types of networks such as Ethernet and others that spawned during the 1980s (part 5). Its open design was a necessary condition for its success. Because the designers never patented it and perceived the technology as a commons, TCP/IP could be easily embedded in computer and networking hardware of the 1980s without the need for licensing or royalty fees. This allowed social-embeddedness in new usage contexts outside of DARPA. Thus, TCP/IP was adopted by users in a grassroots fashion while the competing X.25 protocol lacked this momentum. The NSF adopted TCP/IP for its NSFNET, which began to replace ARPANET in the late 1980s, taking over large portions of the routing infrastructure while updating the capacity of the network (part 6). This new powerful backbone was a necessary condition for global diffusion. It opened-up the Internet to a wider national and international university landscape and quickly increased the user-base to around 2 million. This user-base was large enough to make the network useful and this is a necessary condition for its worldwide diffusion. The creation of NSFNET and its social governance of the technology are yet another instance of path-dependency and a necessary condition for the invention of the World Wide Web, the graphical representation of the Internet.

Tim Berners-Lee, although coming from a different context, adhered to similar academic norms as the ARPA community (namely openness, universality, decentralized control, free-speech). He is just another example of how norms diffuse together with technology (TCP/IP) and resonate with new users. His main vision was to design a coherent, global information space with Hypertext. He developed the necessary tools like HTML in a similar fashion like the ARPA engineers which, again, was a primary condition for the success of HTML. Berners-Lee's invention made the Internet visible and allowed non-technical users to use it. This is another necessary condition for the mass diffusion of the Internet that kicked-off in 1993. In sum, these necessary conditions in combination are a sufficient condition for the mass diffusion of the Internet (part 7).

The following table represents the causal-mechanism in a reader friendly format. The key take-away messages that are important for following chapters are depicted. I follow the graphical advice from Beach and Pedersen who suggest to depict causal mechanisms as actors engaging in *activity* (in italics) (Beach & Pedersen, 2012, pp. 38-40). The same schema will be used for all of the summary chapters.

Table 2. Causal Mechanism of the Social Construction of the Internet

Part 1	*ARPA bureaucratic cultur*e, flexible management and military budget *enables creation* of experimental packet-switching network (1960s).
Part 2	Unique social configuration of academics/engineers *designs* the network to reflect academic norms and ideas. Security blind spots become built in.
Part 3	ARPANET users *coshape/reconstitute* the meaning of the network by adopting new applications and usage scenarios. ARPANET meaning changes to being Information and Communication Technology.
Part 4	Open, scalable protocol design and convincing usage scenarios *enable* mass diffusion of ARPANET through ARPA research sites.
Context	Beginning of Personal Computer revolution & internetworking.
Part 5	Kahn and Cerf *design* TCP/IP protocol in a path-dependent fashion. They embed similar norms into the protocol and maximize decentralization of control.
Part 6	Computer industry and more NSF research sites *adopt* TCP/IP because of its openness, scalability and open-source features, making it the *dominant* design and *enabling* further mass diffusion (1980s).
Part 7	WWW reifies Internet norms, makes Internet easier to use, increases its appeal and thus enables world-wide diffusion beyond the academic sphere (1991).
Outcome	Successful mass diffusion of the Internet.

One of the curious facts of the Internet is that decisions that were made in the late 1960s have implications today. Arguably, the decision to decentralize power and control over the network could be interpreted as an instance of Winner's politics of artifacts because it is the primary point of contestation between cyber-realists and cyber-utopians (see chap. 2.3.3 The Politics of Technology Debate). The fact that the Internet cannot be controlled by a single actor is the primary motivator for cyber-realists to adopt censorship or surveillance legislation, trying to reestablish state-control over this medium. This happens because of security reasons, because it also enables malign usage which was not

anticipated during the construction. The lack of control enabled the user-struggle to defend "their" cyber-space against state encroachment, which will be the topic of the next chapter.

4.2 The Evolution of Cyber-Utopianism

"On the Internet, nobody knows you are a dog."
The New Yorker, July 5, 1993

This famous quote from a comic strip in the New Yorker can be described as a central metaphor or cultural meme for the Internet in the 1990s. Not only was it widely received and influential, it also shaped the initial perspective that the Internet is an intransparent space, a so-called *cyber*-space that enabled online conversations with total strangers that one had never met before. Your chat partner could be a dog because you could not see him or her. The Internet was seen as an anonymous space. That we still use the peculiar term "cyberspace" is no accident, but the result of a somewhat intentional framing effort by the Internet's first users. This chapter changes the perspective from the goal-oriented construction of the Internet to early usage, particularly during the 1980s and early 1990s. It introduces the early users and thus impact constituencies, sometimes called the "digital natives" and their paradigm in respect to the Internet, called cyber-utopianism. It focuses more on the reception and interpretation of the technology in wider social contexts. A disclaimer upfront: Internet utopianism is not advocated by a coherent, homogeneous group (in contrast to the engineering community or cyber-realism). The paradigm has (at least) two origin stories that began to overlap in the 1970s. One developed out of the practice of using early computers in the 1950s. A utopian version of what computers could potentially do was first conceived by a small elite of mostly well-educated, middle-aged, white males at American universities we now call hackers.

The other utopian vision developed out of cybernetics in the early 1950s and like its spiritual predecessor, attracted a wide variety of advocates, from left-wing critical theorists, hippies from the American counter-culture, but also academics from sociology, media-studies, digital-humanities, history or even futurology. Utopianism also is not a mode of self-description of a social group, but a discursive label attached by out-group actors, sometimes even to discredit a certain naivety. As such, the boundaries of the paradigm and those who carry it are not completely clear. The combining element is that these diverse actors shared similar antagonisms, the fear of state encroachment and a positive notion of technology that could be used for human enhancement. They also developed similar norm-clusters, predominantly that the Internet should be governed in a self-regulated way by its "inhabitants". They favored strong libertarianism and free speech and argued that the Internet should be decentralized to avoid central control or surveillance by one single authority.

Cyber-utopianism is deduced from academic literature on the matter and other data sources such as influential books or online articles. This is due to the fact that the field is so diverse, but at the same time well studied within digital humanities or Internet studies (Dutton, 2013b). Due to practical constraints, this is going to be a shorter chapter. Its main contribution is to trace the meaning construction of the Internet, understood as a cyberspace in the early days of its diffusion. As such, this chapter presents the utopian part of the thesis's title and the first part of the norm-change this thesis is about.

It shows how cyber-utopian norms emerged out of two distinct sets of ideas, the hacker (see chap. 4.2.1 Background: Hacker-ethic and Technical Optimism (1960s)) and counter culture that were combined by a central norm entrepreneur called Stewart Brand (see chap. 4.2.2 Ideas: Stewart Brand and the Counter-culture (1960-1970)). Brand also developed two important technical artifacts that played a major role in the social construction of cyberspace (see chap. 4.2.4 Artifact: The WELL and the Social Construction of Cyberspace (1980-1990)). Utopian ideas and norms developed within the usage context of these artifacts and became dominant in regulating state behavior towards the Internet in the 1990s. The general argument of this chapter is that the digital natives adopted a positive vision of technology out of their usage practice and could spread their vision, their technological frames, to a wider discourse once the Internet with the WWW started to diffuse worldwide in 1992 (see chap. 4.2.5 Framing Cyberspace as the Electronic Frontier (1990s)). Their cyber-utopian ideas and norms what the Internet should be and how it should be governed were picked up by the media, economic actors (see chap. 4.2.6 The Californian Ideology (1995-2001)) and ultimately by the Clinton/Gore administration, which the next major chapter is about (see chap. 4.3 Cyber-Utopian Liberalism and the Politics of Cyberspace (1990-2000)). Cyber-utopianism was highly influential during the 1990s, mostly because of its optimist narrative and the economic investment boom, called the dot-com bubble, that followed. The crash of the dot-com bubble is a critical juncture, or a shock for cyber-utopianism (see chap. 4.2.7 Junctures: Dot-com Bubble (2000-2001)) that disenchanted some of its ideas and contested its norms. This was not completely unexpected if one summarizes the key ideas and norms of this paradigm, which happens after the description of the general utopian storyline (see chap. 4.2.8 Norms and Key Ideas of Cyber-Utopianism). In this chapter, I include the theoretical findings and present an overview of the paradigm with its norm-cluster. Afterwards, a critical discussion of the shortcomings of utopianism follows (see chap. 4.2.9 Critical Analysis & Blind Spots of Cyber-Utopianism).

The next chapter will introduce a bit of background regarding the practice of using computers in the early days, which is important to understand the development of technological optimism and utopism.

4.2.1 Background: Hacker-ethic and Technical Optimism (1960s)

The history of information communication technologies began in the military context of World War 2. Computers, or mainframes, were huge and expensive machines (between $500.000 and several million dollars) that filled up special, air-conditioned rooms (Pfaffenberger, 1988). Only a few universities and research centers could afford them and were often dependent on funding from the Defense Department. In the 1950s, the practice of computing basically meant "doing arithmetic fast" (Hafner & Lyon, 1998, p. 24). Users had to learn to use each machine and operating commands individually. Because of these factors, the practice of computing was limited to a small science elite, a computer priesthood within science and/or the military (Levy, 2010, p. chap. 1). Tim Berners-Lee remembered: "a computer was still a sort of shrine to which scientists and engineers made a pilgrimage" (Berners-Lee, 2000, p. 8). Social norms were enforced within this context, for example that it was only appropriate for the trained elite to touch, modify or repair the computer. Games and personal use were a taboo. Access to these devices was highly restricted and controlled by central authorities. In theoretical terms, the use of the computers was highly centralized: "mainframe computers emerged as the symbol par excellence of centralized corporate authority, a way of gaining enhanced managerial control over the minute details of the organization's performance" (Pfaffenberger, 1988, p. 42). This began to change in the 1950s when computers began to become powerful enough to allow time-sharing, i.e. the parallel use of computing power between different users at the same time. This made computers interactive and transcended the meaning of computers as mere number crunchers and framed them to supporters of the thought process, as social machines (Naughton, 1999, pp. 73-76). This was a radical thought at a time where most people thought computers were big calculators and when only around 5371 computers existed in the US (Rid, 2016, p. 117).

This new collaborative mode of computing facilitated the creation of a special epistemic community of computer users and led to the creation of new ideas and norms of computing. According to Levy, the Massachusetts Institute of Technology (MIT) in the late 1950s was the place where a new hacker-culture evolved. In his influential book, Levy (Levy, 2010), describes the struggle of young IT-students, tech-aficionados and tinkerers from the Tech Model Railroad Club at MIT to get access to the universities' mainframe

computers, often during night-times (counter-appropriation). A "hack" was MIT lingo for "elaborate college pranks that MIT students would regularly devise, such as covering the dome that overlooked the campus with reflecting foil" (Levy, 2010, p. chap.1). Ethnographer Gabriella Coleman describes hacking as "turning a system against itself […] the process of using existing code, comments, and technology for more than what their original authors intended […] Hacking is where craft and craftiness converge" (Coleman, 2013, p. 98). Nowadays, the term hacking is connoted mostly negatively (Vegh, 2002). If one types "hacker" into a Google image search, one sees criminals wearing ski-masks doing illicit activities in front of a computer. The criminalization of hacking has to do with the securitization of cyberspace (Coleman, 2014), as will be introduced in later chapters (see chap. 4.2.5 Framing Cyberspace as the Electronic Frontier (1990s)). Originally, hacking described a playful, artful and positive disposition towards technology characterized by exploration and curiosity. It shares similarities with the practice of engineering and science, namely solving complex problems. In this context, the word "hack" meant a clever, not obvious solution to a problem in computing. The main purpose of hacking was curiosity and the joy coming from great solutions. Levy even argues that hacking is an end in itself which often serves no obvious function except testing the limits and possibilities of a system (Levy, 2010, p. chap.6). Repurposing a mainframe computer designed for being a machine to support military action into a device for fun, for example by playing Chess or games like "Space War" (1962), were early examples of a "great hack", according to Stewart Brand (Brand, 1972). The playful and positive attitude towards computers and technology in general led to the realization that they could be used for more than just waging war. In theoretical terms, counter-signification and appropriation of technology lies at the core of hacking (see chap. 2.3.6 Combining the Frameworks).

The practice of hacking and writing software code in this special context of mainframe computing created a special *ethos* and gave computing a new meaning and created a particular computing-paradigm with its own social norms. According to Levy, this hacker paradigm had the following norms.

> "Access to computers and anything which might teach you something about the way the world works should be unlimited and total. Always yield to the Hands-On Imperative! […] All information should be free. […] Mistrust Authority Promote Decentralization. […] Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position. […] You can create art and beauty on a computer. […] Computers can change your life for the better" (Levy, 2010, p. chap.2).

Let's decipher these. The norm that "*access to technology and computers should be open and unlimited for everyone"* stems directly from the highly-centralized context of mainframe-computing. Demanding open access to these systems was an act of political resistance and an attempt in reconstituting computing (Pfaffenberger, 1988). Hackers and computer programmers in general internalized the cybernetic argument that computer programs could do things that humans could not, like solving complex mathematical formulas or storing human knowledge. They could be used for *a greater good,* for example human development and the pursuit of knowledge, as for example ARPA's J.C.R. Licklider wrote (Licklider, 1990). As such, writing software code represented the increase of human knowledge and capacities which ultimately was seen a form of *human empowerment*. For that to happen, access to a system was imperative.

The dictum that "*information has to be free"* directly stems from the access requirement. Hacking is a practice of obtaining information about the inner workings of a system, both its hardware and software. Prohibiting that access makes hacking impossible (Coleman, 2013, p. 68). *Sharing of information* is quite crucial for the practice of complex computer programming in general. Hackers and programmers need to share information of how to solve highly specialized problems or how to write complex algorithms. Sharing this knowledge with peers is a matter of efficiency (writing code that another one has already written is a waste of time) and general creativity: computer programs often built upon the code of other programmers (Levy, 2010, p. chap.2). Programmers learn from each other by looking into each other's source code. Sharing either partial solutions, or even complete programs (or documentation of the source code) with others for free is a practice with many advantages.

Out of the hacking practice, a *sharing norm* evolved: "Code passed back and forth between the members of the community – if you made an improvement you were expected to submit your code to the community of developers. To withhold code was considered gauche – after all, you benefited from the work of your friends, you should return the favor" (Friedman, 2005, p. 106). This fosters collaboration and leads to the creation of a community based on the idea that sharing computer source code is for the greater good.

This sense of community also creates a *mistrust of authority trying to restrict access and information*. Centralized bureaucracies with the power to restrict usage of technology where the natural antagonism for the hacking community. Conservative corporations such as IBM, universities or the military held the monopoly of computing in the 1950s. Turner argues that the late 1950s were an era of mistrust in hierarchized systems of authority and the military-industrial complex that even President Eisenhower articulated in his 1961

farewell address (Turner, 2006, p. 42). The hacker ethos argued for decentralizing access to computers. This has to do with the modus-operandi of writing software code in a collaborative fashion based on the idea of a *meritocracy* that judges the individual skill of hackers based on the merits – the software code produced. Like science, programming is first and foremost a *peer-to-peer collaboration*. It is egalitarian in the sense that everyone can write code and the technical outcome, the hack, is the only criterion that counts (at least idealistically). From this conception of community and selfhood follows a deep mistrust of authority and hierarchical systems that do not judge individuals based on merit, but on arbitrary, seemingly non-rational criteria such as race or degrees.

Finally, hacking is a prime example of technological optimism and an early version of cyber-utopianism. From all these norms derives the thought that computers and *technology can change the life of the hacker, and potentially everyone, for the better*. This is an affirmation of J.C.R. Licklider's (Licklider, 1990) *empowerment thesis* or that computers and mankind can form a symbiosis. The same prognostic frame reappeared in the 1990s with the Internet, which was said to empower the lone individual vis-à-vis centralized authorities such as the military or the state (see chap. 4.2.5 Framing Cyberspace as the Electronic Frontier (1990s)). But software would not just empower the individual, it was also a form of *self-expression*. Hackers argued that the mind of the hacker would live in its source code just like the spirit of Beethoven would live in his sonatas (Levy, 2010, p. chap. 6). This is the reason why many in the free software movement treat code as an expression of free speech and strongly advocate against intellectual property and Internet censorship.[57] At the same time, it is a reference to the cybernetic idea that computers and human minds are both information machines that operate according to similar principles. As such, hacking is a highly idealistic ethic similar to Weber's protestant work ethic (Himanen, 2001) but more focused on the benefits of technology. It projects the utopian idea that everyone potentially can become a hacker, and if everyone would be, the world would be a better place.

How did this hacker ethic, the early version of cyber-utopianism, diffuse and gain more supporters? It is important to stress that this hacker ethic developed at multiple computer sites in the US in the 1950s. The beginning diffusion of the computer created similar working environments with similar constraints at other locations. Levy argues that the

[57] The founder of the Free Software Foundation, and MIT hacker Richard Stallman formalized this idea in the GNU manifesto of 1985. Stallman argues: "When we call software "free," we mean that it respects the users' essential freedoms: the freedom to run it, to study and change it, and to redistribute copies with or without changes. This is a matter of freedom, not price, so think of "free speech," not "free beer " (Stallman, 1985). "The Golden Rule requires that if I like a program I must share it with other people who like it" (Stallman, 1985). Out of this idea developed the General Public License, an alternative to copyright.

hacker ethic and its modality of software production spread together with software they created and distributed to peers (Levy, 2010, p. chap. 6). By sharing programs, hackers indirectly recruited other peers to adhere to the same social norms of sharing, resembling the mechanism of a gift economy.[58] Especially video games like Space War, had a wide appeal and thus attracted more users to computers and potentially exposed them to other hackers and their ideas (Brand, 1972). This is an important theoretical argument: hacking norms developed out of the practice of computing in this special historical configuration. Hacker norms became embedded in technical artifacts – computer code and software – and spread together with software. Social actor-networks played a special role here (Latour, 2005b). Hacking norms also spread because of networking actors, acting as norm-entrepreneurs: hackers that left MIT and went to other universities, held workshops or conferences or started to publish computer magazines, presented the idea of hacking to like-minded groups. With the invention of computer networks such as ARPANET, another channel for paradigm and software diffusion was created. Stanford Research Institute, one of the first host-sites of the ARPANET, was another prime spot for the development of the early hacking culture and thus it is no accident that the design of ARPANET reflects some of the ideals of the hacker-ethic (see chap. 4.1.2.2 Norms Shaping the Construction of ARPANET). Lastly, those university students who first engaged in hacking in the late 50s, later often became leaders of the revolution of the personal computer in the early 1970s and 1980s (see chap. 4.2.3 Artifact: Democratizing Technology (1970-1980)). They thereby transported the ideas of their youth into future business models and products like the personal computer. Physical publications, such as special magazines, played an important role in diffusing techno-optimist ideas, leading to the creation of a cyber-utopian paradigm, as the next chapter will show.

4.2.2 Ideas: Stewart Brand and the Counter-culture (1960-1970)

The hacker community set the foundation of technological optimism at a time when computers were widely unknown to the public. But utopianism had another source in the social movements of the 1960s that formed around Berkeley, the same Californian region where ARPANET was conceived a few years later.

I cannot outline all the motivations for these diverse movements in high detail but the Vietnam War and the fear of nuclear annihilation, especially in the context of the Cuban

[58] Originally developed by Marcel Mauss, the gift creates permanent social structures of exchange because it generates obligations to return the favor (Mauss, 1990).

missile crisis of 1963, were important factors.[59] For the New Left, technology had a negative meaning. They saw computers as dehumanizing technologies, instances of a centralized bureaucracy and ultimately as a symbol of the Vietnam War which they opposed (Turner, 2006, p. 2).[60]

For the New Communalists or the *counterculture*, cybernetic ideas and utopianism had a special appeal. The two movements defined similar problems and had similar antagonisms – "militarism, racism, sexual discrimination, homophobia, mindless consumerism and pollution" (Barbrook & Cameron, 1996). The New Left engaged in the political struggle, changing politics from within, by joining parties or committees. The New Communalists and back-to-the-landers, in contrast, sought to change society by new modes of thinking and escapism. Consciousness and the individual mind became central concepts for their political struggle (Reich, 1971). Their strategy was to change the individual self and lifestyle locally, which over time would usher in social change globally. Their goal was to create and change a global consciousness. By creating new forms of living and social organization – self-sustained, agricultural communes – they tried to achieve this end. Hence, they turned away from politics to everything that changed the self: psycho-active drugs, music, transcendental art-performances but also extravagant academic concepts such as libertarianism, cybernetics or post-modernism (Turner, 2006, pp. 36-61).

Especially cybernetics had a special appeal to them. According to Thomas Rid, a positive vision of the future based on machine automation became popular in the 1960s, mostly among academic and literary circles (Rid, 2016, pp. 133-134). Sociologists started to theorize about an "information society" that, in the near future, would replace the industrial mode of production. Machine automation would lead to *a new industrial revolution that would lead to the abolishment of human labor*. Machines would take over most monotone functions which would produce more economic growth and reduce unemployment. This resembled Karl Marx' idea who argued a century before that because of automatization, mankind could focus on its own intellectual development. Instead of an agricultural there would be "cybercultural revolution" (Rid, 2016, pp. 133-134).

[59] Misiroglu lists several hundred social movements from that time period in her encyclopedia (Misiroglu, 2015).

[60] Turner gives a splendid overview over academic thinking that diagnosed an increasing centralization and hierarchization of society, where means of information and power were centralized among elites. The ideal type of this mode of governance would be the military with its strict hierarchy. This "critique could be heard echoing throughout the 1960s in works as varied as Jacques Ellul's The Technological Society (1964), John Kenneth Galbraith's The New Industrial State (1967), Herbert Marcuse's One-Dimensional Man (1964), Lewis Mumford's The Myth of the Machine (1967), Theodore Roszak's The Making of a Counterculture (1969), and Charles Reich's The Greening of America (1970)" (Turner, 2006, p. 28).

In popular culture, the *cyborg* – the machine-enhanced human – became a popular concept (Vydas, 1965). It was believed that with mechanical modification, human limitations could be overcome, a process that might lead to a self-controlled evolution. The cyborg transcended the boundaries of what it meant to be human, the borders between the consciousness/simulation and the natural/artificial (Haraway, 1983). It was also the age of AI research – artificial intelligence – at many universities like Stanford, which basically fueled the same *cyber-mythos*: in a not so distant future, intelligent machines will take over control (Hope, 2015). For believers, it was *not a question of if, but when*. Cybernetics was the new avant-garde of the time. Herbert Simon argued in 1965: "machines will be capable, within 20 years, of doing any work a man can do" (Simon, 1965). This powerful prediction frame had been uttered repeatedly since the inception of AI research in 1957 and can be even seen today in debates about "Big Data" and "deep learning" (Najafabadi et al., 2015). This indicates a high narrative fidelity and commensurability that only increased the attractiveness of cybernetics as a form of individual transcendence and as such it was appealing for the counter-culture and compatible with their mind set.

In 1964, famous media theorist Marshall McLuhan coined two concepts that deeply influenced Internet utopianism of the 1990s: the concept of *new media with socializing effects* and that of the *global village,* both of which would be facilitated through cybernetics (see chap. 4.2.8 Norms and Key Ideas of Cyber-Utopianism). For McLuhan, cybernetics allowed the re-tribalization of society into tribal forms of organization. Tribalism resonated well with the New Communalists and gave their ideas academic credibility. At the same time, *new media* (cable TV) made people more aware of what happened at the other side of the globe. Electronic technology allowed to "extend our central nervous system itself in a global space, *abolishing both space and time*" (McLuhan, 1964), acting as extensions of man, as the title of his famous publication indicated.[61] For McLuhan, technology offered the possibility of human transformation on a global scale. Whereas the industrial revolution fragmented and alienated mankind, the age of cybernetics would interconnect humans (Rid, 2016, p. 141). This, of course was highly coherent with counter-cultural thinking.

Those academic publications were not necessarily known to a wider, non-academic or even hacker audience. Stewart Brand, a hippie entrepreneur, made techno-optimist and cybernetic ideas available to a wider audience. In his excellent study, Turner calls Brand a central networking hub, a broker connecting highly diverse communities together: the young computer-science community (consisting of students, the hacker community and

[61] My highlights in *italics.*

later ARPANET users), social sciences (cybernetics, sociology and particularly systems theory), Protohippies and New Communalists, the San Francisco psychedelic scene, technologists (high tech-companies and industry), journalists and even parts of the government (Turner, 2006, p. 5). Brand traversed between different communities in the San Francisco Bay area and created two particular technological artifacts that fostered collaboration between these communities: The Whole Earth Catalog[62] (published between 1968 and 1972) and later, the first electronic social network, the Whole Earth 'Lectronic Link or the WELL (1985-present). Both had an enormous intellectual impact across Silicon Valley. The Catalog won the National Book Award in 1971 and sold over a million copies (Turner, 2006, p. 80).

Brand conceived the Catalog as an "information technology" at a time before the Internet existed. Brand defined the design principles of this artifact as:

> "We are as gods and might as well get good at it. So far, remotely done power and glory—as via government, big business, formal education, church—has [sic] succeeded to the point where gross defects obscure actual gains. In response to this dilemma and to these gains a realm of intimate, personal power is developing—power of the individual to conduct his own education, find his own inspiration, shape his own environment, and share his adventure with whoever is interested. Tools that aid this process are sought and promoted by the WHOLE EARTH CATALOG" (Brand, 1968).

Based on the countercultural narrative, hierarchized mass bureaucracies and the establishment were presented as the *problem* and the answer to this problem was *individual empowerment,* education, self-reliance and a do-it-yourself-mentality. "Ask not what your country can do for you. Do it yourself," we said, happily perverting J.F.K.'s Inaugural exhortation" Brand once said (Brand, 1995). The answer to a centralized bureaucracy was *decentralization*, the creation of multiple power centers and thus the flattening of hierarchies in more egalitarian forms of governance, reflecting the notion of liberal-individualism and self-reliance of the hacker ethic and the anarchist spirit of the commune.

A core cybernetic idea promoted by Brand was that *technologies can improve individual life,* a concept that later evolved into the Californian Ideology of companies like Google and Apple (Barbrook & Cameron, 1996). Former Apple CEO Steve Jobs, who also studied at Berkeley around that time, was an avid reader and described the Catalog as "a Bible of my generation […] like Google in paperback form, 35 years before Google came along. It was idealistic and overflowing with neat tools and great notions" (Jobs, 2005). Tim Berners-Lee argued that it was "the first book that made all this Internet stuff

[62] Henceforth "the Catalog".

accessible to the public" (Berners-Lee, 2000, p. 76). The catalog's function was to provide its readers with information how to manage and enhance their (communal) life with technology. Technology was understood broadly, meaning ideas, publications and techniques, but also technical artifacts such as computers which were reviewed (even by the users) and all of which could be ordered within catalog (see chap. 2.3.2 Defining Technology). Technology had the function of personal enhancement, thus artifacts were positively reframed as *deeply personal, even spiritual devices*. This explains why cybernetic trans-humanism had an appeal in the counter culture.

The catalog featured many cybernetic publications and included a feedback mechanism for readers to share their experiences, announce communal projects and give reviews about technologies, reflecting the idea of peer-to-peer collaboration (Brand, 1968). The catalog did not just depict a personal, rebellious image of technology but also of the reader itself. In other words, it constructed the user or reader identity, as a "cowboy nomad figure" or a "Longhunter",[63] pretty similar to native Indians, which were idealized by New Communalists because of their tribal lifestyle (Turner, 2006, pp. 86-91).[64] These actors were presented as being on some kind of "personal frontier" in an "outlaw area" or "ungoverned space". The notion of the *frontier* and the *separate, ungoverned and uncontrolled space* featured prominently in the intellectual concepts of New Communalists of the time and later inspired the concept of cyberspace as an "electronic frontier", the hacker or cyber-punk as the "digital native" resisting the hierarchized mass bureaucracy (see chap. 4.2.5 Framing Cyberspace as the Electronic Frontier (1990s)).

The catalog featured a range of topics and concepts like peer-to-peer collaboration, the idea of decentralization or flattening of hierarchies and the idea of information-sharing and dissemination for human development that resonated both within the American counter culture, but also with the emerging digital community of hackers and tech-enthusiasts. Through the Catalog and its feedback or forum-function, very disparate groups engaged in social and ideational exchange. This led to the fusion of counter-cultural, back-to-the-land ideas with techno-optimism of the young computer culture. Thus, the separate causal paths, the hacker ethic and the counterculture were added together to from one causal pathway into the future. The outcome of these equifinality factors was a coherent paradigm.

[63] An explorer who roams the 18th century frontier for long times.
[64] The readers of the Catalog where mostly white, middle-class males with higher education and native Indians or women did not play any major role in this community (Turner, 2006, p. 97).

> "Together, the creators and readers of the Whole Earth Catalog helped to synthesize a vision of technology as a countercultural force that would shape public understandings of computing and other machines long after the social movements of the 1960s had faded from view" […] "In this way ideas born within Whole Earth–derived network forums became key frames through which both public and professional technologists sought to comprehend the potential social impact of information and information technologies. Over time, the network's members and forums helped redefine the microcomputer as a "personal" machine, computer communication networks as "virtual communities," and cyberspace itself as the digital equivalent of the western landscape into which so many communards set forth in the late 1960s, the "electronic frontier" (Turner, 2006, p. 6).

The Catalog acted as carrier medium and helped to spread cybernetic ideas but also technical optimism and utopianism and synthesized these into a new computing paradigm. The centerpiece of almost every utopia is a vision of a future society that had overcome problems and issue of the present (Levitas, 2010, p. 1). It is therefore no surprise that this utopianism of the counterculture and hackers featured concepts that stood in opposition to the perceived problems of the time: a hierarchized, inegalitarian and even oppressive society (in terms of minority rights) of the 1950s living under the constant threat of nuclear annihilation. What is new about cyber-utopianism is that the solutions to these problems were perceived to be digital technologies. This paradigm reframed the meaning of digital technology from anonymous machines of centralized authorities into decentralized, personal artifacts for individual empowerment and enhancement. This inspired the idea of the personal computer, which will be introduced in the next chapter.

4.2.3 Artifact: Democratizing Technology (1970-1980)

The story of how hierarchized mainframe computers became a *personal* computer has been told in detail elsewhere (Pfaffenberger, 1988; Schmidt, 1997; Ensmenger, 2010). I will only give a cursory overview. The argument of this chapter is that cyber-utopian ideas, originating in the hacker ethic and the spirit of the counter-culture became embedded in the personal computer, which created the myth of personalized technology of individual empowerment and democratization. In the early 1990s, the very same ideas were attached to the Internet by cyber-utopians as well, representing a genealogy or evolution of ideas.

For most people in the 1970s, a computer represented a "relentless, peremptory, repetitive, invariable, monotonous, inexorable, implacable, ruthless, inhuman, dehumanizing impersonal Juggernaut" (Nelson, 1974). Several computer aficionados attempted to change this image because for them, computers represented a means of empowerment. In the Silicon Valley at the time, various grass-roots initiatives like "Community Memory" or the "Peoples Computer Company", cyber-utopian advocates and

norm-entrepreneurs so to speak, began initiatives and publications to educate a wider audience about the benefits of computers. The Peoples Computer Company, inspired by the Whole Earth Catalog both in terms of design and message, issued a publication in 1972 arguing in capital letters:

> "COMPUTERS ARE MOSTLY USED AGAINST PEOPLE INSTEAD OF FOR PEOPLE USED TO CONTROL PEOPLE INSTEAD OF TO FREE THEM. TIME TO CHANGE ALL THAT WE NEED A... PEOPLE'S COMPUTER COMPANY" (Peoples Computer Company, 1972).

This represents a diagnostic frame. Ted Nelson, one famous hacker of the time published a widely-regarded book *Computers lib* that had similar ambitions: "This book is for personal freedom and against restriction and coercion. A chant you can take to the streets. Computer power to the people! Down with the Cybercrud! (Nelson, 1974).[65] Their vision was to *democratize computer usage* (Pfaffenberger, 1988). In line with the hacker ethic, they argued that if more people would use electronic technology and would see their benefits, this would serve a greater good. In their publications, they argued that new *technology could enhance participation in the democratic process*, thus outlining one of the earliest visions of something like electronic voting or what during the 1990s would be called "e-democracy" (see chap. 4.2.8 Norms and Key Ideas of Cyber-Utopianism). They argued that computers could be tools for political networking of advocacy groups, exchange of political ideas and thus were inherently political. Thus, these publications and arguments represent motivational frames to help the counter-culture to engage with computers and to deconstruct their prior negative attitude towards computers (see chap. 2.2.2 Framing). At the same time this represents a counter-signification strategy aiming to change the meaning of computers.

The idea to *democratize computers* was institutionalized with the Home Brew Computer Club, formed in 1975 in the Silicon Valley. It was a club of technology aficionados, hackers, professionals (Stanford & ARPANET staff) from IT companies (like Xerox PARC who also called for "shift in our thinking about what is a computer: we were to scrap the bulky mainframes that filled rooms and imagine a computer on a desk" (Mosco, 2004, p. 21). The founder, Fred Moore stated that the goal of the club was "information sharing" based on norms of peer-to-peer collaboration and meritocracy (Levy, 1993). Out of the home-brew community developed the first truly personal computers, most prominently the Apple 1 and Apple 2 (1977), the computers that ushered in the *Personal Computer or digital revolution*. Steve Wozniak and Steve Jobs, cofounders

[65] I was unable to define the term cybercrud.

of Apple, were home-brew regulars and also hackers, engaging in the widespread practice of "blue box" phone phreaking, a hacking technique of hijacking the dial-tones of the phone network to make free of charge calls (Brand, 1995).

Inspired by countercultural ideas and their personal fascination with technology, they too saw the computer as a means of empowerment of the masses and social change. Stewart Brand once described the computer as the new LSD, a technology that could open minds (Turner, 2006, p. 139). These ideas (and the desire for profit) led to the construction of the Apple computer, a completely open system that allowed tinkering and modification. In other words, the norms and ideas of the counter culture and hacking became embedded in the technical artifact. Counter-artifacts like Apple 1 and 2 and other early personal computers (like the TRS-80 or the Commodore 64) of that era reconstituted the mainframe computer and transported the ideals and norms of the hacker ethic, presenting it to a wider audience.

In 1983, roughly 10 percent of the American households had a PC (see Quantifying the Internet and the Digital Revolution) and Time Magazine labeled the PC the "Machine of the Year" (TIME Magazine, 1983). According to Friedman, the PC gave ordinary citizens the tools that had been monopolized by large companies and the government before, like spreadsheets for individual investment, electronic banking and the creation of digital content such as "words, music, numeric data, maps, photographs and eventually voice and video" (Friedman, 2005, p. 56).

Of course, with the mainstream diffusion of the PC came the "economization of the counter culture" (Mosco, 2004, p. 42). The original hacker spirit got blurred because suddenly these companies had to pursue business interests (thus keeping their source code secret or proprietary). In 1984, when Apple released its most famous computer, the Macintosh, they utilized the democratizing narrative as a PR strategy to increase sales (Pfaffenberger, 1988). The Macintosh was marketed as a people's computer, with an easy-to-use graphical interface with content-windows (that are still used today) that could be used potentially by everyone, even without programming skills. The award-winning "1984" commercial depicted an Orwellian Big brother, a symbol for IBM and centralized computing, speaking on a big screen to mindless, enslaved workers. The screen got smashed by a female athlete (representing Apple), thus liberating the workers from their indoctrination. The narrative or myth of the democratizing potential of the personal computer suddenly became mainstream during the Super Bowl in 1984, with millions of watchers and became also part of the Apple brand with its "think different" marketing campaign (Berger, 2008, pp. 54-57).

The goal of this small chapter was to shed light on the origin of one key-frame of cyber-utopianism, namely the idea that technology can be a democratic and personal tool. Based on the post-structionalist insight that matter does not carry the means of its own representation, it is farfetched to assume that a computer could inherently bring democracy (the Soviet Union, too, used computers and was the very opposite of a democracy). The frame that computers could empower individuals and thus transform the social world had to be socially constructed and this is exactly what the Whole Earth Catalog and the early hacker community did. They were meaning managers, constructing the meaning of the technical artifact, but also the identity of its users and successfully so. This utopian technological frame resurfaced in 1994, when Vice President Al Gore argued that the Internet would be a tool to spread democracy worldwide (see chap. 4.3.3.2 Global Framing of the Internet). In other words, the same frame was attached to the Internet. The most recent instance of this idea was the Arab Spring in 2011, where it was argued that social networks like Twitter allow for political collaboration and civic unrest (Stepanova, 2011). Critics could now argue that the computer is different from the Internet. The bridge between the two was the WELL, the first social network, introduced in the next chapter.

4.2.4 Artifact: The WELL and the Social Construction of Cyberspace (1980-1990)

The Whole Earth Catalog was sold until 1972 and inspired a wide range of new publications addressing similar cyber-cultural topics like *Mondo 2000* and Brand's follow-up project *CoEvolution Quarterly* (Rid, 2016, p. 279). Science Fiction books picked up cybernetic ideas and themes of the counter-culture in a genre called *cyber-punk*. This mix of concepts enriched cyber-utopianism and gave it a new direction. It helped to construct a vision of a separate, virtual space, the cyberspace, which in the 1990s became a key-frame for explaining the Internet.

Around 1983, Brand came in contact with emerging online teleconferencing systems that had been spawning after the ARPANET presentation in 1972 (see chap. 4.1.2.4 Co-shaping the Meaning of Networks). These systems allowed real-time interaction, feedback and thus potentially virtual hacker conferences, collaboration, sharing of ideas and free information with a computer, independent of location. Brand teamed up with Larry Brilliant, an expert in the new emerging market of computer-networking, to construct the Whole Earth 'Lectronic Link henceforth "the WELL", one of the first digital social networks, launched in 1985 (Ryan, 2013, p. 82). With a dial-up connection and a PC one could login into the WELL, which basically resembled a BBS (Bulletin Board System)

messaging board or early online forum. In technical terms, BBS boards are applications that run on top of TCP/IP.

The WELL's black and white login screen (computers at the time often could only depict up to 4 colors) said: "You own your own words", a reminder of the *norms of free speech and content-ownership* but also of social responsibility. There, users could create forum-threats and discuss a wide array of topics, and share information freely among their digital peers. The technical artifact the WELL was a self-governed online commune, a creative network of thought (Rid, 2016, p. 240). Inspired by the Catalog and the hacker ethic, its design principles were:

> "That it be free. This was a goal, not a commitment. We knew it wouldn't be exactly free but it should be as free (cheap) as we could make it […] It should be profit making […] It would be an open-ended universe […] It would be self-governing […] It would be a self-designing experiment […] The early users were to design the system for later users. The usage of the system would co-evolve with the system as it was built […] It would be a community, one that reflected the nature of Whole Earth publications" (Turner, 2006, p. 143).

It would be *self-governing* in the sense that no administrators, as it would become a common practice during the 1990s, would edit or censor the content. As such, it decentralized authority to the users who were responsible for maintaining ethics. Like in modern social networks, users could hide content they did not want to see. Fred Turner describes the governing mechanism as the "Communalist preference for nonhierarchical forms of social organization with a cybernetic vision of control" (Turner, 2006, p. 145). For Brand, the WELL was a revival of the failed back-to-the-land movement of the 1970s, reviving the dream of a shared consciousness, but this time digital. The idea that different users from all over the US could meet online and discuss their shared interest was unheard of in the 1980s and even throughout the early 1990s. It bridged long distances and made real-time communication possible. Physical distance and space suddenly did not seem to matter anymore. To be able to communicate with someone at the other end of the US had a profound impact on its users.

The WELL's user base was a knowledgeable, digital avant-garde of male and female [66] technology professionals, hackers, journalists and even writers and social scientists like Manuell Castells (who coined the term *network society*), Howard Rheingold (who developed the term *virtual community* based on his experience in the WELL) and John Perry Barlow, later founder of the Electronic Frontier Foundation or EFF (see chap. 4.2.5 Framing Cyberspace as the Electronic Frontier (1990s)). These were socialized with the

[66] It was estimated that 40% of the user base was female (Turner, 2006, p. 151).

WELL, drew their experience and knowledge of digital networking from it and later transported their experience into the 1990s discourse of the unfolding Internet. They acted as translators or sense-makers or as "bricoleur—someone who, following Lévi-Strauss's usage, pulls together the bits and pieces of technology's narratives, to fashion a mobilizing story for our time: what Nerone (1987) has called the heroic narrative with didactic effect" (Mosco, 2004, p. 36).[67] Narrative research teaches that the first story occupying a new social phenomenon often is the most important one because it sticks and thus shapes future narratives (Gadinger, Jarzebski, & Yildiz, 2014). The practice of using the WELL established new frames like the *virtual community*, the *electronic frontier,* the social *network* and *cyberspace,* which are key cyber-utopian frames that construct meaning of the Internet in the 1990s.

In 1987, Howard Rheingold firstly coined the term *virtual community* (Rheingold, 1993). Rheingold argued that the WELL made new forms of human interaction possible. Because the screen provided a visual abstraction, individuals could encounter each other without prejudice and in a non-random fashion: human interaction would be a conscious decision based on shared interest. The physical body, race and gender were said to become irrelevant in this digital meeting space. The limitations of the physical world (like geography or body features like skin color) suddenly did seem irrelevant (*disembodiment*) (Turner, 2006, pp. 159-161). In cyberspace, there were only digital subjects, representing a new form of being and thus creating a new type of identity. This refers to the co-shaping of subjectivity and objectivity, outlined in the theory chapter (see chap. 2.3.4 The Social Construction of Technology and its Critique). It is also in line with Kuhn's idea that paradigms address questions of ontology and epistemology (is the digital world different than the analog one?).

The WELL and other networks (like FIDONET, USENET that emerged around the same time) were a digital and non-physical location, a *separate space* inside the computer where one would meet (Naughton, 1999, p. 188). The dualism of *being online* and offline, in the "real" world, emerged. Being digital (Negroponte, 1995) was a new, almost transcendental form of existence. The WELL was also seen as a tool for changing consciousness. Love and friendship could become digital, without even meeting someone physically. This could create new forms of social relationships (Rheingold, 1993, p. Introduction). For Rheingold and others, another crucial factor with potential for social change was the possibility of *digital collaboration* with strangers for entertainment, personal development, work but also for political action.

[67] See for example Brand's article in Time Magazine explaining the Internet in 1995 (Brand, 1995).

The notion of a separate, digital space became appealing in the early 1980s, especially within the Sci-Fi genre called *cyber-punk*. In 1982, novelist Vernor Vinge described an imaginative future where people lived in a separate reality, a virtual space inside the computer and data networks. This alternative reality could be entered with computer terminals (Vinge, 2001). One year later, Sci-Fi author William Gibson coined the term *cyberspace,* at the time an essentially meaningless word that, according to him, was chosen just because it had a "nice ring to it" (Rid, 2016, p. 259). Gibson did not even own a computer at the time. Cyberspace thus was a signifier void of meaning. It had to be constructed and attached to it post-hoc. In 1984, Gibson published the cyber-punk novel *Neuromancer*, where *hackers,* the heroes in these stories, fought against an almighty, centralized and digital surveillance state. He describes cyberspace as:

> "A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts […] A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non space of the mind, clusters and constellations of data. Like city lights, receding […]" (Gibson, 1984).

It is important to note that cyberspace in many cyber-punk novels is described as a post-industrialized and technocratic landscape of either authoritarian or corporate control. The *antagonists* in these novels are either *Orwellian surveillance states* or *large, multinational corporations* that run societies through puppet-governments.[68] The narrative is pretty much in line with the techno-skepticism of the New Left, as described in a previous chapter (see chap. 4.2.3 Artifact: Democratizing Technology (1970-1980)). Pärna argues that the *cyberspace* neologism made the "Internet interesting and accessible to people who were not necessarily specialists in computing or engineering" and that cyber-punk ideas were a "way to understand new technologies and to appreciate their potential" (Pärna, 2010, p. 73). SciFi acted as an *imaginaire*, a lens through which non-tech experts could understand

[68] Interestingly, within this context, the term cyber-war first appeared in the public domain, which normally is attributed either to Jon Arquilla (Arquilla & Ronfeldt, 1993) or James der Derian (Der Derian, 1992), in the early 1990s. But it was already described in 1979 by cyber-utopian publication called Omni (Rid, 2016, p. 357). It outlined the idea of a cybernetic war of hardware against hardware with impacts on social life. The article predicted – two years after the release of the Apple-II computer – that in 1999 there would be 1 billion interconnected and palm-sized computers (that number actually would be reached around 2010). In this future, the computer would drive all kinds of weaponry like flying, autonomous robots shooting laser-guided missiles from the sky. A cybernetic war would mean the intrusion into these computer systems, a war characterized by speed, precision, automation and espionage. War would be automated and fought without humans (Ventre, 2016, p. 75). The computer would ultimately become a weapon of the military-industrial complex. For cyber-utopian believers, this dystopian vision of the future had to be prevented. Resisting the centralized state-war machinery was key. Using hacking tools and technology against them by making them available for everyone as means of self-defense, was the solution (Rid, 2016, p. 361).

the early Internet. It therefore had a high degree of narrative fidelity. More so, cyber-punk was consistent with counter-cultural and hacker ideas (internal credibility in terms of framing theory), so these ideas were commensurable with each other.

The cyberpunk literature reflected a general cultural trend of the 1980s that began to see the impacts of the computer revolution and realize potential dangers and negative effects (see chap. 4.4.1 Background: Growing Awareness of Computer Insecurity (1967 - 2011)). Cyber-utopian ideas even reached cinema with movies such as Tron (1982), Wargames (1983) or even Terminator (1984), that depicted the negative impact of a technology out of control. But for the early computer network avant-garde of the WELL, the positive effects still outweighed the negative ones. The hacker tended to defeat the adversary in these stories. These cyber-metaphors had a special appeal to readers of Whole Earth and the Hacking culture – because "computer scientists and technicians are almost universally science-fiction fans" (Brand, 1995) – and began to fill it with a more positive, utopian meaning. Networks like the WELL or early online-video games like Lucasfilm's Habitat (1986) resembled a graphic representation of data and computer networks. They visualized a different, positive cyberspace, not one of power and domination, but of peer-to-peer collaboration.

Arguing with discourse theory (2.2.1 Discursive Struggles between Paradigms), meanings attached to the WELL by the early user base (its advocates), were *projected* onto the empty signifier called *cyberspace*: real-time and increased speed of communication, the death of distances, the disembodiment of actors based on a perceived anonymity and the decentralized governing principle that gave the impression that centralized authorities like states are irrelevant. The same revolutionizing potential that was attached to the Personal Computer was attached to the Internet: that it would flatten hierarchies, lead to democratization, personal empowerment and to a social transformation. In other words, the WELL and other early social networks became representations or dominant meanings for the word cyberspace. More so, the term cyberspace with its cyber-utopian meaning became a metaphor for the Internet in general, reducing its interpretative flexibility. In theoretical terms, this framing process represents a counter signification by the early impact constituencies, the users of the Internet. This happened during the stabilization phase of TCP/IP and shows how the original artifact got decontextualized and how a new actor network of users established a new meaning (see chap. 2.3.5.2 Stabilization). Interestingly, this deviant use of the network indeed led to the creation and stabilization of a new paradigm, cyber-utopianism.

In sum, the WELL had two important cultural impacts. The first impact was technological. It was a prototype of early messaging boards that inspired a series of descendants and set a technological path that led from services like AOL, Geocities (1994), the Microsoft Network (1995) and MySpace (2003) to Facebook (2004). Nowadays, social networks are everywhere. The second impact was ideational and normative. It introduced a series of mental frames that became powerful in giving meaning to the early Internet. These norms and ideas developed out of the practice of using the WELL. The self-governing ethos with flat hierarchies was a common feature on messaging-boards during the 1990s. This meaning became dominant, reaching closure in the early 1990s with the public and political framing of early Internet advocates, which will be introduced in the next chapter.

4.2.5 Framing Cyberspace as the Electronic Frontier (1990s)

The early 1990s were a timeframe where many of the causal pathways depicted in this and the previous chapters converged (equifinality). Right around the same time when the World Wide Web was created, John Perry Barlow – counter culturalist, utopian, libertarian and singer of the Hippie band Grateful Dead – began to apply the cyberspace metaphor to the newly evolving landscape of internetworked computing. In June 1990, he founded the *Electronic Frontier Foundation* (EFF), together with two other utopians John Gilmore and Mitch Kapor (developer of the famous LOTUS spreadsheet software). The idea to create a digital rights/Internet activist NGO to promote civil liberties in cyberspace came from a WELL article called "Crime & Puzzlement" that Barlow wrote and that is regarded as the ideological founding document of the EFF. The aim was to "raise and disburse funds for education, lobbying, and litigation in the areas relating to digital speech and the extension of the Constitution into Cyberspace" (Barlow, 1990). It was written against the background of a perceived governmental encroachment onto cyberspace in terms of computer security legislation adopted in the mid 1980s (see chap. 4.4.1 Background: Growing Awareness of Computer Insecurity (1967 - 2011)) that led to more and more stories of arrests of young computer hackers. This represents the perceived problem and diagnostic frame for cyber-utopians.

In this article, Barlow adopted the narrative that the early Internet resembled the 19th century West. "It is vast, unmapped, culturally and legally ambiguous, verbally terse (unless you happen to be a court stenographer), hard to get around in, and up for grabs. Large institutions already claim to own the place, but most of the actual natives are solitary and independent […]" (Barlow, 1990). In other words, cyberspace resembled the *frontier*,

the Wild West and its native and rightful inhabitants. *The digital natives*, as they were called later (Prensky, 2001), were the users from the WELL and other communities. Cyberspace was depicted as a *lawless space*, where crackers (malign hackers who hack for personal gain) trespass onto other's territory (breaking into systems). The central government was framed as an *alien actor,* not a natural inhabitant of cyberspace, an "arriver".

Being a Libertarian, Barlow diagnosed a problem, central to the cyber-utopian paradigm: the *negative trajectory of the state entering cyberspace.* Crime on the Internet (the word cyber-crime was not yet invented) would become a welcome excuse for the government to exercise more and more control over cyberspace, for example in terms of censorship. What communists, terrorists or child abductors were in the past, would now become the hacker: "The perfect bogeyman for Modern Times is the Cyberpunk!"[69] Barlow argued that the digital natives must preempt this future scenario of state control by getting ahead of the curve. Being aware of the idea of path-dependency, Barlow argued that "any chaotic system, is highly sensitive to initial conditions", which means that the *digital natives must shape the initial conditions of cyberspace* by shaping the early public discourse about it (motivational frame). It is indeed an insight from Science and Technology Studies that the early meaning given to an artifact influences its further diffusion (Weyer et al., 1997). Barlow argued that the digital natives should become active explainers and meaning-managers: "If we come on as witches, they will burn us. If we volunteer to guide them gently into its new lands, the Virtual World might be a more amiable place for all of us than this one has been" (Barlow, 1990). Herein effectively lay a motivational frame to engage other digital natives to defend civil liberties by guiding and educating external actors. He also articulated the *norm of "inappropriateness of leaving our civil liberties to be defined by the technologically benighted"* (i.e. politicians). A common assumption of the time was that politicians simply did not understand the technology. The aim thus became to illuminate and educate the public and to protect the Internet from the ignorant state.

EFF's co-founder Mitch Kapor argued in a very similar article that cyberspace represented the early United States with settlers creating the republic. "Cyberspace seems to be shaping up exactly like Thomas Jefferson would have wanted: founded on the primacy of individual liberty and a commitment to pluralism, diversity, and community" (Kapor, 1993). This libertarian notion of a *Jeffersonian cyberspac*e, including the primacy

[69] Vegh has analyzed the criminalization of the hacker through popular discourses and finds that the post 9/11 counter-terrorism discourse changed the meaning of hacking from positive to negative (Vegh, 2002).

of the self-determined individual versus the colonializing state, shaped utopian thinking throughout the 1990s.

In the context of government attempts to regulate and control cyberspace with the Communication Decency Act (CDA) of 1996 (see chap. 4.3.5 Junctures: Policy Attempts to Control the Internet (1993-1996)), Barlow wrote the famous "Declaration of Independence of Cyberspace" which he published at the World Economic Forum in Davos 1996. There, he argued: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather" (Barlow, 1996). The counter-cultural *antagonism between the Longhunter, the digital native versus the hierarchized and industrialized government*, becomes immediately apparent. The declaration framed cyberspace as separate from state authority and control: "I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us" because "Cyberspace does not lie within your borders". This argument is based on the *globe-spanning and border-crossing* characteristics attributed to the decentralized network called the Internet (with its end-to-end principle). Barlow picked up the ideas of the ARPA engineers that the Internet was like a global commons, over which no single state authority *should* have control (see chap. 4.1.3.1 Artifact: Internet Protocols and Norms). The Internet is framed as an intangible thing, like air. It is framed to be a place of the mind, where matter is irrelevant (completely ignoring the physical attributes of the networking infrastructure). The consequence of this argument is that it is assumed that *borders do not stop cyberspace*.

"Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live". The *disembodiment* thesis resurfaced here. The body, it is argued, is distributed across multiple jurisdictions much in the same way as the Internet itself is. In other words, the body exists in a no-place, aligning neatly with the Greek translation of the word utopia – no place. Not just are there no physical bodies, but also there is *no matter,* which is turned into the argument that material concepts such as "property, expression, identity, movement, and context do not apply to us. They are based on matter, there is no matter here" (Barlow, 1996).

The laws of the state, but also the laws of nature that govern the movement of matter, are argued to not apply in this new space. Instead, a *peer-to-peer mode of governance is proposed:* "Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance

will arise according to the conditions of our world, not yours. Our world is different" (Barlow, 1996). This is very much in line with the communal spirit of the counter culture and the idea of the virtual community of the 1980s. The state interference into these communes is described as an act of hostile colonialism.

Finally, the declaration of independence picks up a theme that has been gaining traction in academia in the late 1980s and early 1990s, namely the idea that the information or network society (Castells, 1999) that will replace the industrial society. Together with the advent of globalization, the argument goes that the *state is increasingly becoming replaced* by transnational actors such as large corporations but even the emerging global society (a similar narrative as McLuhan presented it in the 1960s). Barlow argues that the industrial state is becoming obsolete. Governments lose control and authority over the Internet, which transcends its borders and makes physical coercion impossible. Therefore, the central norm of cyber-utopianism is that the *central state ought not to interfere with the Internet.* The state should keep its hands off cyberspace. It should not control, not regulate, not censor this ungoverned territory.

All of this represents an influential narrative of cyberspace in the early 1990s that was picked up by a wide range of academic and non-academic publications like *Mondo 2000*, *Reality Hackers* or even the newly founded digital native outlet *Wired.com* (1993). These publications repeated the narrative of the disembodiment of the digital self, the outlaw area called cyberspace in which a battle against government hierarchies are fought. Wired's inaugural issue is full of frames that the "digital revolution" is bringing a profound cultural transformation, "social changes so profound their only parallel is the discovery of fire" (Wired, 1993).

The case can be made that cyber-utopianism succeeded to some degree in the initial framing of the Internet in terms of libertarian and countercultural frames. Even parts of the government and big-business corporations adopted frames from this narrative throughout the 1990s, as the next chapter will show.

4.2.6 The Californian Ideology (1995-2001)

Cyber-utopian ideas had a widespread appeal and were picked up by economists, venture capitalists and particularly CEOs of Silicon Valley computer firms that argued that there was an utterly "*new economy"* forming because of the Internet. As is shown in the timeline in the appendix (see Table 9. List of Internet Milestones and Security Incidents), the commercial services on the Internet, like e-shopping, began to kick off in 1995, after the invention of the HTTP-Cookie, which allowed to store user information across websites

and thus enabled shopping baskets. The cookie introduced the forgotten economics (engineering blind spot) into the Internet (Metcalfe, 2006). Secure, encrypted online data-transmission (Netscape's SSL encryption, released in 1995) was the second crucial artifact (and sufficient condition) that made it possible to buy material objects such as books in the digital world (Berners-Lee, 2000, p. 97). Amazon sold its first book online in 1995. Wells Fargo bank launched online account services and Ebay formed the first virtual second-hand market place. These inventions opened the Internet for commerce and marked the commercialization of Internet services, together with deregulation policies (see chap. 4.3.5.3 Policy: Internet Censorship with the Communications Decency Act (1996)), the privatization of the Internet (see chap. 4.3.4 Artifacts: Privatizing Control over the Internet) and increasing commodification of digital goods (digital music with mp3 in 1996, digital images, videos, news-content, data etc.). The combination of causal events (equifinally) produced an investment frenzy at the Stock-Market, called the "dot-com boom".

Netscape, the market leader of browsers at the time, entered the stock market in 1995 and immediately gained 108% in value (Shinal, 2005), becoming the largest initial public offering (IPO) in the history.[70] Other companies like Yahoo! (Est. 1994) achieved similar results, placing its founders David Filo and Jerry Yang in "Newsweek's 'sixty richest people in the world" (Kaplan, 1999). These rapid success stories turned the public's attention towards this new thing, the Internet. "It also sent an undeniable message to the commercial world: The web was big business. The gold rush was on" (Berners-Lee, 2000, p. 106). This beginning commercialization of the Internet began to fuse economic ideas and norms with cyber-utopianism, creating a distinct branch or forking path of utopianism called *cyber-liberalism* (McEvoy Manjikian, 2010). It builds on the same ideological foundation and shares many utopian core-assumptions, but has a distinct economic flavor.

After initially dismissing the Internet, Microsoft CEO Bill Gates argued in his revised 1995 book:

> "We stand at the brink of another revolution. This one will involve unprecedentedly inexpensive communication; all the computers will join together to communicate with us and for us. […] we may be about to witness the realization of Adam Smith's ideal market, at last. […] Just about everything will be done differently" (Gates, 1995, p. 37).

[70] Netscape pioneered the unusual business model of giving their product, the Netscape Navigator, away for free on the Internet. Their approach was to commercialize services once Netscape had a sufficient user base. This created a substantial risk for any investor because Netscape product, as well as many other companies who copied the business model, did not generate any profits (Berners-Lee, 2000, p. 83).

Influential CEOs like Gates suddenly gave utopian hippie ideas external credibility and authority. The centerpiece of this cyber-liberalism is the idea that the Internet will create a new kind of market, dubbed "*the new economy"* that is fundamentally different from the old, industrial logic (indicating a "then vs. now" frame). This new economy is said to operate according to a *decentralized networking logic* and thus *transcends globally*. Gate's book was highly influential among business elites and occupied the New York Times' bestseller spot for weeks.

Similar frames can be found in the unofficial founding document of this paradigm, the widely regarded "Cyberspace and the American Dream: A Magna Carta for the Knowledge Age" (Dyson et al., 1994), published by the Progress and Freedom Foundation (PFF), a neoliberal think tank with various political connections to the Republican Party (among them Newt Gingrich). Most of the financial supporters of PFF nowadays come from the Fortune 500 IT-Companies (Mosco, 2004, p. 107). This document systematically connects utopian ideas (self-governance, erosion of state authority, individual empowerment, new frontier etc.) with neoliberal thought, such as deregulation and a small state. For cyber-liberalism, cyberspace is not a commons, but a market. "To create the new cyberspace environment is to create new property – that is, new means of creating goods (including ideas) that serve people" (Dyson et al., 1994). The idea that user *data/information is a commodity* that can be sold is conceived in this context. The distributive, decentralizing and empowerment features are not only said to erode hierarchies, but also monopolies into systems of prototypical competitive markets, resembling Joseph Schumpeter's idea of creative capitalist destruction. The assumed positive effects are:

> "Cyberspace will play an important role knitting together in the diverse communities of tomorrow, facilitating the creation of "electronic neighborhoods" bound together not by geography but by shared interests. Socially, putting advanced computing power in the hands of entire populations will alleviate pressure on highways, reduce air pollution, allow people to live further away from crowded or dangerous urban areas, and expand family time" (Dyson et al., 1994).

To enable this, the appropriate role of the government lies in "removing barriers to competition and massively deregulating the fast-growing telecommunications and computing industries." The argument is that the "egalitarian explosion" of the Personal Computer was only possible because:

> "government has stayed out of these markets, letting personal computing take over while mainframes rot (almost literally) in warehouses, and allowing (no doubt more

> by omission than commission) computer networks to grow, free of the kinds of regulatory restraints that affect phones, broadcast and cable" (Dyson et al., 1994).

The norms of cyber-liberalism are similar to utopianism. The government should promote dynamic competition while *keeping its "hands-off"*. Government control harms the growing digital market and will make the US uncompetitive globally. This includes the demand for cheap, but *essentially open access* to the Internet: "Price-and-entry regulation, in short, is the antithesis of dynamic competition". Second, it should support "the key principle of ownership by the people – private ownership – should govern every deliberation. Government does not own cyberspace, the people do" (Dyson et al., 1994). This is a variation of the open-commons theme with the difference that cyber-liberalists argue for commodification and the creation of property rights in this yet uncharted frontier territory (in contrast to hippie utopians). Other arguments where demands for reduced tax burdens for IT companies and the reconfiguration of the large, hierarchized government into a smaller, decentralized network structure.

According to Mosco, the Magna Carta "extended the cybernetic and countercultural analogies current in the social worlds of the Whole Earth and Wired, linked them to a libertarian political agenda, and ultimately used them as symbolic resources in support of the narrow goal of deregulating the telecommunications industry" (Mosco, 2004, p. 228). Countercultural norms found its way into lobbying strategies of large corporations and generated industrial pressure against state control of the Internet, which resonated with the goals of cyber-utopians and influenced US policymaking in the 1990s. Additionally, Silicon Valley companies created new influential lobby companies like TechNet.

The genealogy of the signifier "*new economy"* is interesting. Jeff Madricks's process-traced the evolution in business publications of the 1980s, where it initially described the increased relevance of the service economy, but then disappeared (Madrick, 2001, p. 10). In 1996, the term reappeared with a completely new meaning: *new economy meant Internet* (Madrick, 2001, p. 10). Madricks argues that Wall Street analysts, journalists and scholarly futurologists (among them cyber-utopians such as Manuell Castells, Nicholas Negroponte and Kevin Kelly)[71] picked up the term and turned it into a *social metaphor or diagnostic frame* to explain the uptick in the US economy in 1996. Their assessment was

[71] Kelly's book "New Rules for the New Economy" is particularly interesting. The argument is: "This new economy has three distinguishing characteristics: It is global. It favors intangible things—ideas, information, and relationships. And it is intensely interlinked. These three attributes produce a new type of marketplace and society, one that is rooted in ubiquitous electronic networks." From these perceived Internet attributes, Kelly deduces management strategies like mimicking flat hierarchies, imitate packet-switching in the real world transportation processes and much more. He essentially argues: "The dynamic of our society, and particularly our new economy, will increasingly obey the logic of networks" (Kelly, 1998, pp. 10-11).

not based on empirical, economic analysis but wishful thinking based on anecdotal evidence. In other words, inexperienced journalists ascribed causality to the Internet, arguing that *it* was responsible for the economic growth. Again, the digital avant-garde acted as meaning-managers, bricoleurs and sense-makers of the Internet and had a widespread public impact. At the end of 1996, Bloomberg declared the "*Triumph of the New Economy"* the pillars of which where: rising exports and the globalization and second business investment in information technology (Mandel, 1996). The narrative of the new economy "included just about everything: changing labor markets, the NAFTA trade agreement and globalization, corporate restructuring, the decline of unionization and of course information technology. In effect, a second industrial revolution appears to be washing over the land […]" (Madrick, 2001, p. 11).

Based on a "then and now" frame, it was assumed that the *new economy operated according to own rules* or laws, different from the old ways. The New Yorker argued "the New economy has put a premium on the values of networks, and there are genuine differences between the economics of software and the economics of hardware" (Surowiecki, 2000). Wired Editor Kevin Kelly argued that the Internet economy would be the "beginning of prosperity as we have never known it" because *wealth would not just increase but be distributed to everyone*: "The good news is, you'll be a millionaire soon. The bad news is, so will everybody else" (Kelly, 1999). But not just Internet gurus like Kelly predicted a *long-boom,* but also esteemed economists spoke of "a vast economic expansion that could go on for decades, spreading prosperity around the world and lifting billions into middle-class lifestyles" (Schwartz, Leyden, & Hyatt, 1999, p. 108). James Glassmann predicted that, because of the Internet economy, the Dow Jones Index would reach 36000 points in the new future (Glassman et al., 1999).[72] The rhetoric of the new economy also influenced politics, as a report from the Department of Commerce, which had been drafted before, but ironically released immediately after the burst of the dot-com bubble shows (U.S. Department of Commerce, 2000).

The belief that the Internet is both, a benign emancipating force and a digital utopia which could make everyone with a clever idea rich culminated in the so-called *Californian Ideology* (Barbrook & Cameron, 1996). According to Barbrook and Cameron, who first described this phenomenon, it combines the "free-wheeling spirit of the hippies and the entrepreneurial zeal of the yuppies" (Barbrook & Cameron, 1996). It represents the fusion of cyber-utopian visions with a conservative logic. It could be argued that this is an economical spin-off from utopianism, held primarily by private companies and

[72] While writing this the Dow Jones Index reached 19700 points.

corporations around the Silicon Valley area. One the one hand, it is based on many of the counter-cultural, hacking and cyber-utopian concepts described in the previous chapter (like the emancipatory potential of personal computing devices that allow individuals to express themselves, which shares the liberal-selfhood concept of the hacker culture).

On the other hand, it adopted "the laissez-faire ideology of their erstwhile conservative enemy" (Barbrook & Cameron, 1996), including economic ideas and business models. Liberty, freedom and self-determination meant foremost the liberty of individuals on the market place (economic liberalism). For example: "In place of counterproductive regulations, visionary engineers are inventing the tools needed to create a free market within cyberspace, such as encryption, digital money and verification procedures" (Barbrook & Cameron, 1996). Potentially everyone could become a high-tech entrepreneur, creating products that make people's lives better. This deep core belief still lives on in Silicon Valley companies like Apple, Google or Facebook, which claim that smartphones, intelligent algorithms (machine learning or Big Data)[73], social-networks, apps, fitness-trackers and all sorts of digital gadgetry are designed to improve people's lives. Existing power structures like state regulation should not stand in the way of this new digital market, which is why many of these companies are often accused of engaging in creative tax-evasion strategies. Counter-cultural mistrust of authority combines with neoliberal ideals of a small state, creating a "bizarre mish-mash of hippie anarchism and economic liberalism beefed up with lots of technological determinism" (Barbrook & Cameron, 1996). Instead of rebelling against the establishment, these tech entrepreneurs argue that individual freedom can only be created by technology, like for example the use of encryption to protect private conversations. The interesting impact of the Californian ideology is that it increased the public appeal of cyber-utopianism and thus expanded its influence beyond the counter culture and hacker community. Because banks and corporations adopted the narrative, cyber-utopianism increased its external credibility and the "everyone will be rich" narrative had a certain fidelity and appeal.

According to Madrick, the social metaphor of the new economy "only functioned, however, because people believed it was true. That is to say, they believed it was an economic concept largely because the media and Wall Street treated it as one—indeed, told them it was one" (Madrick, 2001, p. 2). It was a self-fulfilling prophecy that was highly compatible with the general idea of the American dream. The general economic

[73] The current hype about big-data is an evolutionary outcome of the Californian ideology and its commodification of digital services and data. With the rise of the Web 2.0, the idea that data can be monetized became prevalent in economical discourses. It could be argued that this represents a new paradigm, which is studied in higher detail elsewhere (Mayer-Schönberger & Cukier, 2014).

euphoria exerted hegemonic power, although the claims were not based on solid empirical evidence.[74] Explanatory factors for the success of the narrative were that new economy stories were bestsellers and resonated with American beliefs. Pärna analyzed that stories featuring the narrative of the *computer nerd becoming rich*, among them self-made millionaires such as Microsoft's Bill Gates, Apple's Steve Jobs, Yahoo's Jerry Young or Amazon's Jeff Besos, appeared particularly often in business publications of the late 1990s (Pärna, 2010, pp. 140-144). Stories like the documentary "the Triumph of the Nerds" (1996) reignited the American dream with the "from rags to riches" concept. But this new "American dream" was only a short one, as the next chapter will show.

4.2.7 Junctures: Dot-com Bubble (2000-2001)

The cyber-liberal narrative of the new economy (see chap. 4.2.6 The Californian Ideology (1995-2001)) led to an investment frenzy at the stock markets. It was assumed that Internet-related technologies would create new electronic markets (like Ebay), new commodities (advertisement, Big-Data) and new services. This belief derived from the utopian ideas that had been attached to the Internet by media journalists and Wall-Street analysts. Scholars who analyzed the rhetoric of business magazines of the time discovered that it was full of magic (Mosco, 2004, p. 42), myth (Madrick, 2001), faith or religious beliefs (Pärna, 2010).

> "In fact, it promised miracles. A new economy meant that historical precedent was meaningless. It also induced enormous business investment in high technology, including Internet services that were ill founded. Corporate executives leaped into these new technologies so as not to be left out. Many of these were not carefully reasoned decisions […]" (Madrick, 2001, p. 15).

Investors assumed the new economy had unique characteristics and thus began to invest carelessly in stocks related to digital technologies, as the NASDAQ technology index shows. It was assumed that access and connectivity were the primary imperatives, so "massive amounts of fiber optic cable" were laid "which dramatically drove down the cost of making a phone call or transmitting data anywhere in the world" (Friedman, 2005, p. 72). Friedman goes on and speculates that this drove down the costs of fiber optic cables which, almost by accident, enabled the global diffusion of high-speed Internet. Other drivers were emerging electronic markets and online-retailers (like pets.com). Investors

[74] Nowadays, consensus seems to be that the "rate of productivity growth between 1995 and 2000 was by no means unprecedentedly strong" because the young Internet economy "accounted for less than 2 percent of all transactions in 2000" and that the mid 1990s growth had more to do with the lowering of workers wages which increased corporate profit margins (Madrick, 2001, pp. 1-12).

bought stocks and invested in these start-ups without checking if they had a sustainable business model that could generate profit. In fact, many of these new Internet companies were not generating profits but were loosing money constantly. This was rationalized by investors by referring to the unique characteristics of the new economy, were old economic principles did not seem to apply. Careful voices warned of a bubble, but were not heard.

The burst of the dot-com bubble between March 2000 and October 2002 ended the assumed long-boom (Schwartz et al., 1999) only 5 years after it began. NASDAQ lost 78% of its value (Beattie,). In just one month, nearly a trillion dollar was lost (Geier, 2015). Major Internet brands like Yahoo, Amazon and Ebay lost tremendous values and many firms went bankrupt. While there were 457 IPO in 1999, there were only 76 in 2001 (Beattie,). The dot-com-bust had effects beyond the stock market. Companies had to lay off 66000 workers and many websites were closed. 31 million Americans said they were affected by the crash, as a Pew study found (Horrigan, 2001, p. 2). The survey also showed that it was generally believed that the cause for the bubble was the greed of investors who took to many risks.

Figure 18. NASDAQ Index 1994-2004, Source: (NASDAQ, 2016)

While the financial impact of the dot-com bubble was limited (because Internet economy in reality only made up a few percent of the overall economy at the time), the ideational impact was more severe.

> "Business gurus had confidently promised a blooming future for this branch of the economy because it was so dynamic, and Internet companies had been celebrated as the ultimate realizations of free market dreams. This swift, 180-degree change in values exposes a sudden loss of faith in the Internet" (Pärna, 2010, p. 142).

The burst of the bubble presented itself as a shock to both investors and cyber-liberal utopianism itself. The dot-com crash led to a loss of faith and dramatically damaged the utopian narrative. It discredited the expectation of endless growth and the magical powers

of the Internet that seemed to resist traditional economical models. This proved to be a dangerous myth. A similar study reflects this: "Many of those who use the Internet have second thoughts about the meaning of the dot-com failures. In February 61% of Internet users thought weeding out Internet companies was a good thing; in August, half (50%) of users felt the same way" (Rainie et al., 2001).

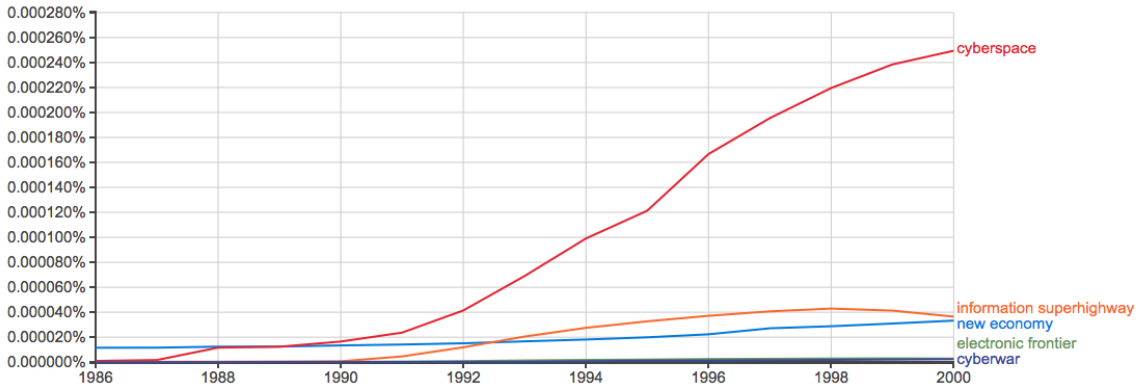
It is important to state that this disenchantment happened only a few months after the Y2K-bug, which was the first instance where an interconnected world showed new risks and problems (see chap. 4.4.5 Discourse: Y2K and Critical Infrastructure Failure). The synchronicity of the two causal factors is important here. Both cases negated the general cyber-utopian narrative that the Internet is a benign force with only positive effects. In contrast, the dot-com crash and the critical infrastructure panic of Y2K showed potential negative effects and blind spots of the digital revolution. At the same time, the dot-com crash had an undesirable outcome (financial loss), which further discredited utopianism (see chap. 2.2.4 Explaining Change). The final blow to cyber-utopianism came with 9/11 when the counter-terrorism narrative overshadowed everything else and presented cyber-realism as a powerful competing narrative to utopianism. Within this narrative, the Internet is framed as a safe-haven for terrorists, removing the remainders of cyber-utopianism from public discourse. "History, geography, and politics returned with a vengeance" (Mosco, 2004, p. 141) although utopianism believed of all this would change. Before we turn to that, let's summarize the key ideas and norms of utopianism.

4.2.8 Norms and Key Ideas of Cyber-Utopianism

This chapter will summarize some utopian frames that developed on different forking-paths with different actor formations over time. Because of time and space constraints, it is impossible to give a full description of all the cybernetic and utopian ideas presented in Wired and like-minded cyber-utopian carrier mediums in the early 1990s. Arguments developed within the hacker- and counter-culture, culminating in the WELL, were picked up in the 1990s by scientists, economists, journalists, educators and many more. While explaining the emerging and complex Internet to the general masses, journalists turned to the experts: hackers, IT-specialists and the digital Avantgarde of the WELL, in order to make sense of this new technology. This allowed cyber-utopian ideas and norms to spill into public discourse and to emerge as the hegemonic meaning for the Internet between

1993/94-2000, until the dot-com bubble disenchanted the narrative (Pärna, 2010, p. 69).[75] This can be quantified by referring to Google Ngrams.

Figure 19. Google NGram Analysis, Source: (Google, 2016)



Ngrams measure the frequencies of keywords in English book publications scanned by Google , which makes them an indicator for the relative dominance of terms. In this example, I have used keywords from each of the paradigms. The utopian metaphor of cyberspace clearly dominates, but other utopian terms such as "new economy" and the cyber-liberal/utopian term "information superhighway" (introduced in chapter 4.3.3 Ideas: Cyber-Utopia on the Information Superhighway (1993)), are relatively important as well. Observe that the cyber-realist term cyber-war (see chap. 4.4.2 Ideas: Formation of the Information War Doctrine (1976-2000)) is highly marginalized and becomes important only after the year 2000, which lies outside the Ngram data-set.

The following discussion will present the cyber-utopian narrative and core arguments, but will not judge their plausibility, which will follow in another chapter (see chap. 4.2.9 Critical Analysis & Blind Spots of Cyber-Utopianism). The core of utopianism is the diagnostic frame that a *digital revolution* is going on, a rapid succession of different *ages*, historical waves (Toffler, 1980)[76] or stages in history (past, present, future). Normally, revolutions are sudden changes within in a short period of time, but the digital revolution is rather slow, going on for the last 30 years. This frame has a function: "the designation of a particular time of human history as an identifiable "age" is meant to highlight its distinctiveness from the past. It signals that a transformation has taken place in

[75] Pärna for example counted that "between 1993 and 2002 the American magazine Time featured the Internet and its many visionaries and heroes on its cover on at least twenty occasions" (Pärna, 2010, p. 71).
[76] According to the Tofflers, history is a succession of rolling waves, the first being the agrarian society. The second wave's characteristics are said to be Fordist factory production, factory-model of mass education, the nuclear family and general giant-corporatist institutions producing core norms such as obedience and punctuality. The third wave will replace the industrial society with an information society, driven by electronics and computers (Lewis, 1980). Knowledge and information becomes the central resource of the Information Age and those who utilize knowledge will benefit. This will result in more network-like forms of organization, putting stress on the nation state with majority rule (Weiss, 1996).

the way human activity is conducted and/or defined" (Harknett, 2003, p. 17). The industrial society then, the new network or digital society now. According to Mosco, the "then" and "now" frame functions like a switch and as a denial of the past with its antiquated models of governance and social order, prioritizing new ways instead (Mosco, 2004, pp. 32-35).

This revolution concept became powerful because it resonated with a narrative emerging at the end of the Cold War that the "world as we knew it" (Pärna, 2010, p. 78) is gone (9/11 being a second of these historical switches). For political scientist Francis Fukuyama, it was the "end of history" (Fukuyama, 1992) and a *Great Disruption* (Fukuyama, 2000) and for Daniel Bell the *"End of Ideology"* (Bell, 2000). In many of these books, technology is depicted as the major driver: "new forms of information technology (IT) promise to create wealth, spread access to information and therefore power around more democratically, and foster community among their users" (Fukuyama, 2002, p. 182). In other words, "the Internet hype transmuted the unease about uncertain times that characterized the post-Cold War years into a very hopeful narrative of a new and better way of life" (Pärna, 2010, p. 80). Furthermore, it resonated well with the general frame of the globalization. The early 1990s presented themselves as an excellent window of opportunity for cyber-utopianism.

This revolution frame has two elements. First, *change is seen as benevolent*, resulting in a positive future. "Not only is technology good, not only is it indispensable, but […] it alone can achieve all that human beings have been seeking throughout centuries: liberty, democracy, justice, happiness (by a high standard of living), reduction of work, etc" (Ellul, 1990, p. 30). This optimistic future is defined ex-negativo, based on perceived current, negative conditions (like hierarchy or inequality) and thus potentially open to various interpretations (interpretative flexibility). This explains the huge bandwidth of utopian arguments. For educators, the Internet is all about better education and for business it is all about economic transformation and so on.

Second, this change is framed as a *natural, irresistible force*. Director of MIT Lab Nicholas Negroponte argues in his book *Being Digital (1995)*: "the change from atoms to bits is irrevocable and unstoppable" (Negroponte, 1995, p. 4) and "like a force of nature, the digital age cannot be denied or stopped" (Negroponte, 1995, pp. 228-229). He envisions digitalization as a form of evolution with natural selection. Others called it a "tsunami of transformation" (Tapscott, 1995, p. 4) or argued "massive and unstoppable changes are under way" (Mitchell, 2000). All these are examples of naturalizing hegemonic articulations.

What changes will the Internet bring? What are its effects? Two major outcomes are predicted: *the Internet causes shifts in the power distribution* and therefore *global governance*. It *empowers smaller, individual or networked actors* and reduces the ability of the central state or large bureaucracies to exercise control. Political scientist Joseph Nye (who is not a whole-hearted utopian), picks up this *cyber-power* thought: "a power transition among states and a power diffusion away from all states to non-state actors" (Nye, 2011, pp. 113-115). The power structure of *the state is becoming obsolete* or is at least incompatible with the new mode of network-governance. Centralized bureaucracies are said to lose control over information flows on their territory and citizens. The Internet is all about the loss of control. *Decentralized network* structures are said to take over control (Castells, 1999). Networks, a hype concept of the mid 1990s,[77] are described as a hybrid between centralized, top-down-control organizations (like the state or the military) and flexible markets with loose affiliations (Powell, 1990). Many publications of the time focus on the assumed positive effects of networks, like flat hierarchies and quick information exchange (Börzel, 1998). The world is becoming more flat, as the Financial Times/Goldman Sachs business book of the year 2005 argues (Friedman, 2005).

A related argument is that because the Internet changes power structures, it also *changes (global) governance* (Steele & Stein, 2002, p. 35). For example, information technologies *encourage reciprocal communication,* from which the democratic process will benefit (Kedzie & Aragon, 2002, p. 123). The Internet is framed as a *tool for democracy* (Gore, 1994b). It could increase voter participation (vote-click) and can short-circuit political processes for lobbyism or advocacy (Hague & Loader, 1999; Shapiro, 2000). Common metaphors are *"global village"*, *"virtual town square"* or *"a new public sphere",* which are created by virtual communities on the Internet (Stebbins, 2012, p. 111). Some even go so far and argue that the Internet will create a *Jeffersonian vision* of direct democracy (Dyson et al., 1994). This frame was particularly popular in policy circles. The assumed end of this process will be a global cosmopolitan society in the Kantian sense (Dahlgren, 2015). The empowerment thesis also leads to an increased focus on non-state actors like NGOs or globalized organizations (WTO, IMF) in global problem-solving (Matthews, 1997, pp. 51-52).

[77] From the mid 1970s, sociologists started to describe a new form of social organization with flat hierarchies and quick information exchange; the social network (Granovetter, 1973). Manuell Castells coined the term network-society (Castells, 1999), a decentralized society, which was inspired from the social organization in platforms like the WELL. In 1990, Walter Powell argued that the network resembled a third mode of social governance between pyramid-organizations and unstructured but more flexible markets (Powell, 1990). Börzel offers a good literature review on the term (Börzel, 1998).

Closely related to the change in (global) governance is the idea of the *end of geography or physical space.* Senior Editor of *The Economist* Frances Cairncross wrote a whole book called *The Death of Distance.* "No longer will location be key to most business decisions. Companies will locate any screen-based activity anywhere on earth, wherever they can find the best bargain of skills and productivity" (Cairncross, 1997, p. xi). This will lead to greater interconnectedness and interdependence of economies and societies and thus "increase understanding, foster tolerance, and ultimately promote worldwide peace" (Cairncross, 1997, p. xv). The potentials of the Internet are economic growth, better, more transparent international relations and a global coming-together of citizens, who now can communicate with whoever they want on the globe. Similar arguments are also made by management consultant Kenichi Ohmae in his book *The Borderless World* (Ohmae, 1999) and MIT media professor William J. Mitchell in his *e-topia* (Mitchell, 2000).

It is also argued that the Internet will change our information processes like *education* and thus make us essentially smarter and *better informed citizen*s. Instead of going to a library or calling an information desk, even highly detailed information is now available for free on the Internet. This is "fundamentally reshaping the flow of creativity, innovation, political mobilization, and information gathering and dissemination" (Friedman, 2005, p. 95). Instead of one-to-many communication (in the past), the Internet allows *many-to-many communication*, which in the end benefits democracy (Benkler, 2006, p. 216). It will erode the monopoly of state media and make propaganda inefficient. Information can be cross-checked easily because it is available everywhere on the Internet and citizen-journalism will create a critical, public opinion. The Internet provides the tools to make everyone a content provider (Mueller, 2010, p. 35). This will lead to more open and transparent societies. Authoritarian societies are said to be incompatible with the Internet. The *dictator's dilemma* is a common argument: either authoritarian states introduce the ICT to gain economic advantages (which negates their monopoly over information) or they block them and fall back economically (while maintaining the information monopoly) (Shultz, 1985). Newsweek even argued that the Internet could overthrow dictatorships (Levy, 1995).

All these effects will occur because they are said to reflect attributes of the technology itself, as utopians claim. In other words, TCP/IP and WWW are understood in a particular way. The assumed effects of the Internet are based on two of its perceived characteristics: its *decentralized network architecture* (end-to-end principle) and its *distributed* routing. These features are said to have decentralizing and distributive effects. Among 1990s utopians, there is a strong belief that the Internet *inherently resists state*

control. Deibert argues that at the time it was "assumed that cyberspace was immune to government regulation because of its dynamic nature and distributed architecture" (Deibert & Crete-Nishihata, 2012, p. 339). John Gilmore from the EFF argued in the early 1990s: "The Net interprets censorship as damage and routes around it" (Harvard Cyber Law). Although this claim was quickly disproved, it had a widespread impact, for example on President Bill Clinton, who argued that trying to control the Internet "That's sort of like trying to nail Jello to the wall" (Allen-Ebrahimian, 2016). Clinton directed this statement at Chinese Internet censorship efforts. This quote is key evidence for the normative constraint of the "hands-off" norm even among political elites. Another variant of this argument is the so-called Streisand-effect: once some information is online, it cannot be taken back because it can be copied or, as one unknown source once said:"You can't take something off the Internet - it's like taking pee out of a pool" (Harvard Cyber Law). Information technologies have broken down the information monopoly a state could have in the past over its territory, for example in terms of propaganda.

One reason for that argument is the idea that the *Internet transcends borders* (Goldsmith & Wu, 2008, pp. 13-29) and thus makes geography and space irrelevant (*death of distance).* Political scientist Anne-Marie Slaughter argues for example that "the emerging networked world of the twenty-first century, however, exists above the state, below the state, and through the state" (Slaughter, 2009). This is based on the assumption that packet-switching and dynamic routing send messages randomly over the net, sometimes even through other jurisdictions.

Another argument put forward, particularly by civil-libertarians and cypherpunks,[78] is that the *Internet increases privacy and civil liberties* because it provides *anonymity* that protects from state oppression. Remember the entry quote "On the Internet, Nobody Knows You're a Dog." This idea stems from the disembodiment thesis[79] of the counter-culture, which states that you can encounter someone online without knowing his/her physical attributes (but based on an IP address and other signatures such as metadata). Even today, many politicians still argue that the Internet provides anonymity for terrorists. This argument is of central concern for national security actors: "trends in individual empowerment, network organizations, and destructive potential lead to the potential for great harm delivered anonymously" (Harknett, 2003).

[78] An anarchist branch of hackers following the idea of total transparency and the overcoming of state secrets, culminating in Wikileaks (Assange et al., 2013).
[79] An extreme version of the disembodiment thesis is Ray Kurzweil's book "The Age of Spiritual Machines" where he argues that neural interfaces between and machines and humans allow backup copies of the brain, thus immortalizing humans (Kurzweil, 1999).

Lastly, the Internet is seen as a *self-governed, generative organism* (Zittrain, 2006). This is based on the do-it-yourself attitude of early communalists who argue for peer-to-peer governance based on mutual interests and not top-down hierarchical control (Goldsmith & Wu, 2008, pp. 13-29). It is also uttered repeatedly in Barlow's declaration of independence: cyberspace is "an act of nature and it grows itself through our collective actions" (Barlow, 1996).

From these normative description follows one central norm promoted by utopians: *open access*, or as MIT Media Lab Researcher Ethan Zuckerman calls it: "[t]he Internet is the most efficient system we've ever built to allow people to seek, receive and import information and ideas, and therefore we need to ensure everyone has unfettered Internet access" (Zuckerman, 2010a). This norm was adopted by both the Clinton administration with its policy of the information superhighway (see chap. 4.3.3 Ideas: Cyber-Utopia on the Information Superhighway (1993)) but also by the Obama administration in 2008 (see chap. 4.5.2 Ideas: Cyber-Utopianism under Obama and Clinton). It is based on the empowerment thesis and puts its emphasis on individual humans and not the state. Internet access is framed as a human right (which the United Nations Human Rights Council adopted in 2016 (United Nations General Assembly, 2016)).

Also mentioned is the norm that the *Internet should be free,* free of censorship in particular, which is a main concern of civil-libertarian inspired cyber-utopianism. The free flow of information shall not be obstructed, resembling the idea of the hacker ethic. As such, cyber-utopians argue for the freedom of speech norm, and define speech as basically everything published on the net. This explains why much of Internet advocacy focuses on censorship, government surveillance of the Internet and interference with technologies such as encryption (Deibert et al., 2008). Implied is the idea that states or large corporations *ought not interfere with the Internet,* representing a strong normative commitment to the "hands-off principle". This is inspired by the cyber-punk narrative of the evil corporation and the self-governance attitude of early cyber-utopianism. The Internet is perceived as space for the individual people, and not considered to be the domain of the state. It represents an *open commons*[80] like the high seas, space or air. "The combination of the technological and normative aspects of the Internet in this period frame the Internet as an "open commons" in which the domain was considered a separate space

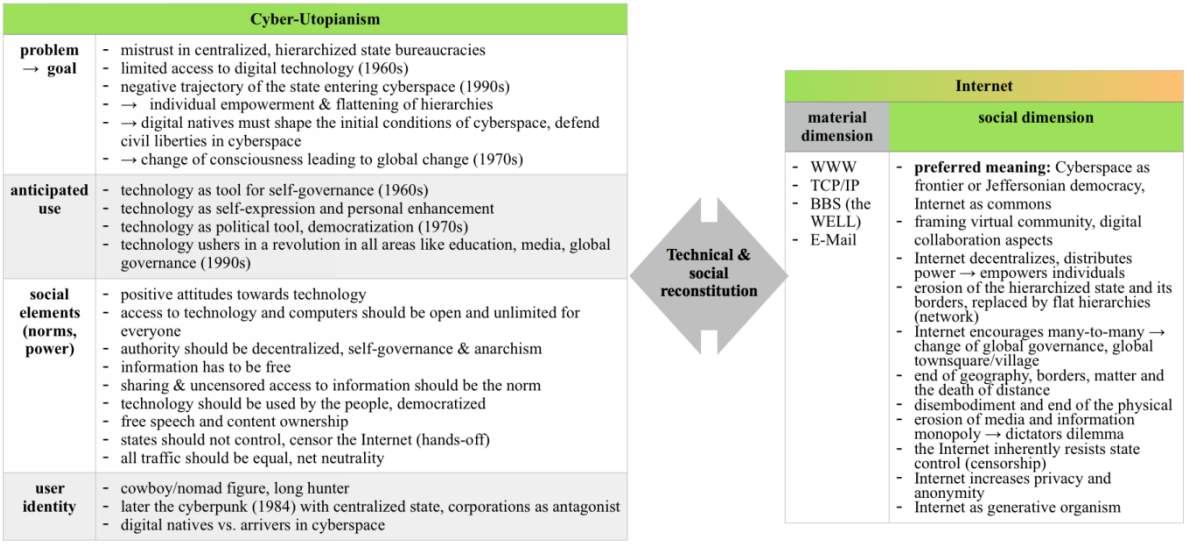
[80] According to Benkler "'Commons' refers to a particular institutional form of structuring the rights to access, use, and control resources. It is the opposite of "property […] no single person has exclusive control over the use and disposition of any particular resource in the commons. Instead, resources governed by commons may be used or disposed of by anyone among some (more or less well-defined) number of persons, under rules that may range from "anything goes" to quite crisply articulated formal rules that are effectively enforced" (Benkler, 2006, pp. 60-62).

resistant to state regulation and control" (Deibert & Crete-Nishihata, 2012, p. 342). This idea inspired the decentralized, multi-stake holder governance of Internet top-level domains with ICANN[81] but also the research and development of Internet standards with Internet Engineering Task Force. Both organizations feature a multi-stakeholder design that was chosen to prevent control of individual states over core Internet technologies and future standards (Hofmann, 2005).

Another political norm is *net-neutrality,* or the idea that every packet should be treated equally and that there should not be any special services from content providers who would be treated with higher priority (i.e. higher speed). In other words, the net should not discriminate.

A key finding of this chapter is that paradigmatic elements, key ideas, identity descriptions and beliefs of the paradigm's advocates that developed since the 1960s were systematically attached and projected to the technology in question. Technology is understood through the values and beliefs of the paradigm. For cyber-utopians, who share a strong commitment to decentralized governance structures, the decentral and distributed features of the Internet are seen as an essence that will produce equivalent societal effects. The argument goes so far that it is assumed that a technology has an inherent essence that reflects the particular beliefs or ideas of a group.

Figure 20. Cyber-utopianism framing the Internet as Cyberspace in the early 1990s (own diagram)



The case can be made that many of these utopian ideas were dominant during the 1990s and influenced how the general population perceived the Internet. The appeal of utopianism increased with the dot-com investment frenzy, when even corporations and

[81] Internet Corporation for Assigned Names and Numbers.

financial actors adopted utopian frames. The dominance of euphoria and utopias lasted only a few years and remained largely unquestioned, although there was much to criticize.

4.2.9 Critical Analysis & Blind Spots of Cyber-Utopianism

This chapter discusses some of the cyber-utopian arguments in a critical way. Mosco argues that the powerful utopian narrative presented itself as hegemonic in framing the digital revolution as a natural fact, an irreversible transformation, thus silencing alternative, more skeptical voices (Mosco, 2004, p. 19). Cyber-utopianism, and especially the Californian Ideology had a widespread appeal, combining ideas from the New Left (self-empowerment, liberalism) and the New Right (market liberalism, small government), thus bridging different ideological camps from hackers to large IT-companies, from Al Gore to Newt Gingrich. This silenced critical voices.

For example, even utopians such as Howard Rheingold brought up the possibility of mass accumulation of citizen data by states through the Internet. He correctly predicted that in the future "instead of just telephone taps, the weapons will include computer programs that link bar codes, credit cards, social security numbers, and all the other electronic telltales we leave in our paths through the information society" (Rheingold, 1993, p. chap. 10). In 1996, critics warned about the privacy implications the Internet has that for example "transactional information [metadata] can be very revealing of one's personal habits when compiled and collected from many sources", so that for example sexual preferences could be deduced from surfing behavior (Wellbery, 1996). The individual empowerment thesis blurred the fact that the powerful (states) had the resources and know-how to adapt to the decentralizing tendencies of the Internet. Authoritarian states like China began their widespread Internet censorship effort in 1996. Russia and the USA began clandestine Internet surveillance activities with their quest for metadata (see chap. 4.4.7.3 Artifacts: NSA and the Full-take Norm of Internet Control (2001 -)) around 1998 (Deibert et al., 2010).

The underlying meta-critique of cyber-utopianism, similar to cyber-realism, is *technological determinism* (see chap. 2.3.1 Theorizing Technology: Traditional Approaches), but with a positive flavor (Winner, 1997). Technology is essentially regarded to be autonomous. Society is the subject, technology the object of change. This determinism implies that technology has certain *revolutionizing characteristics* leading theologically to distinct social outcomes (like better democracy or a global community). Hegemonic articulations such as framing the digital revolution as irresistible and unstoppable argue that there is just *one* path to the future, which denies the possibility of

the social shaping of technological development (see chap. 2.3.4 The Social Construction of Technology and its Critique). Utopianism neglects the conditions for the possibility of its visions. Neither are the concept of power and power-distribution elaborated on, nor are the conditions of possibility for a global community analyzed.

The possibility to communicate globally does not imply its probability because people tend to communicate in closer circles. Language barriers are an issue that were not conceived in the early days, when the Internet consisted of around 99% English content. English is currently replaced by Mandarin as the most spoken online language. Sociological theories about the creation and maintenance of communities are ignored (Winner, 1997). The possibility of class, race or ethnic conflicts like modern networked antisemitism and nationalism are notably absent from cyber-utopian thought. Evgeny Morozov argues that the possibility of *many-to-many communication* alone does not guarantee that someones listens or that some kind of consensus or productive discourse is formed. The Internet can be turned into a *Spinternet*, a tool for spin-doctors to spread dissent and propaganda that drown the truth in an endless stream of noise (Morozov, 2011, p. 153). The current debate about echo chambers and fake news indicates this. In sum, Winner argues that cyber-utopianism operates with under-theorized, banal and *hollow concepts of both community and politics* (Winner, 1997).

The explanation for this lack of social theory is that the creators of the Internet, hackers and early digital communities, as well as the early adopters of the Internet came from the same social class: *white, young, well-educated, English-speaking middle-class males.* The hacker culture, the WELL and the Internet all developed in an elitist context (Ivory league universities) with generous funding from the US military. Women and other ethnicities barely played a role during the social construction of networking technologies. In the mid 1990s, there were still huge entry-barriers to the Internet. The economically disadvantaged could neither afford a computer nor a dial-up connection. The same is true internationally where there is still a digital divide between the interconnected North and South with little Internet penetration (Hargittai & Hsieh, 2013). For these regions, the spread of information technologies with their supporting technical infrastructure, build by large Western corporations, often had the flavor of economical imperialism and colonialism.

In light of all these obstacles, why then is the Internet perceived to be a democratic tool for individual empowerment? Because the *elites projected their behavior, ideas and norms onto these technologies* and deduced from this projection that it would be true for everyone else. They assumed that because their particular community used the Internet for benign

projects with a flat hierarchy to improve individual skill, so would anybody else. The possibility that someone with a criminal background could use the Internet for malign things, did not feature prominently.[82] Mosco argues that "the greatest mistake people make about technology is to assume that knowledge of its inner workings can be extrapolated over years to tell us not only where the machine is heading but also where it is taking us" (Mosco, 2004, p. 14). This *projection fallacy* works in two ways: to the anticipated social effects of a technology but also to its inner workings. The projection fallacy creates the illusion of a technical essence, the end-to-end principle in this case that is unchangeable and will deterministically produce certain effects. Theory teaches us that the effects of a technology lie less in its essence, but within the social context of usage (see chap. 2.3.6 Combining the Frameworks). In a liberal West-coast America, the Internet certainly has communal and liberating effects because the underlying societal structure supports this, while the same technology in China and Russia is used as a tool of oppression (Morozov, 2011).

But not just spatial, but also temporal context matters. Utopianism with its deterministic notion that highlights the "newness" or the distinctness of the "information age" ignores that similar positive attributes have been given to almost all information technologies in the past:

> "Historians have documented that the telegraph, telephone, radio, television, and cable TV were all initially received in startlingly utopian/dystopian terms. Each time, it was claimed that the technology would unite people around the world, bring about the end of war, solute the problems of education, change human consciousness" (Sholle, 2002, p. 9).

These technologies, over time, have become normalized and their meaning changed. Morozov maintains the same argument for the Internet. Its potential for political mobilization is overstated because usage statistics suggest that most people use the Internet for entertainment (Facebook and funny cats) instead of political dissent. Not George Orwell's Big Brother, but Aldous Huxley's "Brave New World" is the better metaphor, because as long people feel entertained, they will not resist state encroachment, censorship and surveillance (Morozov, 2011, pp. 57-85).

[82] Coleman correctly argues that the hacker ethic creates the false impression of a coherent community. Even among hackers there is a great variance of people believing in different norms. The open source ethos is not shared by all programmers. Crackers for example hack for personal or financial gain and already were a problem when Barlow launched the EFF in 1990s. Cypherpunks advocate radical transparency and publication of state secrets (Wikileaks) while information security hackers are committed to information security. In contrast, anti sec hackers lobby against the disclosure of software vulnerabilities because of anarchist notions. There are also regional differences. US hackers tend to be more libertarian while European hackers are more social democratic (Coleman, 2013, pp. 18-19).

In other words, the *empowerment thesis* and the description of the Internet as a self-governed open commons must be questioned. Statements like "everyone will be rich" or "empowered" ignore the fact that every social revolution produced winners, most notably large corporations like Amazon, and losers like small book stores or small business that cannot compete with the economy of scale. A common mistake by cyber-utopians is "to conflate the activities of freedom seeking individuals with the operations of enormous, profit seeking business firms" (Winner, 1997). Current debates about data sovereignty indicate a huge power imbalance between users and large corporations such as Facebook. The modern saying "if an online service is free, you are not the customer but the product", reflects this.

Cyber-utopians, with their focus on cyberspace and disregard of matter and geography, *ignored that the physical infrastructure of the Internet is owned* by large telecommunications corporations and other intermediates with particular interests. The neglect for matter also reinforced the false belief that the Internet resisted state or corporate control because fiber optic cables and server-farms (the Internet backbone) are geographically bound to the jurisdiction of states.

This leads to the final and most profound critique of cyber-utopianism: the belief that the Internet has an uncontrollable essence written into its protocols that cannot be altered. Lessig (Lessig, 2006) convincingly argued that states can control technology, for example by standard-setting, policies (like censorship laws or wiretapping requirements such as CALEA, see chap. 4.3.5 Junctures: Policy Attempts to Control the Internet (1993-1996)). He also argues that utopianism adheres to the fallacy of "is-ism – the mistake of confusing how something is with how it must be" (Lessig, 2006, p. 32). While it is true that the Internet originally relied on technological features that determined how the technology operated and how it can be controlled, this does not imply that this cannot be changed. Policies, ideas and norms shape the Internet and can alter these technological principles over time (see chap. 2.3.7 Digital Technology: Software and Code). The future Internet may allow greater surveillance and centralization. Cyber-realists in fact demand this, as another chapter will show (see chap. 4.5.4 Discourse: Cyber-Doom and the Hegemony of Cyber-Realism).

Although it is easy to criticize cyber-utopian ideas retrospectively, the paradigm made an important contribution. Cyber-utopianism constructed a particular vision of the Internet that reduced its interpretative flexibility. It is the reason why we even nowadays associate the Internet not primarily with packet-switching and dynamic routing but with terms like *cyberspace*, *virtual communities* and the creation of a *global village.* All these terms

describe the same phenomenon but have completely different meanings. The idea of the positive effects of the Internet became attached to this technology by cyber-utopianism and shaped its initial perception and worldwide diffusion. The idea that states should not control, censor or monitor cyberspace was a powerful narrative that would not exist had the technology developed in a different place, say the Soviet Union, as for example Peters shows in his book on networking experiments in Russia (Peters, 2016). Although it was idealistic, it embedded Western liberal-democratic concepts into the technology, such as freedom of speech and open access as a human right.

Without the belief in the freedom of information, there would not be a global database such as Wikipedia, but maybe different pay-wall encyclopedias, based on the traditional financial models. Without cyber-utopian thought, there might not have been one global network but instead many incompatible, walled-off network-islands, or what some scholars call a *"balkanized network"* or *"splinter net"* (see chap 4.1.4 Artifact: The World Wide Web (1989-present)). The Chinese and Russian Internets are showing signs of this trend. Alternatively, corporations are building "walled gardens" or subsections of the Internet where they determine social norms and types of connectivity to other networks, often for a price. Apple for example censors smartphone apps covering clandestine US drone operations and Facebook censors images depicting human nipples. Via these technologies, US moral standards are forced upon other countries with different moral sensibilities. Telecommunications providers advocate visions of a basic Internet, where you can access news and websites, but if you want to watch videos online, you have to pay extra, just like the US cable-TV model. The application, the replacement of websites with apps, is another trend that might fragment the Internet. In other words, "just as it was not preordained that the internet would become one global network where the same rules applied to everyone, everywhere, it is not certain that it will stay that way" (Economist, 2010).

4.2.10 Summary

This chapter showed that cyber-utopianism is not a homogenous political paradigm or philosophy. It is held by various actors with different interests and motivations. Replicating the structure of the last summary chapter, I will first describe the parts of the causal mechanism in a narrative fashion and provide a table with the key take-away messages at the end.

First, a positive attitude towards computers developed in the highly centralized context of main-frame computing in the 1950s (part 1). Those who understood new technology were less afraid of it and saw its potential for realizing personal goals. The

hierarchized prestructuration of computer-use was undesirable for the impact constituencies, young IT-students, because it prevented effective problem-solving and code-writing. Hierarchized bureaucracies restricting access to information and technologies became the prime antagonist for cyber-utopians, an idea that resonated well with the counter-culture and the general 1960s zeitgeist of mistrust in authority and the military-industrial complex. New technologies such as time-sharing enabled collaboration and led to the creation of a sense of community of like-minded individuals who began to share a common set of ideas and norms (a paradigm), such as that technologies should be open and information should flow freely (resembling freedom of speech). Thus, this community engaged in the discursive *practice of counter-signification and appropriation*, engaging in deviant use of computers for playing games and tried to change existing practices and norms (part 2). Without this positive perspective of the hacker culture, it is very unlikely that a utopianism with a special focus on digital technologies (i.e. a *cyber*-utopianism) would have formed, since the counter-culture initially was skeptical towards computers (see chap. 4.2.3 Artifact: Democratizing Technology (1970-1980)).

The *practice of sharing ideas and open software code* was an important causal factor for the diffusion of early utopianism because it exposed other IT-students at other universities to the same ideas that were transported through the shared software. The idea of peer-to-peer collaboration served the same function. Later, ideas and norms got diffused through hacker-conferences, staff-exchange between universities and even computer networks such as ARPANET. Additionally, many of the early hacker generations and IT students became business-professionals in the early 1970 and ushered in the era of the personal computer. Without these operational platforms and idea-hubs, cyber-utopianism would have most likely been a geographically limited phenomenon.

The later Home-brew community that formed in the Silicon Valley, the epicenter of cyber-utopianism, adhered to the same norms and ideas and engaged in the *process of counter-appropriating computer use*, this time successfully (part 3). They developed the idea of the democratization of computer-usage: access to computers had to be democratized and decentralized away from military research applications into the home of the people. By creating personal computers, the Home-brew Community embedded this norm into these artifacts. With the successful mass diffusion and commodification of the PC, these ideas diffused to a wider, non-expert audience. The narrative that computers could empower individuals and create a better democracy became an appealing narrative during the 1980s and later was attached to the Internet as well.

The second branch of the causal mechanism was the American counterculture, the hippies, the back-to-the-landers trying to change the political system and global consciousness through techniques of the mind. They too shared the *antagonism of hierarchies*, particularly the military-industrial complex that was made responsible for the Vietnam War. The solution to this perceived problem was creating new forms of living, consciousness and decentralizing power into communes. One of their key goals was self-determined governance without state interference, resembling a strong libertarianism (a uniquely American tradition and thus a case-specific causal factor). They also turned to extravagant scientific ideas, such as cybernetics and theories of new media. This exposed them to new ideas, like that digital technologies, artificial intelligence and machine automation could be used to create a new form of global society, one of the core ideas of cyber-utopianism. The compatibility and consistency of cybernetic and hacker ideas with counter-cultural ideas, for example in terms of the hierarchies as the key antagonists, is a key explanation for the fusion of these. At the same time, these scientific ideas gave utopians some external credibility and increased the fidelity of the utopian narrative. This factor is highly case-specific because this libertarian-inspired idea-cluster was nonexistent in other countries.

The *fusion of hacker and counter-cultural ideas* was facilitated by Stewart Brand, who gave hackers and communalists a shared forum, a platform to share ideas and techniques (part 4). The Catalog exposed the two communities to each other's ideas. Another facilitating condition was the geographical proximity of the mostly Californian counter-culture and the Silicon Valley, where many hacker-ideas were conceived. Brand personally visited both communities, acting as a networking broker. His other important contribution came in the 1980s, when the diffusion of the PC reached a critical mass of users and networking technologies were market-ready. This enabled his first social network, the WELL to become successful among early Internet users. The WELL enabled new practices such as exchanging ideas with people from the other end of the country. The *practice of using the WELL led to the creation of new norms* such as free speech, the self-governance of this online community, association by interest and concepts such as the death of distance or new forms of being (online) in virtual communities. The period between 1982 and 1992 thus can be seen as the period where a coherent cyber-utopianism formed out of the hacker and counter-culture. During this time, the Internet became the primary point of focus for the paradigm. It can be argued that a form of utopianism might have emerged absent of Stewart Brand and his influence (necessary condition), but chances are that this utopianism would have looked different, relying on different motives and non-

technical themes, for example resembling more left-wing themes like its European counter-part with the protests of 1968. Studies comparing the European and American hacker culture diagnose that libertarian and counter-cultural themes are mostly absent from the former (Alberts, 2014). Alternatively, one could hypothesize that a *non-cyber* form of utopianism might have vanished much in the same way as the counter-culture and commune-living disappeared during the mid to late 1970s (Turner, 2006, p. 129).

The most important idea that emerged was that the WELL resembled a space inside a computer, *a cyberspace,* an empty signifier that was created by the Sci-Fi literature of cyberpunk around the same time. The WELL filled the empty notion of cyberspace with a concrete meaning (signification). Cyber-punk certainly had a narrative fidelity and was highly commensurable and compatible to cyber-utopianism and the counterculture, because it shared the same antagonism. Cyber-punk literature helped to transport these relatively marginal ideas into the public discourse, explaining the early Internet to non-technical users and as such, *engaging in a sense-making practice* (part 5). Without it, we might not use the futuristic "cyber" term at all and might understand the Internet in completely different terms, for example as a network of networks. The early Internet users played a special role, acting as bricoleurs, sense-makers or paradigm-advocates. Because they were socialized with the WELL, they used this experience as a frame of reference for explaining the Internet when it reached mainstream diffusion in 1992.

Most notably was John Perry Barlow and the advocacy group he founded – the EFF, which politicized utopianism. Barlow and other utopians framed cyberspace in terms of the frontier. This technological frame highlighted design principles of the Internet such as its borderless nature and the idea that distributed routing and packet-switching would provide anonymity, prevent censorship and other forms of state control. Because of this projection they argued that the state had no role to play there, thus *advocating for the norm that the state should not interfere with cyberspace and let the users engage in self-governance of this medium*. This, too, represents a technical counter-signification and appropriation strategy, trying to establish the users as the dominant actors in cyberspace while denying this to the central state (see chap. 2.3.6 Combining the Frameworks). This happened because of the perceived state encroachment onto cyberspace with new legislation and represents diagnostic and motivational frames. He tried to motivate other utopians to shape the initial conditions of cyberspace by explaining it to new users. It can be argued that this strategy worked. Cyber-utopianism established the first widely shared meaning of the Internet in terms of utopian frames and thus influenced future discourses by other paradigms about the technology.

This overlap of ideas and concepts shows that the early 1990s represented a juncture where different causal pathways converged or interacted. I showed that many utopian frames, ideas and norms *resonated well in academic, public, economic, policy and media-discourses of the early 1990s*, which is a key explanation for the success of utopianism (part 6). Comparably, the technological frames of the engineering community were not as imaginative and commensurable as the vibrant cyber-metaphors. Some of the most influential utopian ideas were the concept of an irresistible information revolution that was going on, changing the logic of everything. Many of these ideas had the character of diagnostic or prognostic frames (see chap. 2.2.1 Discursive Struggles between Paradigms). New information technologies were said to lead to the dissolution of state power, to make borders irrelevant and empower the people vis-à-vis the central state. States would no longer be able to control media and information systems, thus making censorship and information controls obsolete. It becomes clear that the Internet had a high interpretative flexibility because digitalization affected all aspects of life, which led to a profound narrative fidelity.

Timing is an important contextual factor here. Cyber-utopianism could become dominant in public discourses because it *filled an ideological and narrative void at the end of the Cold War by providing a positive vision of the new millennium.* At the end of history, there was no alternative narrative so utopianism occupied that space, using this window of opportunity. An important necessary condition here is the invention of the WWW by Tim Berners-Lee, which made the Internet visual and more user-friendly, thus creating a large enough user base and thus momentum for mass diffusion of this technology (see chap. 4.1.4 Artifact: The World Wide Web (1989-present)). The equifinality of causal factors is particularly prominent during the early 1990s (see chap. 3. Methodology & Research Design). One should also keep in mind that the audience cyber-utopian advocates were talking to was rather limited. Only 2-3% of Americans used the Internet between 1993 and 1994, but they were the early adopters who picked up utopian frames and thus further inspired and educated later adopters. Utopianism was the first mainstream narrative for the Internet and drew strength from this early-mover-advantage to shape the initial discourse.

Around 1995, new technologies such as SSL encryption enabled electronic commerce and the *commodification of cyber-space,* creating new business models and practices diffusing utopianism into the business world. Another necessary condition was that cyber-utopianism resonated well with economic ideas of privatization and deregulation that were en-vogue at the time, creating the so-called Californian Ideology.

Renowned experts, entrepreneurs and Wall Street investors picked up the utopian narrative and began to *frame cyberspace as the realization of Adam Smith's ideal market and in terms of a completely new economy* that operated with a completely different logic (diagnostic frame). These advocates speculated about infinite growth and the distribution of wealth. This had a widespread appeal, as with many investment bubbles and thus increased the number of cyber-utopian advocates and lobbyists in Washington (part 7). Again, the internal logic of TCP/IP was extrapolated and assumed to produce external effects, a common fallacy of utopianism (see chap. 4.2.9 Critical Analysis & Blind Spots of Cyber-Utopianism). But *stories of self-made Internet millionaires and the growing economy silenced critical voices*. Additionally, the prospect for profit was a powerful incentive for industry and business to adopt cyber-utopian ideas and also the norm that the state should not interfere in this technology. They began promoting a more liberal version of this hands-off norm, focusing not on the Internet as an open commons but on private ownership. This liberal-utopian agenda was highly influential in policy circles, as the next chapter on Al Gore will show, where the cyber-liberal spin-off is analyzed more deeply. The argument can be made that all these parts in the causal mechanism are a minimal sufficient explanation for the rise of cyber-utopianism with its distinct and case-specific counter-cultural flavor.

Talk of the "new economy" became highly influential in public discourses because it operated with rosy predictions that were not necessarily grounded in empirical evidence. Several scholars observed a tendency for wishful thinking in these discourses (see chap. 4.2.7 Junctures: Dot-com Bubble (2000-2001)). When the dot-com bubble burst in 2000, many of these predictions were proven wrong. This *dramatically diminished the explanatory power of the cyber-utopian narrative* (outcome). More people realized that not everyone would become rich and that digital technologies had potential downsides and negative implications as well. The blind belief in the positive effects of technology was challenged by other instances, such as Internet Sex Panic of 1996 and the Y2K panic that are discussed in the following chapter (see chap. 4.4.5 Discourse: Y2K and Critical Infrastructure Failure).

Table 3. Causal Mechanism of Cyber-Utopianism

Context	Hierarchized Mainframe Computing.	Cold War.
Part 1	Hierarchized prestructuration of computer-use was undesirable for the impact constituencies.	Hierarchized mass bureaucracies as antagonism. Turn to the mind and self-governed commune-

	Practice of hacking leads to creation of like-minded communities.	living to change the world.
Part 2	Hackers engage in counter-signification and reconstitution of computing as positive, life-enhancing technology. Ideas spread in computer science community.	Counter-culturalists turn to (utopian) theories of the mind, libertarianism and cybernetics and thus develop utopian core frames.
Part 3	Homebrew community counter-appropriates computer & digital technology as personal and democratic, adds another core frame of utopianism. Cyber-utopian ideas begin to diffuse with the PC.	Stewart Brand launches Whole Earth Catalog and initiates idea and norm exchange between hacker and counter culture. The Emergence of digital-utopianism.
Part 4	Stewart Brand launches the WELL. Practice of using the WELL creates new norms (free speech, self-governance) and new ideas (death of distance, being online) and thus stabilizes cyber-utopianism. Cyberpunk helps to diffuse utopian concepts (cyberspace) into the mainstream.	
Context	Diffusion of the World Wide Web & end of Cold War.	
Part 5	Digital avant-garde engages in public sense-making practices, framing the new Internet technology in terms of the WELL. Cyberspace becomes a key metaphor for the Internet (signification). They advocate the norm that the state should not interfere with cyberspace.	
Part 6	Cyber-utopian ideas and norms resonate well with academic, public, economic, policy and media-discourses of the early 1990s. Utopian ideas diffuse through the mainstream and become dominant.	
Part 7	Economic actors develop a cyber-liberal spin-off of utopianism (Californian ideology) that influences to the dot-com investment boom.	Cyber-utopian ideas resonate with Gore administration and become politicized.
Outcome	Dot-com crash and Y2k discourse discredit utopian narrative.	

In sum, the equifinality of events presented an anomaly for cyber-utopianism that it could not explain. Around the same time, cyber-realism became a coherent competing paradigm

that was set to become influential with the Bush administration that entered office in 2000. Thus, as Legro argues, a competing paradigm was ready to take the place of utopianism (Legro, 2000, p. 266).

Before we turn to that, I want to shed some more light on part 7 of the causal mechanism, i.e. the political impact of utopian ideas. To show that cyber-utopian ideas were influential within the political sphere is important for evidence for the hypothesis that utopian norms and ideas dominated the 1990s.

4.3 Cyber-Utopian Liberalism and the Politics of Cyberspace (1990-2000)

"I took the initiative in creating the Internet."
Vice President Albert Gore, CNN Interview 9 March 1999

Although Vice-President Albert "Al" Gore Jr. (1992-2000) clearly did not invent the Internet, as the above-quoted live interview mishap on CNN suggests, he and his vision of an Information Superhighway played a huge role in shaping early Internet policy. He shaped dominant norms and the overall meaning of the technology for a wider audience – both domestically and globally. This chapter shifts the focus from the digital natives as paradigm-advocates to politics and particularly to the perception of the Internet in the early 1990s within the White House. Al Gore can be viewed as a (neo-)liberal cyber-utopian who, through his policies, framed the Internet in terms of a positive, liberal and economic vision. Together with President Bill Clinton, they adopted a market-oriented, hands-off norm in government behavior towards the Internet, opting for the primacy of the market instead of strict government regulation and control. Gore acted as a norm-entrepreneur, framing the meaning of the Internet in terms of global connectivity, economic growth and the creation of a peaceful, global community of citizens. Gore and Clinton were key advocates promoting positive, liberal and utopian discourse on the Internet, politicizing utopian ideas and creating a hybrid or a spin-off paradigm, cyber-*liberal* utopianism.

The analysis focuses on political documents created by the Clinton and Gore administration that deal with the Internet. These include election campaign materials, policies, interviews and secondary literature. One argument of the theory chapter is that norms of a paradigm not just become embedded in technological artifacts, but also in policies. This chapter shows the politicization of cyber-utopianism, which explains why it could become dominant. The early 1990s time-frame of analysis logically overlaps with the second half of the previous chapter but of course focuses on the political or intra-state level of analysis (see chap. 3. Methodology & Research Design). Here, the norm that the Internet should be a) democratic and b) not controlled by the state or at least only in minimally intrusive way, was conceived. This made the "hands-off" norm more stable. The norm that states should not control or censor cyberspace was advocated by Gore, not just on a local, but also on a global level and was dominant during the 1990s.

The chapter proceeds as follows. First, the regulatory background of telecommunications policy is introduced (see chap. 4.3.1 Background: The Governance of Information Technologies (1970-1990)). This is necessary to understand the policy field. After that I introduce the key advocates in this chapter, Al Gore and President Clinton (see chap. 4.3.2 Politics: Bill Clinton and Albert Gore as Internet Advocates (1992-2000)).

They picked up utopian ideas and fused them into politics, which will be discussed in the chapter on the idea of the Information Superhighway, the central policy agenda (see chap. 4.3.3 Ideas: Cyber-Utopia on the Information Superhighway (1993)). This agenda established utopian ideas and norms as politics and at the same time defined the appropriate role of the state vis-à-vis the Internet at arms-length, which represents the key norm of cyber-utopianism (see chap. 4.3.3.1 The Hands-off Norm & the American Internet Governance Model). Then I will explain how Gore framed it as inappropriate for states to control or regulate cyberspace on a global scale (see chap. 4.3.3.2 Global Framing of the Internet). These ideas had a concrete material impact, namely the privatization of the physical Internet infrastructure in the US, giving control over switches and fiber optics to the market (see chap. 4.3.4 Artifacts: Privatizing Control over the Internet). This is necessary to understand what hands-off actually means. This was not the final outcome of the process. Cyber liberal-utopianism was not completely stable or even hegemonic. The final chapters introduce a series of junctures, understood as points of contestation where different visions of the Internet clashed, particularly how the cyber-realism of the intelligence community with the utopianism of digital natives and partly the administration. The encryption debate (see chap. 4.3.5.1 Policy: The Clipper Chip (1993)), Internet-surveillance (see chap. 4.3.5.2 Policy: Wiretapping the Internet with CALEA (1994)) and censorship episode (see chap. 4.3.5.3 Policy: Internet Censorship with the Communications Decency Act (1996)) represent different realist attempts in controlling parts of cyberspace. As with every paradigm before, I introduce some blind spots and provide a short critique of the paradigm (see chap. 4.3.6 Critical Analysis and Paradigm Blind Spots). This is necessary to understand why realism, presented in the next chapter (see chap. 4.4 Information Warfare and the Origin of Cyber-Realism) could become dominant.

4.3.1 Background: The Governance of Information Technologies (1970-1990)

This chapter provides the background to understand early Internet politics and to contextualize the important policy changes that were introduced by the Clinton administration.

The initial Internet and telecommunications policy between the 1970s and early 1990s can be described by a lack thereof. At this time, Internet policy was a nascent subsystem that emerged because of the digital revolution. Drake argues that early US telecommunications policy was driven by the Federal Communications Commission (FCC) and the courts, not by the White House (Drake, 1995a, p. 307). Presidents Reagan and

Bush mostly neglected the new electronic media and the only leadership they provided was by endorsing deregulation, privatization and competition (Broad, 1992). Both presidencies were strong advocates of the laissez-faire or neo-liberal, economic paradigm gaining popularity in the 1970s with the Chicago school and 1980s Reagonomics (Niskanen, 1988). The core norm of this economic paradigm is the idea that the appropriate role of the state in economics is a marginal one, maintaining order and security, for example in terms of contracts and the protection of property rights (Noam, 1995, pp. 32-33). The state ought not to interfere in the market competition, but let the invisible hand of the market govern instead. This explains why neither Reagan nor Bush attempted to alter the existing legal and regulatory telecommunication framework that has been in place since the 1930s (Drake, 1995a, p. 307) in order to make it more compatible with the growing convergence of computing and telecommunications industries that began in the late 1970s (Baran & Farber, 1977). The 1934 Communications Act, the dominant regulatory framework, only provided weak regulatory oversight, so that telephone provider AT&T could build and own 80% of all telephone and access lines in the US and as such hold a monopoly over the Internet infrastructure. In contrast to other Western countries, the dominant telecommunication carrier was not state-owned, but a private business. This monopoly worked sufficiently in the 1950s and 1960s, so the government did not interfere.

With the dawn of computer networks in the early 1970s, demand for long-distance data transmission over the telephone network and consequently corporate advocacy for the liberalization of telecommunications grew (Drake, 1995c, p. 15). Smaller companies wanted to transport computer data (value-added services) over the AT&T-owned telephone network without paying the costly long-distance fees (early ARPANET used leased AT&T copper lines). In theoretical terms this can be described as a demand-push. In 1969, the FCC, the independent agency regulating interstate radio, TV, wire, satellite and cable communications ruled that AT&T had to open their network for other carriers, which the company only reluctantly did. In 1974, the Department of Justice started an antitrust lawsuit against AT&T, because of unfair business practices directed against smaller telecommunications and packet-switching providers. For example, AT&T prohibited the attachment of "foreign devices", such as modems, to their phone network (Ryan, 2013, p. 66). Without a modem, there could be no access to the Internet. After a lengthy trial, the AT&T monopoly was broken up in 1982 and two-thirds of the assets and employees were split into Regional Bell Holding Companies.

According to Milton Mueller, this ruling was a necessary condition in order to enable the rapid spread of the Internet in the early 1990s (Mueller, 2010, p. 56). This FCC-ruling

is described as the "most massive reorganization in business history" (Noam, 1995, pp. 33-36). Voice and value-added services were separated and this increased competition. Hundreds of new smaller data-service providers formed and began to offer cheaper rates for data-transmission, resulting in the "most dynamic, heterogeneous, multivendor, and user-driven communications and information industries in the world" (Drake, 1995b, p. 15). Instead of one monopoly controlling the entire infrastructure and fixing prices and proper use, the FCC opted for a decentralized governance model very much in line with the Internet's own norm of decentralization. This is sometimes called the US Internet Model. The AT&T episode highlights the general political hands-off and laissez-faire approach that guided much of early Internet policy. There was a complete lack of a coherent policy-vision and the Internet was understood in terms of the telephone and the regulatory framework of the FCC. This represents a mild form of pre-structuration in the policy field, but it can be argued that telecommunications and Internet politics, at the beginning of the 1990s, represented a nascent subsystem without much political debate and contestation. This made it potentially open for new actors, ideas and paradigms.

4.3.2 Politics: Bill Clinton and Albert Gore as Internet Advocates (1992-2000)

In contrast to the Reagan and Bush administration, the Clinton election campaign in 1992 began to formulate a coherent vision, narrative and policy for a global, interconnected network of networks, containing video, audio and telecommunications systems. This vision systematically framed information technology in terms of economic growth, job creation, social equality and education. This has to do with two causal factors.

First, the economic focus of the Clinton ticket had to do with the small recession between 1990 and 1991, which led to an increase of unemployment (Gardner, 1994). The early Clinton presidential campaign chose to focus on economic topics, as its famous campaign slogan "*It's the economy, stupid!*" indicated (Bennett, 2013, p. 123). With this slogan, Clinton was able to successfully differentiate himself from the general foreign-policy focus of President Herbert Walker Bush, who was running for a second term. This economic focus in times of growing unemployment, together with the ill-conceived campaign of President H.W. Bush, plagued by accidents and mishaps, is a key explanation for him winning the presidency in 1992 (Bennett, 2013, pp. 152-159).

The second factor was the *personal advocacy by the Vice President*. Albert Gore Jr., is described by some observers "as a bit of a nerd" leaning towards scientific and technological topics such as climate change or telecommunications (McCullough, 2014b). Internet pioneers called him "the first elected official to grasp the potential of computer

communications to have a broader impact than just improving the conduct of science and scholarship […]" (Cerf & Kahn, 2000). This technological literacy explains Gore's early involvement in the history of the Internet at a time where most people did not even own a PC (see appendix. Quantifying the Internet and the Digital Revolution). Since the late 1970s, Gore began to popularize the metaphors *"information superhighway"* or *"data highways"* which will be analyzed in the next chapter (see chap. 4.3.3 Ideas: Cyber-Utopia on the Information Superhighway (1993)). Gore's name is connected to several policy bills that played a major role in the development and diffusion of the early Internet. As chairman of a congressional science subcommittee, Gore was involved in legislation called *the Supercomputer Network Study Act of 1986* that although it never became a law, inspired the creation of five inter-networked supercomputer centers within the context of the National Science Foundation (Wiggins, 2000). This super-computer network was the aforementioned NSFNET, which became the technological backbone of the Internet infrastructure in late 1988 (Kahn, 1995, pp. 17-18) (see chap. 4.1.3.3 The Internet Backbone). In 1988, then-senator Gore began to formulate the goal of National Research network, supported by ARPANET inventor Leonard Kleinrock (National Research Council, 1988). This eventually led to the *High Performance Computing and Communication Act of 1991,* or the "Gore Bill", spending $2.9 billion federal dollar over five years on super computer research (Broad, 1992). Money from this bill allowed the rapid expansion of NSFNET, interconnecting NASA, the Department of Energy, NSF and ARPANET with high-speed 1.5-Mbps lines (Ryan, 2013, p. 94). It also provided the salary for many early Internet developers, among them later Netscape-founder Marc Andreessen, who created Mosaic, the first graphical browser (see chap. 4.1.4 Artifact: The World Wide Web (1989-present)). Theoretically, the Gore Bill is inspired by many ideas of the engineering paradigm. In sum, Al Gore was an early advocate of the Internet as envisioned by the engineers of ARPANET, nicely described by Vint Cerf and Robert Kahn as the follows:

> "When the Internet was still in the early stages of its deployment, Congressman Gore provided intellectual leadership by helping create the vision of the potential benefits of high speed computing and communication" (Cerf & Kahn, 2000).

As the inventors of TCP/IP highlight, Gore's role was an intellectual one: he provided an optimist future vision, a narrative of what the Internet could become and therefore shaped the meaning of this technology and the appropriate norms for government and private corporations therein. It could be argued that Gore was one of the few politicians who

understood what the Internet, as its inventors Cerf, Kahn and Berners-Lee conceived it, really was about. The social norms and political goals Gore formulated were an aggregation of the different norms of the engineers and cyber-utopians, mixed with market-liberal ideas. In sum, the governmental change from Bush to Clinton was a necessary condition for the emergence of cyber-utopian thought in the political sphere. Because Gore had a personal interest and literacy in the topic, utopian ideas were able to spill into the political discourse. The analysis of this intellectual contribution or in theoretical terms, the underlying paradigm, is part of the next chapter.

4.3.3 Ideas: Cyber-Utopia on the Information Superhighway (1993)

This and the next sub-chapters will analyze the major policy documents and statements produced by the Clinton/Gore administration. It will analyze problem definitions, solution strategies, political goals and general reoccurring themes and frames describing the Internet (its design, characteristics, functions but also its envisioned positive and negative effects) as well as general metaphors used for understanding the technology. To do so, I will focus on the technological agenda called the National Information Infrastructure Agenda (NII) (Clinton & Gore, 1993). The Information Superhighway was officially defined in a document by the *Information Infrastructure Task Force* that was created by Gore only 28 days after entering office (Information Infrastructure Task Force, 1993). This task force, chaired by Gore and Secretary of Commerce Ronald H. Brown, included a huge variety of private and public actors, while the military was notably absent (Cate, 1994). The agenda is a piece of smoking-gun evidence for the existence of both cyber-utopian but also neo-liberal ideas within the Clinton/Gore administration that created an interesting hybrid, a liberal spin-off from cyber-utopianism. To complement the analysis, I draw on other policy documents of the time as well (see appendix Information Superhighway Corpus).

First, what strikes the observer, especially compared with the cyber-realist paradigm is the lack of problem-definitions driving the agenda (see chap. 4.4.2.2 Problem Definitions of Cyber-Realism). The only problems that are very briefly mentioned are the struggling economy,[83] depicted in goals such as "to revitalize our economy" (Clinton & Gore, 1993, p. 2), the international competition and environmental challenges:

[83] Out of all documents analyzed, only in two of them are these problems defined. They play a marginal role and are not even defined as problems but rather challenges. This is probably due to the fact the recession was a little bit exaggerated in the Clinton campaign to attack President Bush. The economic downturn was mostly over when Clinton entered office (Gardner, 1994).

> "We face new challenges, from our competitors around the world and from the people we serve here at home, that demand new solutions and creative thinking. Technology offers new opportunities for jobs, for a cleaner environment for better schools, for high-quality health care and for scores of other advances. We must move to seize these opportunities" (Clinton & Gore, 1993).

This quote presents both the general diagnostic frame (challenge for the economy) and motivational frame (seize these opportunities). These statements are accompanied by the need for new thinking. It is argued that defense-dominated technology policy with its "trickling down" of goods to the private sector worked during the Cold War, but that the government now should play a greater role and engage in more private-public partnerships to create more civilian and dual-use R&D (Clinton & Gore, 1993, pp. 7-8). The vision of technology included the *primacy of civil-societies' interests vis-à-vis military interests* (Clinton-Gore Campaign Headquarters, 1992). For example, Clinton and Gore pledged to invest $30 billion, the same amount as Reagan's SDI-initiative, in civil robotics, fiber-optic communications and national computer networks (Broad, 1992).[84] Clinton developed its economic agenda "much in the same way we developed a national security strategy", ushering in a paradigm-shift in technology policy (Broad, 1992). As a result, Clinton created the National Economic Council as an equal to the National Security Council, further underscoring the primacy of the civilian sector vis-à-vis the military.[85] This civilian primacy explains why the Internet was not predominantly understood as being a military technology as in cyber-realism.

What becomes clear is that solutions and goals were not formulated by deriving them from a problem, but they were presented on their own terms. It seems like the new information technology policy was adopted because the key advocate, Gore, wanted to adopt it on its own terms because he genuinely believed in the positive effects and because he wanted to seize the opportunity for third-order policy change (see chap. 2.2.3 Degrees of Change). The central element here is the so-called *"information superhighway"* metaphor which has been coined by Al Gore in the late 1970s. For example in 1989, Gore argued:

> "High-capacity fiber optic networks will be the information superhighways of tomorrow. A national network with associated supercomputers and data bases will link academic researchers and industry in a national collaboratory. This information

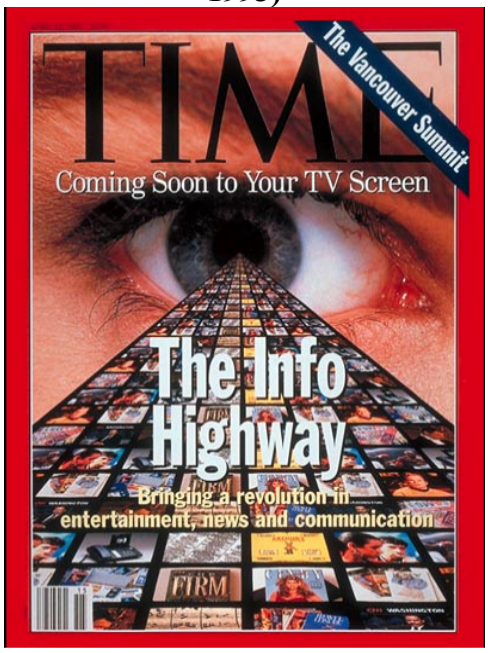
[84] After the Cold War, defense and intelligence budgets were "cut by $60 billion and total acquisition by $100 billion" (Shorrock, 2009, p. chap. 3).

[85] Clinton's relationship to the military and intelligence community can be described as ambiguous because he did not serve in Vietnam and was an anti-war activist. The reduced military spending made matters worse. The relationship with the CIA was also not optimal (Shorrock, 2009, p. chap. 3).

> infrastructure will cluster research centers and businesses around network interchanges […]" (Gore, 1989).

According to Hülsse, metaphors serve the function to explain something new by referencing something old and by projecting the "known to the unknown, metaphors create reality. They constitute the objects they signify" (Hülsse, 2006, p. 403). This metaphor was a clear reference to Gore's father, Albert Gore Senior, one of the prime congressional architects of the US Interstate Highway System in the 1950s, modeled after the German Autobahn. The information superhighway metaphor framed digital networks of networks in terms of the motor-highway system of the 1950s that connected large parts of the US. Data-packets resembled cars, different transport lines such as fiber-optic or copper cable resembled different types of roads connecting cities – initially super computer research sites but later even smaller local area networks. "Speed bumps, danger signs, traffic jams, road kill, and so on – to frame issues involved" (Drake, 1995b, p. 4) all have their digital equivalent such as network congestion or packet-loss. Take for example the Time Magazine cover of 12 April 1993:

Figure 21. Time Magazine Information Superhighway, Source: (TIME Magazine, 1993)



The highway metaphor is interesting not just because of its *assumed* technical similarity between two vastly different technologies (road-networks and packet-switching networks) [86] but also because it assumes similar modes of governance and societal impacts.

[86] Indeed, academics contested the highway metaphor as misleading. For example the interstate-highway system was built and owned by the state, whereas the Internet was build and managed by private entities. The notion of overtaking is not relevant in digital networks and all packets have the same size and speed, meaning

The main envisioned effect was that the information highway "could do for the *productivity* of individuals at their places of work and learning what the interstate highway of the 1950's did for the productivity of the nation's travel and distribution system" (Broad, 1992). The highway is not an end in itself but adopted because of its assumed positive economic impact. As such, the highway metaphor is a powerful technological frame of the underlying paradigm that is driving Clinton's and Gore technology policy. It provided a broader vision of the early Internet and made it tangible for a wider social audience besides technology experts. The media and private sector quickly jumped the hype-bandwagon, outlining "rosy predictions of increased access to information, improvement of education and health care, and a diversity in home entertainment that would all come from the promised "500 channels" of information" (Besser, 1995).

The Information Superhighway quickly became a widely used the buzzword between 1992 and roughly 2002 (see chap. 4.2.7 Junctures: Dot-com Bubble (2000-2001)). This technological frame became so powerful that some present-day politicians still refer to the Internet in terms of the "Datenautobahn" (DPA, 2013). It became a dominant meaning within the political discourse at a time where most people did not even know what it was. Therefore, it is worthwhile to analyze the policy and discourse surrounding it in more detail.

What must be stressed though is that the Information Superhighway itself is more than packet-switching networks and the Internet. It has an "expansive meaning" predominantly understood as a *National Information Infrastructure* (NII) (Information Infrastructure Task Force, 1993, p. 5). This information infrastructure consists of:

> "A wide range and ever-expanding range of equipment including cameras, scanners, keyboards, telephones, fax machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, optical fiber transmission lines, microwave nets, switches, televisions, monitors, printers, and much more" (Information Infrastructure Task Force, 1993, p. 5).

Although the idea of a national information infrastructure (the sum of all information technologies) is largely based on the design of the Internet (at this time represented through the inter-connected super-computer networks such as NFSNET), but it is not completely equivalent to it. At the same time it is modeled very much after the decentralized Internet-architecture and the dominant understanding of the network of networks that developed in the 1970s within the context of the engineering paradigm (see

---

there are no cars or trucks. Also, it is not one single, integrated system with one logic or set of rules, but rather a distributed network of heterogeneous networks (Drake, 1995b, p. 4).

chap. 4.1.3 Constructing the Internet (1972-1991)).[87] Gore himself often conflates the terms, for example when describing the NII for children in the kids-section of a popular newspaper: "The Information Superhighway is a web of communications networks that will forever change the way we live, learn, work and communicate with each other" (Debnam, 1994).

The "promises of the NII" clearly dominate the Taskforce document. This highlights the general optimist and even utopian perspective on the topic, including a series of prognostic frames. The most often uttered promise is economic, namely the creation of jobs and greater economic growth. The following quote is a good representation because it includes other several key codes such as the positive, life-changing affects and the common features ascribed to the Internet, the death-of-distance concept (see chap. 4.2.8 Norms and Key Ideas of Cyber-Utopianism):

> "The NII will enable U.S. firms to compete and win in the global economy, generating good jobs for the American people and economic growth for the nation. As importantly, the NII promises to transform the lives of the American people. It can ameliorate the constraints of geography and economic status, and give all Americans a fair opportunity to go as far as their talents and ambitions will take them." (Information Infrastructure Task Force, 1993, p. 12).

The belief that technology will create *new and better jobs* and will *increase economic growth* is central in these documents and one of the core ideas of liberalism. It highlights the Clintonian civil-economic frame through which digital technologies are perceived. In contrast, the cyber-realist advocacy coalition that forms around the same time in secrecy (see chap. 4.4.2 Ideas: Formation of the Information War Doctrine (1976-2000)) sees technology mainly through a military lens. It could be argued that neoliberalism meets cyber-utopianism, forming a spin-off, which Manjikian calls utopian cyber-liberalism (McEvoy Manjikian, 2010). This positive belief is closely connected to concepts of the *information society* or the theories of the information age envisioned by futurologists like Alvin and Heidi Toffler, whose 1980s aforementioned concept of the *third-wave* (Lewis, 1980) is quite often referred to in political discourse in the 1990s, thanks to their close affiliation to then-Republican leader of the House Newt Gingrich (Murphy, 2012).

But there is more optimism, for example the assumed *positive benefits on education* and *health care*. This is because of the border-spanning and geography-transcending characteristics assigned to the new networking technology:

[87] Gore states "Currently, the information superhighway exists through programs such as the Internet, a massive network of computers that connects an estimated 20 million computer users worldwide" (Debnam, 1994).

> "The best schools, teachers, and courses were available to all students, without regard to geography, distance, resources, or disability […] The vast resources of art, literature, and science were available everywhere, not just in large institutions or big city libraries and museums […] Services that improve America's health care system and respond to other important social needs were available online, without waiting in line, when and where you needed them" (Information Infrastructure Task Force, 1993, p. 5).

What is described here is the general utopian vision of an empowering Internet technology. In cyberspace, physical disabilities, gender, class and physical distance are said to be irrelevant and all that matters is information. It is believed to magically *empower the disadvantaged*, exemplified by Gore by referring to famous physicist Stephen Hawking, who suffers ALS and can only participate in the scientific community with the help of digital technology (Gore, 1994a). This is quite similar to the utopian disembodiment thesis.

The NII is also said to have *democratizing and empowering effects*, allowing all to participate and allowing all to access, thereby almost magically creating equality. The other utopian frame that is uttered here is that of the *global library and the diffusion of knowledge and information*. Al Gore, by referring to his origin from a small, remote town of Carthage, repeatedly stressed that every child, regardless of income and geography, should be able to plug digitally into the library of congress to retrieve knowledge (Gore, 1994a). In sum, the Internet being an information exchange system is said to have *positive effects on education* in the future. Focusing on positive effects creates a powerful vision and narrative.

> "The challenge, therefore, is to ensure that all Americans – rich and poor, urban and rural – have access to the benefits of the NII. That's why President Clinton and I are committed to connecting every classroom, hospital, library and clinic to the NII by the year 2000 so that no one gets left behind on the information superhighway" (Debnam, 1994).

What is indicated in this often-repeated argument is the central social democratic *norm of equal access to the NII* and thus, equal chances. Universal access is quite similar to the idea of openness of the engineering paradigm. This norm of digital equality is uttered repeatedly in sentences like: "As a matter of fundamental fairness, this nation cannot accept a division of our people among telecommunications or information 'haves' and 'have-nots.'" (Information Infrastructure Task Force, 1993, p. 8). Again, the Internet is seen as a tool for social equality and justice. At the same time, Gore provides a future vision connected to a somewhat mystical date – the year 2000, the new millennium.

It was shown that the Information Superhighway agenda included generally positive ideas, but also some normative commitments. The next chapter introduces the central norms of the proposal. It presents the "hands-off" norm that regularizes the government's position vis-à-vis cyberspace.

4.3.3.1 The Hands-off Norm & the American Internet Governance Model

Now that we have covered the ideas and promises of the Information Superhighway, what were the core objectives and goals of this NII policy agenda? These goals tell us something about promoted norms as well as modes of governance of this new system – the primacy of the private sector and the "hands-off" approach of the government. The goals are:

> "Our plan is based on five principles: First, encourage private investment; Second, promote competition; Third, create a flexible regulatory framework that can keep pace with rapid technological and market changes; Fourth, provide open access to the network for all information providers; and Fifth, ensure universal service" (Gore, 1994b).

The primary goal is to foster *private sector investment*, together with the promotion of *competition instead of monopolies*. These are central neo-liberal concepts. The focus on private sector investment underscores the dominance of economic and liberal thinking. The idea here is that the government, through taxes and regulatory policy, can encourage long-term development. The US government acknowledges early on that it will not and cannot build the NII and therefore repeatedly declares a primacy of the private sector in terms of construction and management of the infrastructure (Information Infrastructure Task Force, 1993, pp. 2-3). Although the government will provide some funding, for example for super-computer research, most of the investment comes from private enterprises. Closely connected is the idea to prevent future monopolies in this young telecommunications field. The split-up of AT&T echoes here.

Other central goals are the norms of *universal service* and *open access*. Both are quite similar and "virtually all administration speeches and testimony concerning the NII have repeated these goals", creating a noteworthy consistency of "diverse policymakers singing with one voice", as Cate argues (Cate, 1994). Universal service refers to the norm of equality, that as many people as possible should have access to the technology.[88] This means that it requires affordable prices and a widespread distribution of the system, even

[88] "Although the details of universal service will vary from country to country and from service to service, several aspects of universal service apply everywhere. Access clearly includes making service available at affordable prices to persons at all income levels. It also includes making high quality service available regardless of geographic location or other restrictions such as disability" (Gore, 1994b).

in remote, rural areas. Open access on the other hand refers to the norm of openness or net neutrality promoted by the ARPANET engineers. It states that the infrastructure is open in a way "that users can develop new services and applications or exchange information among themselves, without waiting for services to be offered by the firms that operate the NII" (Information Infrastructure Task Force, 1993, p. 9). It means that the private firms operating the technology should not be able to dictate the services and applications offered therein. As such it reaffirms the idea of distributed or decentralized control and user- or end-to-end driven innovation. According to Gore, "we must have an information-superhighway network that is as accessible and as open and as democratic and as ubiquitous as the telephone network" (Auletta, 1994).

Taken together, these goals and norms lead to a specific formulation of the *appropriate role of government* in this process of building and maintaining the NII. The question what role the government should play within this infrastructure, represents a sense-making and place-finding process, where different actors tried to find an appropriate position in a new technological environment (or policy subsystem) and a period of industrial reorganization (Drake, 1995c). Private firms feared government regulation and control of the system. For example, AT&T CEO Robert Allen accused Gore of proposing that the government will build this infrastructure and lobbied for minimum government involvement (McKnight & Neumann, 1995, p. 138). Part of the confusion seemed to stem from the very highway metaphor, since the original highway system was indeed build be the government (Sugrue, 1994). On the other hand, small firms and (utopian) Internet users feared a radical commercialization and state encroachment on "their" cyberspace (see chap. 4.2.5 Framing Cyberspace as the Electronic Frontier (1990s)), in which giant corporations could suppress user innovation and expression, for example by dismantling net-neutrality, open-access and the idea of decentralized, distributed control (Drake, 1995c, pp. 17-19). This debate forced Gore to repeatedly articulate the role of the state in several interviews. The core features of his argumentation are the following.

First, Gore repeatedly stressed the *primacy of the private sector* and corporations and companies in building and controlling the infrastructure, already spending more than $50 billion annually with which the government cannot compete anyway (Information Infrastructure Task Force, 1993, p. 6). "The private sector will build and run virtually all of the National Information Infrastructure, the President and the Vice President have stated clearly that the Federal government has a key leadership role to play in its development" (Information Infrastructure Task Force, 1993, p. 19). This is an important deviation from classical utopianism, which sees the primacy for controlling the Internet with the digital

natives (see chap. 4.2.5 Framing Cyberspace as the Electronic Frontier (1990s)). With this more liberal interpretation of utopianism, economic actors are framed as the dominant ones. It is argued that it is appropriate for them to control the physical cyber-space infrastructure and the digital services therein. According to Gore, the state should only provide a "sense of direction" a a vision: "one role government can play is to articulate vision, to put certain issues and goals on the public agenda" (Sugrue, 1994). The NII agenda defines the government as a "catalyst to promote technological innovation and new applications" (Information Infrastructure Task Force, 1993, p. 6). Other terms describing this approach are "neutral" (Sugrue, 1994), not favoring one actor over the other but maintaining principles of fair competition and the prevention of monopolies. In other words, it is not the government that decides what is built by whom, but rather it formulates a broader vision and gives the private sector a relatively free hand. What is quite interesting is that "much of the leadership on NII-related issues comes from the Department of Commerce" (Cate, 1994, p. 47) and the NII-Task Force and not for example the FCC or the military. However, this is not the radical laissez-faire approach of Presidents Reagan and Bush, but represents something that Gore and others call "*flexible regulation*". Journalist Ken Auletta describes it as:

> "The Clinton-Gore Administration wants government to assert a role. "We want to serve the public interest with a minimalist approach to regulation," Gore said, but his definition of government's role proved not to be minimalist. Asked to describe government's mission, he answered, "Referee. Facilitator. Envisioner. Definer." Under Reagan and Bush, he said, government was a mere spectator" (Auletta, 1994).

Flexible or minimal regulation is described as: "to devise investment incentives, to ensure affordable universal service, to keep the highway democratic, and to protect both privacy and intellectual-property rights" (Auletta, 1994). It is a more proactive approach. Gore and other democrats criticized the inability of the old Reagan laissez-faire approach to foster civil development and to create benefits for more actors than just large corporations.[89] For example, in a speech Gore argues: "We need this limitation to ensure that no single giant entity controls access to homes and offices. We cannot permit the creation of information bottlenecks that adversely affect information providers who use the highways as a means of supplying their customers" (Gore, 1994a). Here we see the interconnection of different

[89] "All these guys who say government has no role in this–if their philosophy had prevailed when A.T. & T. was broken up, A.T. & T. would not have been broken up. And this competitive explosion would never have taken place. And we would not dominate the fastest-growing market in the world today." Government's challenge, Gore said, is to "steer the enterprise away from the shoals" of both monopolistic business practices and bureaucratic government" (Auletta, 1994).

norms forming a norm-network (see chap. 2.1.2 Critique of Deontological Norms). The government makes sure that its core norms of equal and universal access, the norm of openness and the benefits for education are indeed realized, that competition is maintained and monopolies are prevented, but does not attempt to do more. This is closely connected to the "no one should be left behind" norm of social justice but also to the ARPANET norm of decentralization of authority.

Without going into more details of telecommunications regulation, it can be said that Clinton and Gore promoted a "hands-off" approach in government behavior towards digital technologies. In theoretical terms, this policy provides an important counter-signifier, the information superhighway, and counter-appropriates its use and governance of the Internet (see chap. 2.3.6 Combining the Frameworks). The policy proposal includes ideas and norms conceived within the engineering paradigm, general cyber-utopian but also new neo-liberal ideas. It is not the full-scale neo-liberalism favoring the market over regulation, as proposed by Reagan and Bush, but adds a slightly more assertive role for the government. At the same time, it is not full-fledged utopianism as proposed by the early adopters. It should have become clear right now that during these early days, the government did not claim any right to interfere with the development of this infrastructure nor does it claim a right to tap into this infrastructure. This represents the basic model of early US Internet-governance which was developed between 1992 and 1995. Because the Democrats held both Houses in Congress, they were able to push through with this agenda. However, in the mid 1990s the topics shifted somewhat from building this infrastructure to the questions of securing this infrastructure, which will be the topic of a later chapter (see chap. 4.4.4 Politics: Turn to Realism - Critical Infrastructure Initiative (1996-1999)). The next chapter will introduce Gore's framing of the Internet in democratic terms, arguing that no state alone should control this technology.

4.3.3.2 Global Framing of the Internet

Now that the central promises and goals have been covered, let's turn to the perception and description of this technology. What meaning an actor has of an object can best be shown when he/she is describing this very object to an audience, that is unfamiliar with it. In Buenos Aires 1994, Gore presented the NII initiative at the World Telecommunication Development Conference held by the International Telecommunications Union, the governing international body for the harmonization and governance of telecommunication. This conference was the (successful) attempt to inspire the development of NII in other

states – in the image of the US Internet model – and interconnecting them in a Global Information Infrastructure (GII).

In his speech, Gore starts by referring to common utopian frame, namely that of the interconnected *global-village* or even McLuhan's concept of a global nerve system "of communications around the globe, linking all human knowledge" (Gore, 1994b). These utopian metaphors are used to describe the early Internet and the promises of global interconnectivity. It is important to highlight that the concept of globalization was a central theme in political academic debates of the early 1990s.

> "These highways or, more accurately, networks of distributed intelligence–will allow us to share information, to connect, and to communicate as a global community. From these connections we will derive robust and sustainable economic progress, strong democracies, better solutions to global and local environmental challenges, improved health care, and – ultimately – a greater sense of shared stewardship of our small planet. The Global Information Infrastructure will help educate our children and allow us to exchange ideas within a community and among nations. It will be a means by which families and friends will transcend the barriers of time and distance. It will make possible a global information marketplace, where consumers can buy or sell products" (Gore, 1994b).

Several of the aforementioned norms and ideas are woven together into one narrative. The first thing to note is the description of *networks of distributed intelligence*, which is a technological frame developed by the ARPANET engineers. That Gore uses this (accurate) description is noteworthy and highlights his familiarity with the original concepts of the Internet. One explanation is that ARPANET engineers such as Leonard Kleinrock or Vint Cerf served as advisors for Gore. *Interconnectivity* and increased connections between nations are described as positive. They are said to produce better economies, stronger democracies and solutions to global (climate) challenges. Other utopian ideas such as the *transcendence of time* and the *death-of-distance*, together with social, economical, political, ecological and educational benefits are clearly articulated and function as prognostic frames. The general optimist undertone is quite striking in this quote, but there is more:

> "In a sense, the GII will be a metaphor for democracy itself. Representative democracy does not work with an all-powerful central government, arrogating all decisions to itself. That is why communism collapsed. Instead, representative democracy relies on the assumption that the best way for a nation to make its political decisions is for each citizen – the human equivalent of the self-contained processor – to have the power to control his or her own life. To do that, people must have available the information they need. And be allowed to express their conclusions in free speech and in votes that are combined with those of millions of

> others. That's what guides the system as a whole. The GII will not only be a metaphor for a functioning democracy, it will in fact promote the functioning of democracy by greatly enhancing the participation of citizens in decision-making. […] I see a new Athenian Age of democracy forged in the fora the GII will create" (Gore, 1994b).

Now, this lengthy quote is quite remarkable and worthwhile to be analyzed more deeply. First he says that the Global Information Infrastructure (GII) is a *metaphor for democracy itself.* He seems to say that networks of distributed intelligence are essentially democratic because there is no "all-powerful central government". Power and intelligence rests with the end-nodes, the users or citizens of the network. This clearly refers to the norm of decentralization put forward by ARPANET engineers (see chap. 4.1.3.1 Artifact: Internet Protocols and Norms), but goes beyond it, since the latter would not go so far as describing their system as inherently democratic (Crocker, 2015). Gore assumes an inherent connection between the Internet and democracy (diagnostic framing). The belief that the Internet will lead to greater democratization both *within* Western democracies as well as outside of them in *autocratic regimes*, is central in this speech. Domestically it is argued that the Internet will lead to greater government transparency and accountability. Government services could be offered digitally and government information could be more easily disseminated, resulting in a cheaper, better, more efficient and transparent government (Clinton & Gore, 1993, p. 20; Information Infrastructure Task Force, 1993, p. 11).[90]

He then states that communism collapsed because of power-centralization and technology. The positive role of technology (fax machines, photocopiers) in the collapse of communism and the promotion of democracy is a common diagnostic frame at the time (Kedzie, 1997). It can be traced back to the so-called *"dictator's dilemma"* that was formulated by former Secretary of State George P. Shultz, on a trip to Moscow in 1985 (Shultz, 1985). The assumption is that information technology allows the dispersion of government-critique and the organization of protest movements such as Solidarność. When authoritarian regimes try to control these technologies, they will hurt their economies and fall behind economically. If autocracies allow information technologies to maintain economic development, their power-structure is said to erode because they lose control

[90] To make this argument more substantial, the White House launched its official website on 21. October 1994. Besides videos of Socks, Bill Clinton's cat, users could tour the White House electronically as well as access government documents and speeches by the president (McCullough, 2014b). This website started the practice that citizens can access government information on their websites, which is a taken-for-granted norm in modern Western societies that is mostly realized by technological means. "As of February 10, 1994, the Administration had published electronically more than 1600 documents and had processed more than 220,000 electronic requests for information since September 1, 1993" (Cate, 1994, p. 45). Also in 1994, Bill Clinton sent the first Email to Prime Minister Carl Bildt of Sweden (Clinton, 1994).

over information circulating their territory, which then allows the formation of oppositional forces.

The dictator's dilemma could be interpreted as an identity construction with the "we", the democratic non-internet-controlling Western governments and the "other", the authoritarian regimes who control the Internet and the information space. In other words, information technologies are framed as tools that decentralize power structures and control and thus are inherently destructive for authoritarian regimes. This is a further affirmation of the idea that democratic governments should keep their hands off these technologies. When screening more contemporary documents of the time, these utopian frames are quite prevalent.[91] Gore basically argues that the GII and the Internet are positive forces for global development. In other words, not just some LSD-taking cyber-utopians believed in the democratizing effects of technology, but it was a widespread belief shared in political and intellectual circles.[92]

Turning back to Gore, he further argues in his 1994 speech that information freely distributed over a communications network empowers citizens and lies at the core of democracy as well as the Internet. This is what he seems to say when he *equates the GII and the Internet with "democracy itself"* (Gore, 1994b). Both are similar entities that rely on the same norms: information should float/circulate among citizens freely and uncensored, freedom of expression is to be guaranteed and power should be distributed. He refers to the Athenian democracy, which seems to imply a highly distributed political power structure such as in the direct democracies in Greece in the classical antiquity. The belief that *technology is positively tied to democracy* lies at the core of both cyber-utopianism and its liberal variant advocated by Gore and Clinton (see chap. 4.2.8 Norms and Key Ideas of Cyber-Utopianism).

This perception of the Internet as democratic shapes the perceived appropriate roles of states. He does not just say that the Internet is based on democratic norms; he also argues that the Internet should be governed in the same manner. The belief in the democratizing effects of the Internet technology leads to the formulation of a core norm of cyber-liberal utopianism: The *Internet should be a grassroots democracy*. No single

[91] In his RAND article, Kedzie traces the evolution of the "information-technology correlates with democracy" thesis. He discovered that it was shared by several state leaders during the 1980s, among them famous figures such as Mikhael Gorbachev (Kedzie, 1997).

[92] Even the highly respected and independent Office for Technology Assessment (OTA), that was dismantled in 1995, repeatedly affirmed many of the beliefs uttered by utopians. For example: "The prospects for democracy in developing countries are also greater because of technology advances. For example, improved networking capabilities, which make it possible to develop specialized, distributed, many-to- many applications such as bulletin boards and groupware, can help individuals locate information; identify like-minded people; deliberate their ideas, organize their activities; and lobby for their points of view" (Office of Technology Assessment, 1995). This is key evidence for the widespread appeal of utopian thought.

authority should control it. He stresses that the development of a GII must be a cooperative effort and that "It cannot be dictated or built by a single country. It must be a democratic effort" (Gore, 1994b). Again, he repeated the idea of decentralization and the distribution of authority that is underlying TCP/IP. No single country should dictate (i.e. control) or build the system. This is a reaffirmation of the hands-off norm of the American Internet Governance Model that was outlined by the Clinton administration domestically with the NII initiative.

Gore also reaffirms the sharing-norm of the ARPANET engineers: "As the GII spreads, more and more people realize that information is a treasure that must be shared to be valuable. When two people communicate, they each can be enriched – and unlike traditional resources, the more you share, the more you have" (Gore, 1994b). The norms promoted by Gore are an aggregate of those developed within the context of ARPANET as they became embedded in the TCP/IP protocol and cyber-utopian ideas. What Gore does – in theoretical terms – is to reaffirm this historic trajectory of the technology as envisioned by the engineering paradigm and, at the same time, gives it greater relevance. By lobbying for other states to follow the American NII model, he thereby reinforces these norms by managing that they diffuse globally along with fiber-optics and the Internet technology. Gore acts as a norm-entrepreneur, promoting the American "hands-off" governance norm as well as the idea of a democratic Internet in front of a wider audience. This is a global bottom-up process of norm-diffusion emerging from the level of the nation state.

The graphic summarizes the key elements of the paradigm and how it frames the Internet in utopian and liberal terms (color transition). But it was not all just words and rhetoric. The ideas had a real material impact in terms of technological artifacts as well as in terms of politics, as the next chapter shows.

Figure 22. Cyber-liberal Utopianism framing the Internet (own diagram)

Cyber-Liberal Utopianism	
problem → goal	- Revitalize economy - private sector investment
anticipated use	- Information Superhighway as means for: education - healthcare - economic development, jobs - democratic participation - global cooperation & problem solving by states (climate change)
social elements (norms, power)	- Primacy of the private sector in building and governing cyberspace - State should adopts a „hands-off" posture with flexible regulation, prevention of monopolies - no state alone should control cyberspace, idea of a democratic governance of the Internet - universal and equal access - openness and net-neutrality
user identity	- digital haves and have nots - liberal democrats vs. authoritarian regimes

Social reconstitution

Internet	
material dimension	**social dimension**
- Computer Networks - Cable, Satellite TV - Entertainment Media	- **preferred meaning:** Internet as local and global Information Superhighway - privatization of Internet backbone infrastructure - Internet as civilian, economic and not military technology - Internet as Athenian democracy - Internet as economic driver, market

4.3.4 Artifacts: Privatizing Control over the Internet

According to Bennett and Checkel, an analysis of ideational factors "need[s] to show that norms prevented actors from doing things they otherwise would have done" (Bennett & Checkel, 2014, p. 34). This chapter shows that the "hands-off" norm was not just rhetoric, but had material implications.

The material outcome of the cyber-liberal policy was the privatization of the Internet backbone, i.e. the technological infrastructure carrying and switching large portions of Internet data. As the previous chapters have shown, the Internet's predecessor ARPANET was built and funded by military R&D and thus state-owned and controlled (see chap. 4.1.2 The Social Construction of the ARPA-Network (1966-1972)). In the 1980s, most of the digital infrastructure was transferred to the National Science Foundation, a state-owned and funded entity (see chap. 4.1.3.3 The Internet Backbone). In other words, the government could exert a great deal of control over this technology and it did, for example by regulating acceptable use of ARPANET and NSFNET (National Science Foundation, 1992). This policy strictly prohibited commercial applications on NSFNET and thus prevented economization or commodification of services (National Science Foundation, 1992).

The Gore Bill of 1991 (High Performance Computing Act) first outlined the goal to privatize NSFNET. Since then the plan was set in motion to replace the one and only Internet backbone operated by the NSF with multiple, privately-owned backbones, interconnected through Network Access Points (Shah & Kesan, 2007). In other words, central switching nodes (so-called Internet Exchange Points or IXP) carrying data were

gradually transferred from the state to private corporations like Sprint, MFS, or Ameritech. In 1995, NSFNET was decommissioned and in August 1996, NSF transferred sponsorship of the last public access points to the private sector (Shah & Kesan, 2007). In 1993, the Clinton administration moved the registration of domain names – the Internet addresses of websites (.com, .org etc.) – to a company called Network Solutions (Shorrock, 2009, p. chap. 3).

In 1998, the Department of Commerce proposed to hand over control of the global Domain Name System (DNS),[93] from US authorities to a new and private organization called ICANN, the Internet Corporation for Assigned Names and Numbers, thereby transferring an important means to control global cyberspace to a private entity (Hofmann, 2015). The rationale for this move was:

> "A private coordinating process is likely to be more flexible than government and to move rapidly enough to meet the changing needs of the Internet and of Internet users. The private process should, as far as possible, reflect the bottom-up governance that has characterized development of the Internet to date" (U.S. Department of Commerce, 1998).

In other words, this decision was very much in line with the ARPANET community's approach to Internet governance. The very same spirit can be found in the founding statement of ICANN: The Internet "shall operate for the benefit of the Internet community as a whole" (Ryan, 2013, pp. 101-103). ICANN and similar multi-stakeholder models institutionalized, to some degree, the hands-off norm in a governance model and the idea that no single authority should control the Internet. If the US government wanted to control cyberspace, it would not have privatized it since prior to this, the government, through the NSF had formal stewardship over the technology. This shows the working of the "hands-off" norm.

In retrospect, history proved Gore right. The ITU conference in 1994, leading to the Buenos Aires declaration (International Telecommunications Union, 1994), was a key milestone in the global diffusion of both the Internet and the central democratic norms. Instead of several, disconnected and incompatible local or national information infrastructures relying on different technologies (a balkanized Internet), one of the outcomes was the global and open Internet that we have today. Many states, especially

[93] Domain names are crucial for the use of the Internet, because they translate abstract numeric IP addresses into comprehensible names. Since there can be only one domain name called www.whitehouse.gov, it is of crucial importance who assigns these domains to public or private actors. According to Goldsmith and Wu, the DNS system is of great economic importance, since domains are valuable, but also they are a crucial means of political control over the Internet (Goldsmith & Wu, 2008, pp. 31-32). Those who control the root authority of the DNS system could for example prevent a political antagonist or another country from obtaining a domain name, and as such preventing a website to be found on the web.

European states like Germany, followed the US role model of Internet governance. They, too, privatized former state-monopolistic telecommunications providers, created commercial IXP and allowed open-access for smaller service providers and user-driven innovation. They also adopted similar governance norms. In theoretical terms, Gore's cyber-liberalism pre-structured the global development path of the early Internet and created a lock-in effect that institutionalized the early core norms of the Internet such as open-access and the idea of democratic Internet governance.

However, this perspective became challenged by different actors who did not agree with the "hands-off" perspective and outsourcing of government control over the Internet. The next chapters will introduce some junctures where different actors, most notably law-enforcement actors adhering to a cyber-realist paradigm, advocated for state-control over the Internet. These attempts ultimately were not very successful.

4.3.5 Junctures: Policy Attempts to Control the Internet (1993-1996)

This chapter introduces several key events where utopians and realists engaged in public discourse about the governing norms of the Internet. This implies the process of contesting paradigms and norms that are not yet dominant. During the early 1990s, cyber-realist advocates made several attempts to control various aspects of the Internet. The first attempt, the so-called Clipper-initiative, aimed at establishing control on the technological level, by interfering with the standard-setting process and by pushing for government-controlled encryption technology. The second attempt was to regulate technology via policy, by demanding that private companies support FBI[94] wiretapping operations of the Internet with the CALEA initiative. The third attempt was to control Internet content, i.e. the distribution of pornographic material. All these initiatives faced major public resistance from a wide variety of different actors: engineers, private corporations or cyber-utopian or liberal advocacy groups or even the political opposition and the Supreme Court. In the end, it can be argued that utopian ideas were dominant in the early days of the Internet. Because of this dominance, attempts to control the Internet by cyber-realist advocates were removed from plain sight and developed in secrecy, until the time was ripe for them to re-emerge, which of course was 9/11.

4.3.5.1 Policy: The Clipper Chip (1993)

The first noteworthy juncture where different paradigms clashed with each other was the Clipper-debate in 1993. In analytical terms, it is a techno-political drama discourse

[94] Federal Bureau of Investigation.

(Pfaffenberger, 1992a) about the reconstitution of the technical artifact Internet. It happened directly at the beginning of its mainstream diffusion. The debate was about how the Internet and information sent over networks could be made more secure by encryption. [95] The very purpose of encryption is that only sender and receiver and no third party can read the content of communication. The debate addressed the fundamental issue of how security should be technically and politically implemented and who should be responsible: the state, industry, civil society or all of them. In larger terms, it was also a debate about the power of the state vis-à-vis the power of the Internet users. Since I have analyzed the Clipper discourse in higher detail elsewhere (Schulze, 2017), I will only provide a short overview of the main positions.

On the one hand, cyber-realists like the FBI and NSA argued for a greater role of the government in regulating and steering the early diffusion of digital technologies such as the Internet and digital telephony. They argued that the government should influence the code-design of encryption-technologies. FBI and NSA argued that encryption would make Internet surveillance harder and thus they had the goal of building a "backdoor", enabling government monitoring of encrypted messages (Lessig, 2006, p. 66). In theoretical terms, they argued for a reconstitution of Internet technologies in a way that the US government could control and monitor the information traveling on the Information Superhighway just like it could wiretap traditional telephony. It was the first major attempt of the US government to force a norm of control upon the spreading Internet technology. The norm included that the US government (and only the US government) would have a legitimate right to decrypt any digital communication between any two individuals carried over digital networks. Had it been successful, the US government would have potentially been able to decrypt all future Internet communication (McCullough, 2014a).

On the other hand, there was a loose coalition of cyber-utopians (like the EFF), Internet-users and private companies arguing for the "hands-off" norm that the government should not interfere with the software design of Internet core technologies such as encryption. Ultimately, the latter group "won" this war on cryptography, as later NSA General Hayden admitted (Hayden, 2016a). What was this "crypto-war" about (Levy, 1994)?

[95] Encryption translates a plaintext (the message to be send) into a piece of gibberish or cipher-text by using a key that describes how letters are to be exchanged. The Romans interchanged every letter of plaintext with the letter that followed three steps further in the alphabet. The plaintext "VENI VIDI VICI" would be encrypted to "YHQL YLGL YLFL. The cipher-text can only be reversed into plaintext by knowing the key (replace by 3 steps down the alphabet). Stronger encryption uses longer keys that cannot be randomly deciphered (National Research Council, 1991, pp. 252-253).

Historically, encryption was a top-secret, centralized technology owned and controlled by the military and the state. In 1976, researchers Whitfield Diffie and Martin Hellman published the revolutionary concept of public-key cryptography that promised almost unbreakable encryption (Diffie & Hellman, 1976). The top-secret British Intelligence Agency GCHQ[96] had developed a similar system a bit earlier but kept it secret (Rid, 2016, pp. 303-314). With the scientific publication of public-key cryptography, the genie was out of the bottle and potentially everyone could use top-grade military technology. The knowledge of secure cryptography was decentralized from NSA and GCHQ and distributed among researchers worldwide. After the release of public-key cryptography, NSA director Bobby Inman gave a famous "the sky is falling" speech in 1979, warning that "non-governmental cryptologic activity and publication […] poses clear risks to the national security" (Levy, 1993). NSA and GCHQ began to lobby their governments against the widespread use of public-key cryptography, arguing for outlawing civil use of the technology and (allegedly) threatening researchers of the National Science Foundation with gag-orders, trying to cut public funding of civil crypto-research (Bari Kolata, 1980). As a result of this successful lobbying effort, cryptography was classified as military, dual-use technology and thus was placed under a strict export control regime which prohibited widespread public adoption (Kehl, Wilson, & Bankston, 2015, p. 12).

The debate resurfaced in 1992 when AT&T announced a cryptographic phone for the consumer market that allowed encrypted und thus surveillance-proof phone calls. This market introduction threatened the core function of the National Security Agency and its primary mission to decipher communication (McCullough, 2014a; Levy, 1994). NSA feared that the new Internet could spread globally with encryption technology on the application layer (see chap. 4.1.2.3 Artifact: The Network Control Program). If, for example, AT&T developed an encryption standard that would come bundled-together with every AT&T Internet access contract sold, wiretapping these AT&T connections would become very hard. Thus, the NSA and FBI argued that "the deployment of strong cryptography that is widely used will diminish the capabilities of those responsible for SIGINT" (Dam & Lin, 1996, p. 101f.).[97] NSA director and later Director of National Intelligence Michael McConnell warned that the agency would be "going dark" if the Internet would diffuse world-wide with encryption in place (Hayden, 2016a).[98] For cyber-realists, this represented the major problem that guided their agenda.

[96] Government Communications Headquarter.
[97] SIGINT means Signals Intelligence, the interception of radio-waves or any other types of communications signals.
[98] The metaphor means that one stream of interruptible communication would become unusable and thus the NSA would sit in the dark, not knowing what was communicated over digital channels.

To prevent such a scenario, the NSA engaged in a standard-setting process by designing a software algorithm for encryption (called Skipjack) and a tamper-resistant computer-chip (called Clipper) that executed the algorithm and was to be attached in the hardware of communications devices like phones, Fax or modems (U.S. Senate, 1994). The Clipper chip would be built into Internet devices and then scramble all messages going through so that two parties (sender and receiver) could easily use encrypted messages (like E-mail). The caveat was that the NSA devised the algorithm to include a third key that could unscramble the encryption between two parties without their knowledge. This third key would be held in escrow by two separate government institutions and intelligence services could obtain the key with a court order. With this system called key-escrow, government law enforcement could override any encrypted communication and wire-tap into encrypted, digital conversations (The White House, 1994). If an NSA standard instead of a public standard would become mainstream, then communication-interception in the digital age would be guaranteed.

Originally, the NSA presented the proposal to the George H.W. Bush administration but it did not implement it (Levy, 1994). Instead, on February 9 1993, the NSA proposal was directed, via the FBI, towards the White House (Sessions, 1993). The newly elected Clinton-Gore Administration, which in its election campaign relied heavily on technological investment and utopian visions such as the advancement of the Information Superhighway, decided to adopt the proposal (McCullough, 2014a). An interesting question is why the liberal and utopian inspired Clinton/Gore administration co-sponsored this cyber-realist technology initiative. Dam and Lin argue that this was presidential pragmatism: The Clipper chip seemed to be a reasonable compromise between doing nothing, thus endangering surveillance capacities for law-enforcement and global signals intelligence, or by having no possibility for secure Internet communication at all (Dam & Lin, 1996, p. 170). The key-escrow scheme, with the warrant-requirement, theoretically prevented abuse by intelligence and law-enforcement agencies. Thus, in theory it sounded like a good compromise between safeguarding the privacy of individual citizens and law-enforcement interests. However, when initiating the proposal in 1993, the government must have been aware of a potential backlash, indicated by its reluctant commitment to the initiative.

On 16 April 1993, the administration announced the Clipper initiative as "a voluntary program" between the government and industry (The White House, 1993b). It was not a policy bill (that probably would not have made it through Congress), but a technological initiative that basically bypassed the legislative process and thus was not mandatory. The

initiative was framed as a compromise or balance between increasing citizen's privacy with secure communication, the interest of the private sector for secure global communication (to protect intellectual property or financial transactions) and the "legitimate needs of law enforcement" in fighting terrorism, drug-traffickers and child molesters (The White House, 1993a). The terrorist threat frame is a key figure in cyber-realist discourses, even today. The "going dark" metaphor (diagnostic frame) also is highly prevalent in cyber-realist discourses (Comey, 2014). One other key argument put forward by realist advocates was that the Clipper chip was state-of-the-art and thus potentially better and more secure than competing cryptographic technology available on the market (Brickel et al., 1993). This was a major selling point.

Further anticipating a strong public reaction, the White House announced a one year review period for public hearings with implementation of the Clipper initiative one year later. During this period, a large grass-roots movement consisting of technology companies, computer-science, the early Internet avant-garde and advocacy groups such as the EFF loudly opposed this perceived government standard-setting attempt. Whitfield Diffie argued that Clipper created a backdoor in an otherwise secure system that would make the chip insecure. He criticized NSA's role in the standard-setting process, because it was the mandate of the National Institute of Technology (NIST) to develop public standards. Furthermore, NSA held the source-code classified so it could not be vetted by the expert community, which is a common peer-review practice in academia (Diffie, 1993).

Convincing private companies to build a Clipper chip into their devices was seen as necessary government regulation of the market. Companies argued that this would drive up manufacturing costs and would make US cryptographic products uncompetitive on a global market, since nobody, especially not actors with malign intent, would buy technology of which he/she knew that the US government could listen in through a backdoor (U.S. Senate, 1994). Cyber-utopians warned of the privacy implications and that surveillance of communications is a feature of authoritarian regimes that should not be replicated in a democracy (Diffie, 1993), very much in line with the argument of the dictator's dilemma (see chap. 4.3.3.2 Global Framing of the Internet).

In sum, most crypto-experts, tech companies and renowned institutions such as the NIST urged the government to stop the initiative.

> "In 1993, the Digital Privacy and Security Working Group — a coalition that included both privacy advocates and communications and computer companies like Apple, AT&T, Hewlett-Packard, IBM, Lotus Development Corporation, Microsoft,

> RSA Data Security, and Sun Microsystems — submitted a letter to President Clinton expressing concerns about the Clipper program" (Kehl et al., 2015, p. 7).

The National Institute of Technology conducted an expert hearing on the matter: "we received 320 comments, only 2 of which were supportive" (Levy, 1994). Several famous engineers such as Internet pioneer Vint Cerf opposed the proposal (Cerf, 1993). An open letter by a group called Computer Professionals for Social Responsibility, which included many of the nation's leading cryptographers and security experts from January 27 1994, argued strongly against the initiative. The letter was the first electronic petition distributed via E-mail, which generated 45000 signatures (Computer Professionals for Social Responsibility, 1994). In a CNN poll, 80% of the public opposed the initiative (U.S. Senate, 1994).

The death-blow to Clipper came in late 1994, when a computer researcher found a fatal flaw in Clipper's software code, thus falsifying NSA's statement that Clipper would be more secure than anything else on the market (Kehl et al., 2015, p. 9). Republicans and Democrats also questioned the few benefits of the system compared to the relatively high costs (U.S. Senate, 1994). The National Research Council (NCR) argued against NSA: "the advantages of more widespread use of cryptography outweigh the disadvantages" and "the widespread nongovernment use of cryptography in the United States and abroad is inevitable in the long run" (Dam & Lin, 1996, p. 300). One of the reasons why the counter-movement was successful was because their arguments were better, as later NSA generals acknowledged: "America is simply more secure with unbreakable end-to-end encryption" (Hayden, 2016a). Thus, the voluntary initiative was silently dropped by the Clinton administration and over time, the strict export controls for encryption where relaxed.

In 1996, Al Gore acknowledged the value of encryption for e-commerce and launched an initiative to rethink crypto-politics. Cryptography would no longer be regarded as a military dual-use technology. White House Executive Order 13026 placed encryption technology under the export regime of the Department of Commerce, instead of the State Department. In 1999, the White House announced to remove all restrictions on the export of cryptographic technology (Kehl et al., 2015, pp. 15-17). The Internet itself contributed to this relaxation because open-source cryptography was available for free online, thus completely circumventing the US export control logic. Other countries, like Germany, replicated this process.

From a theory point of view, the crypto-war discourse was about norms and about the appropriate role of the state and its citizens with regard to technology. Cyber-realists wanted to maintain the historical regularization that put them in charge of cryptographic

matters while excluding the general public and most of the private sector. Cyber-utopians engaged in counter-appropriation, claiming rightful access to cryptographic technology and arguing for the citizen's rights to use cryptography to guarantee privacy without government interference. Cyber-realists in contrast argued that the government has the right to control and monitor encrypted communications with a warrant, if law-enforcement or signals intelligence demand it. By sidestepping the NIST in developing a national standard, the NSA actively tried to intervene in code and hardware design for Internet-devices. As such it can be seen as an attempt to alter the core functionality of the Internet in order to realize cyber-realist interests. It did not aim at the Internet protocols directly, but was directed at the Internet devices running applications such as E-mail or web-browsing (it was an end-to-end control attempt so to speak). This was supported by strong lobbying for the maintenance of export controls. Had the program been successful, it could be counterfactually speculated, the Internet would have spread domestically and maybe even globally with a US government backdoor in place. The early Internet thus would have represented more the Havard Model of Internet control (in Lessig's analogy) and not the free Chicago model as it later turned out (Lessig, 2006, p. 34). This however, was not the case and the Internet spread globally without encryption built-in.

The NSA attempt to publicly shape technology design failed and it did not try the same approach again. Instead, it shifted tactics and began to approach the problem of intercepting digital technology in secrecy, as will be shown in a later chapter (see chap. 4.4.7 The Politicization of Cyber-Realism with the War on Terror (2000 - 2008)). The Clipper episode also showed the relative dominance of cyber-utopian norms. The public, the private sector and even Democrats *and* Republicans endorsed the "hands-off" norm, being skeptical of the fact that the US government tried to assert itself as a central authority being able to monitor encrypted Internet communications. Thus, this juncture increased the relative dominance of utopianism and liberalism vis-à-vis cyber-realism in the public discourse. This was also the case during the next juncture, which dealt with similar issues.

4.3.5.2 Policy: Wiretapping the Internet with CALEA (1994)

Another instance of an early attempt of cyber-realist advocates to dominate the digital revolution before it was even in full swing was the "*Digital Telephony Bill*", an attempt to mandate service providers to enable wiretapping at their digital switching-infrastructure. Like the Clipper proposal, the initiative came from the FBI, the predominant public cyber-realist advocate at the time. It can be argued that after the Clipper proposal, NSA preferred

to stay hidden from plain sight. Because it deals with the Internet only indirectly, I will not conduct a full-fledged policy analysis including the surrounding discourse, but rather offer a quick snapshot of the debate and its outcomes.

The proposal of the FBI was initially aimed at the George H.W. Bush administration for implementation in 1992 (BeVier, 1999, p. 1071). However, because of the general skepticism towards the bill and the upcoming election, it was not implemented in time. After Clinton's election, the FBI started another attempt to lobby for the bill in Congress. In its original form the proposal was quite broad and represented cyber-realist ideas to its core. The bill was designed to address the "digital telephony problem" or the difficulties of wiretapping digital and packet-switched telecommunications. Since the late 1980s, law-enforcement agencies recognized that "the digital technology of computers would render existing phone surveillance techniques useless" (Cohen, 1994). Traditional wiretaps[99] aimed at copper-lines, which could be easily tapped with Alligator-Clips (Landau, 2010, p. Chap. 4). The increasing number of cellular phones, integrated voice and data or value-added services, the rise of the PC and the increase of telecommunications providers other than AT&T (to around 2000) made this old technique obsolete (U.S. Congress, 1994, pp. 23-25). FBI Director Louis Feech defined the cyber-realist problem in a congressional hearing:

> "The United States is facing a grave and growing problem. New telecommunications technology is impeding or preventing law enforcement from conducting court-authorized electronic surveillance, or what we call wiretapping. The problems are just beginning, in my view. […] It will be a disaster if this and other emerging telecommunications technologies spread nationwide without needed law enforcement safeguards " (U.S. Congress, 1994, pp. 5-6).

During this congressional hearing the FBI established two major discursive frames, which are remarkably similar to NSA's "going dark" metaphor (Inman, 1979) and that of FBI director James B. Comey in 2016 about encryption. The fear of "going dark because of the digital revolution" and the frame that the "FBI fell behind the curve of technical capabilities" is remarkably stable (Schulze, 2017). It is argued that electronic surveillance would virtually become impossible and that law-enforcement would lose its crime-fighting

[99] Wiretappig in the US is a controversial issue because it is the most intrusive form of surveillance. Therefore, it was discussed by the Supreme Court several times. Initially, intercepting communications was forbidden (since 1934 with the Communications Act), but over time, Supreme Court altered this norm. The 1968 Omnibus Crime Control and Safe Streets Acts of 1969 prohibited all wiretapping except for law-enforcement. There needs to be a court order that outlines probable cause and explains that wiretaps are the ultima ratio in an investigation (Cohen, 1994).

ability (BeVier, 1999, p. 1073). The digital telephony bill was to be the solution to this "grave" problem because it aimed to:

> "preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without [either] impeding the introduction of new technologies, features, and services" (BeVier, 1999, p. 1051).

The solution was controlling the very design of digital technologies and their market. The FBI-sponsored bill mandated that the providers of electronic communications, defined quite broadly to include telecommunications carriers, information services *and* ISP, grant the government the capacity to intercept wire *and* electronic communications services. The FBI demanded the capability to gather meta-data such as the timing and duration of a call (or Internet access), or the physical location data of the phone tower or switch over which communication was established. In other words, the providers had to build in wiretapping capacities in the Internet backbone itself, for example by implementing a back door for electronic surveillance at key Internet Exchange Points and large packet-switching facilities (see chap. 4.1.3.3 The Internet Backbone). Private companies also had to bear the costs for this (Landau, 2010, p. chap 4.4).

This was an extension of traditional telephony wiretapping because it included not just telecommunications carriers (as in the past), but also Internet services and the Internet infrastructure itself. More so, Internet data is richer in information as traditional audio intercepts because it can include images, videos, voice or information on surfing behavior and interests, which allows to create very detailed profiles of users. Whereas the Clipper proposal aimed at the Internet's application layer (see chap. 4.3.5.1 Policy: The Clipper Chip (1993)), this attempt targeted the underlying physical infrastructure (see chap. 4.1 Engineering the Internet). More so, it would have given the government the authority to influence the development of new technology and if a company did not meet FBI's wiretapping needs, it could demand changes for example in software code. Thus, early versions of the bill gave the government the right to interfere actively in how private companies write their code (see chap. 2.3.7 Digital Technology: Software and Code). It aimed to ban sales of nonconforming equipment and required providers of "electronic communications services to modify their existing equipment within 180 days or face fines of $10,000 per day" (BeVier, 1999, p. 1073). All of this should be done with a subpoena, instead a court order (Drake, 1995a, pp. 330-331). Court orders have higher legal barriers

which must be fulfilled in order to initiate surveillance of personal spaces, thus they protect legal subjects. In this form, the Digital Telephony Bill would have been a far-reaching attempt of interfering and regulating the nascent market for digital technology. As Lessig argues, it was an attempt to control the code, influencing the technical design of the emerging networking architecture to "adequately serve the interests of the government" (Lessig, 2000, p. 63). It was a policy initiative clearly driven by a cyber-realist mindset.

As such, the proposed bill faced major resistance by industry and privacy advocates but also from Congress itself. Several authors called the initiative a "paradigm shift" (BeVier, 1999, p. 1053) or a "radical transformation of U.S. Wiretap law" (Landau, 2010, p. chap 4.5) because in the past, telecommunications providers could individually decide themselves how to technically implement intercept warrants. Now the FBI itself was put in charge of developing switching-standards, while placing the financial burden onto private companies, thereby potentially harming their competitiveness (Landau, 2010, p. chap 4.5). More so, by defining carriers quite broadly to include Internet and telecommunications carriers, the old wiretapping law was significantly expanded.

Critics questioned whether the FBI was really going dark in an era of almost limitless electronic data and new sources for criminal investigations. Some thought that the evidence the FBI published to support the seriousness of the threat was not really convincing. The head of the Telephone Association argued against the bill by arguing that that government should concerning itself with "maintaining the more appropriate arms-length relationship between common carriers and law enforcement", thereby pledging for the "hands-off" norm (Cohen, 1994). Opposition not only came from cyber-utopians such as John Perry Barlow and civil liberty groups, but also from Democrats *and* Republicans.

Because of the substantial criticism from both outside Congress and within, a lengthy congressional process with several alterations followed until the bill was signed into law in October 1994 under the name of *Communications Assistance for Law Enforcement Act* (CALEA). The final outcome was way more restrictive and included several privacy protections. It limited access to telephony providers only, which had to be reimbursed. The providers had to assist law-enforcement, but the FBI was not allowed "to require or prohibit any specific design of equipment, facilities, or system configurations to be employed by telecommunications carriers in compliance with the statute" (Cohen, 1994). Additionally, the carrier was not responsible for decrypting encrypted communications or altering code in their systems, as the FBI initially demanded. Most importantly, Internet and Voice-over-IP communications were excluded from the scope of the bill. There was more time for implementation and reduced fines. Meta-data about the physical location of

a subscriber was removed from data gathering and the bill prohibited automated remote surveillance. Instead of a subpoena, the FBI required a court order with higher standards for an intercept attempt.

Although the bill passed in the end, it was rather limited in scope and did not, as originally intended, affect the Internet. The EFF argued in a statement: "the bill draws a hard line around the Internet and other online networks. We have carved cyberspace out of this legislation" (Cohen, 1994). Like with the Clipper proposal, one explanation for the relative victory of cyber-liberalism and the "hands-off" norm was the hegemony of cyber-utopian ideas of the time. For example, Time Magazine reported in March that "two-thirds of Americans said that it was more important to protect privacy of phone calls than to preserve the ability of the police to conduct wiretaps", reflecting a clear primacy of cyber-utopian norms (Cohen, 1994). However, this was only a short-term victory, since CALEA got significantly expanded after 9/11 to include the Internet as well (Bloss, 2007, p. 219).

4.3.5.3 Policy: Internet Censorship with the Communications Decency Act (1996)

A final event in the history of the Internet of the 1990s and one final juncture, where the appropriate role of the state vis-à-vis the Internet was debated, happened in 1996. The question here was: should the state be able to control or even censor information on the Internet?

If one mentions the term Internet-censorship, most people think of the People's Republic of China, which began the construction of its Great Firewall of China or "Project Golden Shield" in 1996. This censorship and surveillance infrastructure became functional in 2003 and filters global Internet data traffic at the large IXP points connecting the Chinese Intranet with the rest of the world.[100] A similar initiative surfaced in the US during the "Internet Sex Panic" in 1996 when several newspapers and magazines launched front-page stories about pornography on the Internet (Daniel, 1996).[101] Following the outcry of concerned parents, a bipartisan initiative piggy-backed the *Communications Decency Act (CDA)* onto the *Telecommunications Act of 1996*, a major telecommunications reform bill

[100] Early Internet censorship used the simple technique of address-blocking or and DNS or URL filtering that has been pioneered in Western software called Firewalls (Anderson & Murdoch, 2008). What this censorship infrastructure does is looking for keywords within Internet data packets or preventing access to URL's and Websites that are blacklisted by political authorities. These include pornography but often also regime critical websites (Deibert et al., 2012).

[101] Because the Internet was designed to be open for all kinds of services, it should not come as a surprise that the Porn-Industry discovered the Internet quite early. Even during the 1980s, pornography was distributed through the Internet's private predecessors such as FIDONET and USENET and the help of Bulletin Boards (McCullough, 2015). For example, the Website of Playboy Magazine went online in 1994.

inspired by cyber-liberalism. While the Telecommunications Act aimed at privatizing Internet functions, market competition and liberalization of rules, the CDA would:

> "Make it a crime, in interstate or foreign communications, by means of a telecommunications device, knowingly to transmit a communication that is "obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person." Section 502 of the CDA also amended 47 U.S.C. § 223(a)(l)(B) to make it a crime, in interstate or foreign communications, by means of a telecommunications device, knowingly to transmit a communication that is "obscene or indecent, knowing that the recipient of the communication is under 18 years of age [...]"" (Cohen, 1997).

This bill was signed into law by the President in 1996. However, civil liberty, free speech and cyber-utopian advocacy groups such as the American Civil Liberties Union (ACLU) and the EFF filed a lawsuit (EPIC, 2002). John Perry Barlow's declaration of independence of cyberspace was written as a reaction to this law (see chap. 4.2.5 Framing Cyberspace as the Electronic Frontier (1990s)) and several internet advocacy groups began the "Black World Wide Web protest" on February 8-9, 1996. Timed with the presidential signing of the bill, several major web sites changed their background to black for 48 hours to protest against the violation of freedom of expression.

The bill was struck down as unconstitutional by the Supreme Court in 1997 (ACLU vs. Reno). The judges ruled that portions of this act violated the First Amendment which says that "congress shall make no law [...] abridging the freedom of speech, or of the press (Cohen, 1997). Pornography is protected as free speech by the First Amendment.[102] Such material is not to be banned/censored but to be made inaccessible to children (via age or pin-code verification for example). But the judges made a larger point, way beyond pornography. They made a statement about the Internet in a democracy. The three judges (Dolores Sloviter, Ronald Buckwalter and Stewart Dalzell) – following the ideas of cyber-utopianism and the belief in the democratizing effects of the Internet – argued:

> "[…] the Internet has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country – and indeed the world – has yet seen. The plaintiffs [ACLU] in these actions correctly describe the 'democratizing' effects of Internet communication: individual citizens of limited means can speak to a worldwide audience on issues of concern to them. Federalists and Anti-Federalists may debate the structure of their government nightly, but these debates occur in newsgroups or chat rooms rather than in pamphlets. […] In these forms of communication, regulations on the basis of decency simply would not survive First Amendment scrutiny. The Internet is a far more speech-enhancing medium than print, the village green, or the mails. Because it would necessarily affect the

[102] With the exception of violent material (rape videos) and child pornography.

> Internet itself, the CDA would necessarily reduce the speech available for adults on the medium. This is a constitutionally intolerable result" (Naughton, 1999, p. 191).

This ruling is pretty much in line with Gore's utopian frame about the democratic nature of the Internet. Also, the empowering component, the "speech-enhancing" nature of the medium is highlighted, which is presented as far more significant as the invention of print-media. In cyber-utopian circles, the significance of the Internet is often highlighted by referring to the invention of the printing-press which is seen as a key-enabler in the period of enlightenment. The Internet is presented as some kind of meta-infrastructure that is an enabler for public discourse in a democracy. Finally, Judge Dalzell affirmed the "hands-off" norm that was guiding government behavior towards the Internet in the early 1990s:

> "We should also protect the autonomy that such a medium confers to ordinary people as well as media magnates. Cutting through the acronyms and argot that littered the hearing testimony, the Internet may fairly be regarded as a never-ending worldwide conversation. The Government may not, through the CDA, interrupt that conversation. As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from governmental intrusion" (Naughton, 1999, p. 193).

That the Internet "deserves highest protection from governmental intrusion" (Naughton, 1999, pp. 190-193) affirmed the cyber-utopian norm that the state shall not encroach onto cyberspace and thus stopped further attempts by the state to assert control over cyberspace. This first attempt to control content within the Internet failed with this landmark ruling. This ruling codified the "hands-off" norm into law and further constituted the idea of the democratizing effects of the Internet. It basically argued that freedom of speech is a greater good than government interests and demanded some form of democratic constraint. Democratic governments in particular should not intrude into the worldwide conversation, which can be seen as a wink to the appearing Internet censorship attempts occurring in other non-democratic countries but could also be seen in the context of the US information warfare doctrine developing around the same time (see chap. 4.4.2.3 Core Ideas: Information Weapons & Digital Battlespace).

This ruling also had an influence on the technical and economic structure of the Internet. Economically, the Telecommunications Act itself deregulated the market and allowed the creation of smaller Internet exchange carriers in competition with large carriers. It lowered prices and increased competition (Friedman, 2005, p. 74). Technically, age-verification sites became a common practice on websites, shielding minors from adult content (at least theoretically). It can be argued that this ruling set the general tone.

Proponents of state control of the Internet suffered a strong defeat. Cyber-realists, advocating for greater state control over cyberspace metaphorically "got their fingers burned" and did not attempt similar initiatives during the Clinton administration. This indicates a socialization or learning-effect that also set up a temporary closure or lock-in, which slowed or even stopped the path-trajectory of Internet control. In methodological terms, this episode is key evidence in showing that the "hands-off"-norm exhibited a normative constraint on actions, meaning that it prevented actors from doing something (censoring the Internet) that is not in line with the norm's logic of oughtness (Bennett & Checkel, 2014, p. 34). The ruling gave the "hands-off" norm legal credibility, reified it and thus influenced the temporary dominance of the hands-off norm and cyber-utopianism in cyberspace, at least until the crash of the dot-com bubble and 9/11.

4.3.6 Critical Analysis and Paradigm Blind Spots

It should have become clear by now that "the discourse about the Information Superhighway" is dominated by "rosy utopian predictions of increased democratization and access to information and culture" (Besser, 1995). However, like every paradigm, early cyber-utopianism has some blind spots and issues that are not addressed. The following presents a series of critical arguments directed against the liberal-utopian vision of the Internet within the policy sphere. Since the general critique of utopian thought has been provided in a previous chapter (see chap. 4.2.9 Critical Analysis & Blind Spots of Cyber-Utopianism), I will only make a few arguments that did not appear before.

Besser reminds us that "the prediction made for cable television more than two decades ago sounds remarkably like the predictions being made for the Information Superhighway today" (Besser, 1995). Although cable-TV started with similar social norms, predominantly a call for openness and universal access, the media landscape looks quite different now, with several media conglomerates. The same can be said with the introduction of public telephony. In both cases, cable TV and telephony, the goal of universal services was not reached, for example with a telephony penetration rate of 94% in 1994, leaving 5.7 million homes without a phone (Cate, 1994, p. 52). If people, with lower incomes are excluded, it has implications for the democratic potentials of the technology. Democracy requires that every vote counts and that every voice is heard.

More so, the framing of a global town square and the argument that the Internet is equivalent with democracy and as such a public good blurs the fact that it is not. The Internet is less a public sphere and more a privately-owned environment run by corporations who operate the physical (switches, IXP, cables) and digital-infrastructure

(web services, access). McChesney argued in 1996 that with the privatization of the Internet, "the market, and not public policy, will direct the course of both the Internet and the information highway." The rush to commercialize the Internet was in full swing in the mid 1990s and corporate media giants "are aggressively working to dominate the Internet" (McChesney, 1996, pp. 104-105).

Besser warned in 1995 that *digital information can be altered* and manipulated quite easily. This invites propaganda, censorship and information warfare: "Because digital images can be seamlessly altered, how can the viewer be sure that the image on view has not been manipulated?" (Besser, 1995). In 1993, futurologist and Sci-Fi writer Howard Rheingold warned of a so-called *Disinformocracy*, a democracy where the public perception is shaped by a constant information war. He argued that the service and information providers of the Internet could use their information-dominance to manipulate users. "The prospect of the technical capabilities of a near-ubiquitous high-bandwidth Net in the hands of a small number of commercial interests has dire political implications. Whoever gains the political edge on this technology will be able to use the technology to consolidate power" (Rheingold, 1993, p. chap. 10). He also envisioned the chilling-effects on privacy by big corporations and Big-Data: "The most insidious attack on our rights to a reasonable degree of privacy might come not from a political dictatorship but from the marketplace" (Rheingold, 1993, p. chap. 10). Nowadays, we see this impact of corporate control over cyberspace with Internet giants such as Google and Facebook and their algorithms having a major influence on how we compute information and thus how deliberations over the Internet look like. Concepts like echo-chambers and filter-bubbles remind us of the overheard warnings of the 1990s.

Other issues that are systematically overlooked are matters of *privacy, freedom of speech and the potential for surveillance*. Cate argues that:

> "None of the Administration's NII pronouncements mention the First Amendment. It does not appear in the Agenda for Action or in a single speech by Vice President Gore, Secretary Brown, Assistant Secretary Irving, or any other senior Administration official. Free expression is not the subject of any NII committee or working group" (Cate, 1994, p. 54).

Cate argues that the principle that "Congress shall make no law abridging freedom of speech or of the press – erects a very high barrier to government intrusion" (Cate, 1994, p. 54). This very principal is crucial for the function of the NII and for the public interest in general. Closely connected to freedom of speech is the issue of *privacy*, which is largely ignored in the Information Superhighway discourse, although it is quite relevant. Besser

argued that the privatization and commercialization of the Internet will bring with it threats to privacy (Besser, 1995). In 1996, Wellbery wrote that the Internet creates new possibilities to compile, transmit and distribute personal information relatively easily, which allows the allocation of user data and the creation of user profiles, for example for advertisement. Because of relatively weak privacy laws, US customers would not be adequately protected from misuse (Wellbery, 1996). This would create a structural incentive for corporate surveillance and foreshadowed the business models of Google (1998) and Facebook (2004). However, the NII initiative did not even address this issue. This trend was only increased and accelerated with the realization in the late 1990s that data can serve as a commodity that can be sold, which ultimately led to the current Big Data frenzy in the Web 2.0 period.

In sum, it can be argued that cyber-utopianism dominated the early discourse on the Internet between 1993 and 1996, at least on the surface. This can be shown by referring to polls. Drake argues: "Several opinion polls conducted over the past two years indicate that a majority of the people who have heard of it think the new information infrastructure will be a "good thing" but also they do not really know what it is" (Drake, 1995c, p. 3). Below the surface, hidden in the shadows of the intelligence community, cyber-realist ideas and initiatives began to grow, as the CALEA and Clipper episodes have shown. Because of the dominance of cyber-utopianism these attempts to enable state control over the Internet failed because the advocates were not able to rally major support for their norm of Internet control. Instead, the "hands-off" norm, the idea that the Internet should not be controlled by the US Government, prevailed.

4.3.7 Summary

The causal mechanism developed in this chapter works as follows. That the Clinton-Gore administration won the presidency in 1992 was a key necessary condition for the dominance of liberal cyber-utopianism (part 1). It was also an instance of *paradigm-change via regime change,* i.e. The change of dominant ideas when a new government from another party entered office (see chap. 2.2.1 Policy Paradigms). Former President H.W. Bush showed no particular interest in technology and did not engage in any political leadership trying to steer the telecommunications sector.

The *structure of this policy subsystem* is an important conditional factor for the dominance of cyber-utopianism in the early 1990s. When Clinton/Gore entered office, Internet policy was a nascent policy subsystem without much political leadership, existing laws and regulations and thus little pre-structuration in terms of policy or dominant ideas

or paradigms. Most guiding decisions came from the FCC or the large players like AT&T (Mueller, 2010, p. 56). At the same time, the policy subsystem was already big enough (because of the digital revolution) to be relevant and in need of political leadership. Being a nascent subsystem means that rules of the game were not established, compared for example to the national security subsystem, where power positions and the appropriate roles of different actors are historically pre-structured. Theory assumes that it is *easier in nascent subsystems for new actors and ideas to get their voice heard,* which is a key explanation why cyber-utopianism, a paradigm born outside the realm of politics, could become influential. In this nascent Internet subsystem, there was no prior hegemonic paradigm and thus no staying power of the status quo. This enabled the Clinton/Gore administration to define the appropriate role of different actors like the private sector, the users or the military and intelligence community as well as the regulative goals and instruments with its Information Superhighway agenda, representing a third or second order policy change.

Besides the structure of the policy subsystem, the other important factor is that the central actors were *receptive to cyber-utopian ideas*. *Technology literacy and personal advocacy of actors in a powerful position* are key explanations for the dominance of utopianism within the early politics of the 1990s. Al Gore was the central figure here. Gore's personal interest in the Internet and technology resonated with the ideas of cyber-utopianism developed by the digital natives like the *principled belief in the positive impact information technology on education, economic growth, democracy and personal empowerment.* Closely interrelated is Gore's personal history or background (socialization). In the past, he sponsored several Internet related policies such as the High Performance Computing initiative, which exposed him to the ideas of the ARPANET engineering community and gave him (enough) technological literacy about computer networks. He continued this path once being in high office. But there is also another path-dependency argument: had it not been for his father, Gore probably would not have adopted the term Information Superhighway as a reminiscence to the interstate highway system (and to draw external credibility from this fact). With these factors, it is hard to determine which one came first, so that combined working of these factors (equifinality) is probably the best explanation.

The *Information Superhighway initiative is a direct causal outcome of this personal advocac*y and probably would not have been adopted (part 2) had there been another Vice President (necessary condition). The argument goes that cyber-utopian ideas got embedded into this policy. Technology was mostly understood in terms of its positive economic

impact. This economic frame also influenced the appropriate actor positions with regard to the Internet: it gave primacy to the private sector building and running information infrastructures. It positioned the US government at arms length. Gore personally argued that the state should neither own, run nor control cyberspace, *thus adopting the cyber-utopian norm that the state has no (or little) role to play in cyberspace.* However, since he was no die-hard libertarian and a political professional, he devised the appropriate role of government as some kind of neutral referee, preventing the creation of monopolies and providing only flexible regulation and hands-off leadership. A factor that should also be mentioned is that the telecommunications industry was afraid of too much government regulation and thus argued, and probably lobbied, for the hands-off norm as well. This coincides with the general neo-liberal zeitgeist of the 1990s.

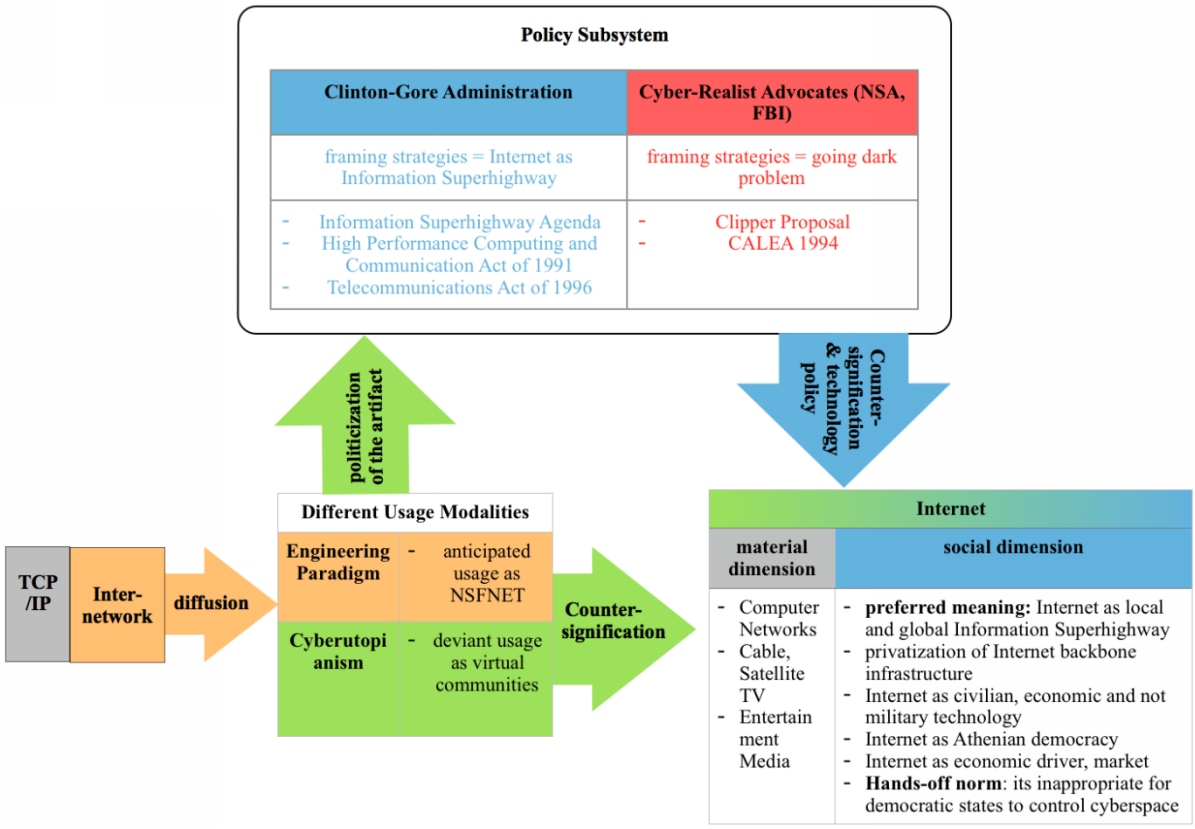
The technological frame of the *Information Superhighway had a widespread societal and political appeal* (part 3). It was not only highly congruent with utopianism put forward by the digital natives, but it also provided a positive political vision or prognostic frame for the future. The metaphor of the highway was highly commensurable and helped citizens to understand the abstract concept of the Internet. It had a high narrative fidelity, addressing a wide array of different issues from education to entertainment. More so, it was compatible with economic thought, giving it a greater credibility. The belief in the positive effects of the Internet became wide-spread in the early 1990s, as the dot-com frenzy showed. It was also a powerful frame for global norm diffusion. The Information Highway Agenda became a prototype of how states could govern this new medium. The privatization of the Internet backbone infrastructure in 1996 manifested and materialized this norm and established a new type of Internet governance model that many other Western countries adopted or emulated to some degree (part 4).

Gore also acted as a global norm-entrepreneur, *diffusing the norm that the Internet should be democratic* on a global scale (part 5). Here, Gore picked up a common frame of the time that argued that states either could control information technologies and information, or fall behind economically (the dictator's dilemma) and the idea of decentralization of authority, which was a common neo-liberal and cyber-utopian narrative of the time. In sum, Gore acted as a top-down norm-entrepreneur inside the US and as a bottom-up entrepreneur globally, trying to establish the hands-off norm.

The graphic shows the mainstream diffusion of the technical artifact on the left (with its material components, i.e. TCP/IP and its engineering meaning of an "internetwork"). The next step shows the impact constituencies and how the deviant usage of cyber-

utopians (green paradigm) led to a counter-signification (see chap. 4.2 The Evolution of Cyber-Utopianism).

Figure 23. Cyber-liberal Utopianism framing the Internet during the early 1990s (own diagram)



The previous chapter showed how the utopian interpretation and framing (green) of the Internet became dominant in the early 1990s, replacing the signifiers and concept of the engineering paradigm (orange). This counter-signified the Internet as cyberspace. At the same time, utopianism got politicized by the Gore administration creating a liberal spin-off (blue). These new ideas got fused into new policies such as the Information Superhighway agenda, which framed the Internet in economic terms, established new actor positions and the "hands-off" norm. But during the mid 1990s, this "hands-off" norm and cyber-liberal utopianism was still fragile. We saw attempts of cyber-realist policy-making (red) within the political spheres, trying to establish control over the Internet and contesting the "hands-off" notion. Several government and congressional initiatives aimed at introducing some control, either in terms of wiretapping of digital communication (CALEA 1994) or in terms of setting encryption standards (Clipper 1993), or by imposing content censorship of indecent material (CDA 1996). These instances were paradigmatic clashes of advocates of cyber-realism trying to exert political influence over the Internet. I would argue that these

initiatives failed because of various, case specific reasons. Clipper was immature, CALEA too broadly conceived and the CDA unconstitutional.

The following table summarizes the causal mechanism for this chapter.

Table 4. Causal Mechanism of Cyber-Utopianism & the Clinton/Gore Administration

Context	Relatively unregulated policy subsystem of telecommunications with little pre-structuration but large enough to be relevant.
Part 1	Clinton election as a necessary condition for paradigm-change via regime change. Clinton-Gore administration was *receptive* to original cyber-utopian ideas (resonance) and launched a political process of interest aggregation, creating a more neo-liberal version of the paradigm.
Part 2	Gore's Information Superhighway agenda *prioritizes* the private sector in cyberspace. The policy assigned actors positions in the new policy field and *defines* appropriate role for the state at arms-length. Policy process establishes/creates "hands-off" norm (norm emergence).
Part 3	Hands-off norm *resonates* well with private sector and fits into the neo-liberal Zeitgeist in the economic sector but also fits into general cyber-utopian ideas of digital natives in the early 1990s.
Part 4	Information Superhighway agenda *initiates* the privatization of cyber-space, *enabling* a path-trajectory of decentralizing control over cyberspace into the hands of private corporations.
Part 5	Personal Gore advocacy *frames* the Internet in terms of democracy and defines government control over cyberspace as inappropriate. This norm & US Internet governance model begins to diffuse domestically and globally together with the Internet.
Part 6	Cyber-realist policy initiatives (Clipper, CALEA) and the Communications Decency Act *contest* the hands-off norm and *attempt* to establish partial state control over aspects of cyberspace but face public resistance.
Outcome	Supreme Court creates a legal precedent by ruling that the state should not control cyberspace by censoring content. Legal precedent codifies the "hands-off" norm into law and makes it temporally hegemonic (closure).

The ruling of the Supreme Court, arguing that the government should not control content in cyberspace, is theoretically important because it represents an instance of temporal closure. The legal ruling of this magnitude had set a legal precedent that placed freedom of speech and information as a high priority and cemented the idea that the state

has no business regulating it. The utopian-liberal meaning became dominant. It was dominant but not necessarily hegemonic (in the sense of an unquestioned truth). This established a path or a future trajectory that is still valid to some degree since there was no other attempt of this kind. However, during the second half of the 1990s, cyber-realism evolved out of the military information warfare doctrine. This doctrine began to form an alternative paradigm, contesting the dominance of cyber-liberal utopianism. Cyber-realism particularly filled in the blind spots that utopianism ignored, i.e. the question of security, as the next chapter will show.

4.4 Information Warfare and the Origin of Cyber-Realism

"A strange game. The only winning move is not to play."
Joshua, AI in the movie War Games (1983)

Organizations concerned with national security, such as the military, intelligence and law-enforcement agencies used to be the first adopters of expensive, new technologies. Especially the US military has a long tradition of using computers. One of the first large-scale cybernetic technical artifacts was the Semi Automatic Ground Environment (SAGE) Radar system which incorporated the first mainframe computers (1945-1952) for automated radar detection and warning. Before the Internet, SAGE was the biggest data-network (Rid, 2016, p. 109). Since then, computers have taken over many military command functions (called C3I, command, control, communications and intelligence) and have replaced human operators (Edwards, 1997). With this ever increasing automation of war, it does not come as a surprise that the national security community was the first to be concerned about security issues of inter-networked computers.

This chapter focuses on military (Air Force), intelligence (NSA, CIA) and law-enforcement (FBI) actors and their interplay with policy-makers. These are key advocates of a national security or military perspective on cyberspace, which is called cyber-realism. I argue that the roots of the paradigm lie within the concept of information war (IW), first conceived in the 1970s and reformulated as a military doctrine in the mid-1990s, until it became an actual national security policy and coherent paradigm under the Bush presidency. Ultimately, information war was reframed as cyber-war, the term that we nowadays use. Cyber-realism assumes a national security and state-centric perspective on ICT and predominantly perceives the technology as having a negative impact on national security. Realism is carried by a coherent set of actors which produced a large corpus of policy documents that act as the carrier medium for analysis (see appendix Cyber-Realism Corpus). I will focus on military doctrines, national security directives[103] and strategies to extract the core ideas and norms out of these documents. The central norm of cyber-realism is that the state, through its military and intelligence apparatus, should be able to monitor, control and monitor global cyberspace, even beyond its national jurisdiction, in war and times of peace alike. The function of this chapter is to trace the origin of this norm and answer the question of how it could replace utopian norms. Thus, this chapter is about the second part of the norm-change process and the second part of the title of this

[103] In terms of academic analysis, military sources are a dual-edged sword because they only reflected the published military thinking. In terms of surveillance and intelligence research, much of the thinking and material is classified. This thesis only has the possibility to look at unclassified or leaked material that exists in the public domain.

dissertation: *cyber-war*. It is a central chapter in this thesis, which is why it is the longest in the empirical part.

First, I will provide a bit of historical background regarding the question of computer-insecurity, a blind spot mostly ignored by the engineering paradigm (see chap. 4.1.5 Development Blind Spots). The purpose of this chapter is to understand the actual problem that forms the basis of cyber-realism. After that, I turn to the central ideas of realism by introducing core concepts such as "information war" and its little brother, "cyber-war" (see chap. 4.4.2 Ideas: Formation of the Information War Doctrine (1976-2000)). Since these ideas are the basis for the norm of control, I will dissect the central ideas in high detail according to the logic outlined in the theory chapter. This includes an initial euphoria about the perceived changing nature of warfare (see chap. 4.4.2.1 Optimistic Cyber-Realism: Revolution in Military Affairs (1992-2000)), but also problems that derive particularly from the perceived shortcomings of the TCP/IP protocols, i.e. the degree of anonymity the Internet provides (see chap. 4.4.2.2 Problem Definitions of Cyber-Realism). I argue that this central problem perception and definition of cyber-realism guides much of the political, technological and normative response of realists to the Internet. If the Internet is perceived as a battle-space and information regarded as a weapon and a source of power (see chap. 4.4.2.3 Core Ideas: Information Weapons & Digital Battlespace), it logically follows that the state should control these resources. In other words, out of these ideas evolves the norm that states should control cyberspace (see chap. 4.4.2.4 Analyzing Emerging Norms of Cyber-Realism). After having analyzed these ideational and normative elements of cyber-realism, the following chapter addresses the question of how these ideas became institutionalized within bureaucratic structures, a key theoretical element for the stabilization of norms (see chap. 4.4.3 Setting the Path: The Institutionalization of Cyber-Realism). This and the following chapter explain the story line how realist ideas began to influence policy-making of the later Clinton administration, particularly after the terror attacks of the mid 1990s and the debate about critical infrastructures (see chap. 4.4.4 Politics: Turn to Realism - Critical Infrastructure Initiative (1996-1999)). This process culminates in a critical juncture, the Y2K panic at the end of the millennium, when it was feared that a computer-bug could shut down the entire world, which represents a key-narrative of cyber-realism that suddenly spilled over into public discourses (see chap. 4.4.5 Discourse: Y2K and Critical Infrastructure Failure). Afterwards, I will summarize the causal mechanism in the 1990s (see chap.4.4.6 Preliminary Summary), before I turn to the politicization of cyber-realism in the war on terror, which represents another juncture (see chap. 4.4.7 The Politicization of Cyber-

Realism with the War on Terror (2000 - 2008)). These chapters are absolutely crucial for this thesis because the ideas that formed and the political/technological decisions that were made in this period still have implications in terms of surveillance and cyber-war today.

The description of the war on terror-period is structurally similar to the that of IW in the 1990s: I start by describing the structural composition of the Bush administration during the juncture that was 9/11 (see chap. 4.4.7 The Politicization of Cyber-Realism with the War on Terror (2000 - 2008)). I argue that cyber-realist hawks had a tremendous influence shaping the political response to 9/11. I show this by analyzing counter-terrorism strategies (see chap. 4.4.7.1 Ideas: Cyber-realism and Counter-Terrorism (2001 - 2007)) in order to assess correspondence with cyber-realist ideas developed in the 1990s. I argue that that the 9/11 policy response has two concrete outcomes: First, realist inspired policies such as the Patriot Act (see chap. 4.4.7.2 Policy: The Patriot Act and Intelligence Reform (2001 - 2004)) and second, technical artifacts developed by the NSA (see chap. 4.4.7.3 Artifacts: NSA and the Full-take Norm of Internet Control (2001 -)). Both are political instruments (Hall, 1993, p. 279) that are designed to control the Internet. The chapter about NSA Internet surveillance is absolutely crucial and a key smoking-gun for state control of the Internet. It enables the offensive turn to cyber-war, as the following chapter describes (see chap. 4.4.7.4 The Fusion of IW, Surveillance and Cyber-war (2003-2008)). The core argument is that we should not see IW, cyber-war and surveillance as separate functions but as an interconnected nexus of practices, and that we should maintain a critical stand to the arguments put forward by supporters of mass surveillance (see chap. 4.4.8 The Norm of Internet Control) The summary shows how the Bush administration militarized cyberspace and how it normalized Internet surveillance as a norm that began to diffuse globally since the mid-2000s (see chap. 4.4.10 Summary).

4.4.1 Background: Growing Awareness of Computer Insecurity (1967 - 2011)

The theory assumes that the spread or mainstream diffusion of a new technology creates more points of contact, resulting in more people engaging with the technology over time. This enables deviant usage scenarios. The causal mechanism depicted in this chapter works like this: the mass diffusion of the *Internet interconnected more civil and military computer systems* and attracted more users. Because the Internet is open for all kinds of uses, more *unintended activities such as malicious hacking or data extraction emerged*. The more malicious activity on the network, the more users were potentially affected, which in turn led to an *increase of their awareness of IT security issues such as data*

protection. This mechanism repeated itself between the 1970s and the mid-2000s and thus worked in a spiral, or escalating fashion, leading to increased awareness with every turn.

As was shown before (see chap. 4.1.5 Development Blind Spots), Paul Baran wrestled with the question of secure networks since 1964, and ARPA engineer Willis Ware pointed to intrusion-problems in computer networks in 1967 (Ware, 1967). In 1979, Jürgen Kraus argued that software could self-replicate and thus mimic a simple life-form: a Virus, which was the birth of the term (Rid, 2016, p. 189). The problem was that nobody saw this issue as a *general* problem because no-one anticipated that the experimental ARPANET would be used outside of academia or even on a global scale. In other words, the engineering-paradigm did not perceive computer security as a problem until it received wake-up calls during the 1980s.

During that time, pop-cultural references such as movies like Tron (1982), War Games (1983), or William Gibson's novel Neuromancer (1984) picked up the motive of rogue computer systems that gained an independent artificial intelligence and that threatened human life (see chap. 4.2.4 Artifact: The WELL and the Social Construction of Cyberspace (1980-1990)). War Games made the risks of computer hacking visual to the general public. The movie describes the digitalization and automation of the US nuclear arsenal, which is becoming controlled by an artificial intelligence called Joshua. A teenage computer hacker breaks into the command system of the US forces and tinkers around with simulations about nuclear first-strike scenarios. Believing it is a game, he almost accidentally initiates a thermonuclear war. The film ends with the conclusion that the only way to win would be not to play this war game. Although War Games was a science fiction movie, it was inspired by real hacking incidents prompted by young computer hackers. According to Kaplan, President Ronald Reagan was deeply impressed by the movie and asked his advisors "Could something like this really happen?" (Kaplan, 2016, p. chap. 1). A task-force concluded that there actually was a problem because nuclear command and control functions largely depended on computer networks that were potentially vulnerable. Thus, the movie was a trigger event and the first recognition of a security problem. Consequently for the first time it set the diagnostic and prognostic frame within the administration.

On September 17th 1984, President Reagan ordered the *National Security Decision Directive Number 145: National Policy on Telecommunications and Automated Information Systems Security*. The government realized that the "recent advances in microelectronics technology have stimulated an unprecedented growth in the supply of telecommunications and information processing services" (The White House, 1984). While

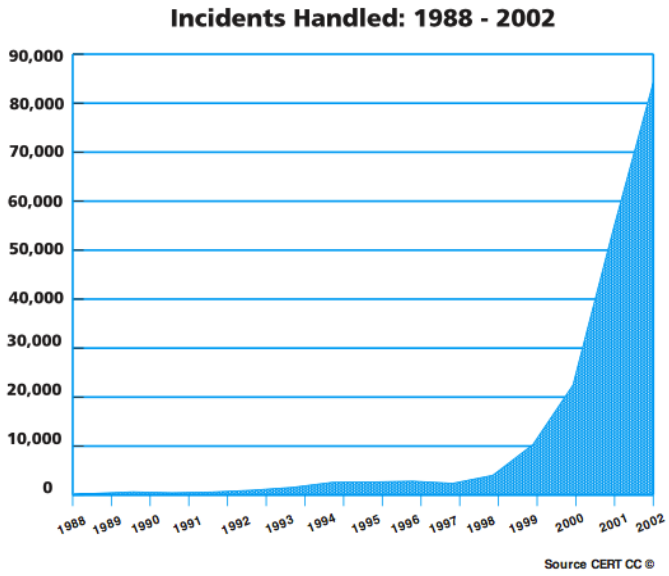
this trend seemed to be beneficial for the economy, it also created security challenges: "automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat" (The White House, 1984). Electronic systems of the government and of businesses are targets that can be exploited by foreign nations, terrorists and criminal elements.

The directive formulated a new aim to assure the security of automated information systems as well as "classified national security information, and other sensitive government national security information" (ibid 2.) carried over networks such as ARPANET. Its general mission is to probe and vet the current communications infrastructure. For that purpose, the National Telecommunications and Information Systems Security Committee was founded, which included members of the intelligence community (FBI, NSA, CIA), the armed forces (Chiefs of army, Navy and Air Force) and the secretaries of commerce, transportation and energy. NSA was given the task of setting standards for computers because of its unique expertise, which was very controversial (Kaplan, 2016, p. chap. 1). The result of this third order policy-change was the so-called "Rainbow series", a series of computer security guidelines published by the US Government between the 1980s and 1990s. The NSDD-145 was the first time the issue of computer security was brought to the political agenda and was formulated as a policy problem. It also alerted the US intelligence community: if someone from the outside could hack into US networks, the other way around was also possible. For example, when NSA realized the growth of computer vulnerabilities, it set up a Computer Security Center to combine Signals Intelligence and Information Security (Kaplan, 2016, p. chap. 1). Around the same time, the US House of Representatives started hearings on computer security that led to a series of laws, like the "Comprehensive Crime Control Act" (1984), "The Computer Fraud and Abuse Act" (1986) and the "The Computer Security Act" (1987).

In 1988, another shock moment happened that is described by some as the "fall of man" that thrust the Internet out of Eden (Landau, 2010, p. chap. 3.4). Graduate student Robert Morris launched one of the first computer worms that automatically spread through the ARPANET and disrupted about 1/10 of all devices connected, including Air Force computers (Kaplan, 2016, p. chap. 4). The Morris-worm had a self-replicating mechanism that allowed it to infect other machines. The computer science community at DARPA and the military command witnessed, for the first time, something resembling a cyber-crime. As a reaction to this shock, DARPA formed a Computer Emergency Response Team

(CERT)[104] at Carnegie Mellon, thereby inventing the CERT-concept (Saalbach, 2015, p. 58). These CERT teams were an institutionalized response to computer security breaches and became a common practice in the DoD and large businesses. CERT teams also began to measure cyber-security incidents such as viruses and network intrusions, as the following graph, released in 2003, shows.

Figure 24. Measured Computer Security Incidents in US Systems, Source: (The White House, 2003, p. 8)



While there were roughly a few hundred incidents during the 1980s that number increased to around 5000 in the mid 1990s and then skyrocketed in 1999 to over 10000 incidents. In 2014, there were around 42,8 million incidents (117000 per day) globally, many of which represented automated network-probing and are not necessarily dangerous. Cyber-crime like data-theft or spam for economic gain is the motivation behind 62,3% most of the attacks, followed by espionage (24,9%) and hacktivism (10,2%). Only 2,5% are disruptive cyber-attacks, according to Data from Hackmageddon (Passeri, 2016). Just by the statistics, state-sponsored cyber-war is a less urgent issue compared with cyber-crime. The rise of network incidents correlates with the beginning mass diffusion of Internet connections worldwide: the more connections, the more potentially malign users and the more valuable targets. However, the peculiar thing is that the steadily growing number of incidents does not correlate with political awareness. Political awareness did not grow in a linear fashion, but happened in bursts that are hard to quantify. Healey argues that the history of cyber-security and cyber-war is a history of repeated slumber and wake-up calls,

[104] CERT Teams are a group of computer experts that handle computer security incidents, shutting down critical infrastructure, removing malware and enabling protection services. Nowadays, CERT team are a norm and regarded as essential for computer network security.

as for example the Wargames story and the Morris-Worm showed (Healey & Grindal, 2013). A dramatic incidence or a shock raises awareness, political action is taken and then the issue is forgotten again. Over time, every new headline reinforced the salience of the issue, representing an additive or cumulative effect.

Another burst of awareness came in 1991 with a report from the National Research Council called *Computers at Risk* (National Research Council, 1991). In it, many of the nation's top scientists (including some who worked on the ARPANET) highlighted the fundamental insecurity of current computer systems. The report started with a strong diagnostic framing: "The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb" (National Research Council, 1991, p. 7). The increasing proliferation of computer systems without security measures, the increasing number of software applications, the growing computer expertise within the general population and computer interconnection multiplied individual vulnerabilities (National Research Council, 1991, p. 1). The authors make it clear that computer security[105] is not just a technical issue, but rather a social problem (National Research Council, 1991, p. 3). The report diagnoses a market-failure because the demand for trustworthy systems is concentrated in the defense community while basically ignoring public and business demands for computer security, such as public encryption for example (National Research Council, 1991, p. 146).

The report had a substantial impact on the political establishment and also on the wider discourse. First, it influenced the development of the information warfare doctrine, which will be introduced in the next chapter. Second, it influenced the discussion about encryption, as the Clipper debate in the previous chapter showed (see chap. 4.3.5.1 Policy: The Clipper Chip (1993)). Third, it had an ideational and discursive effect, because this report set the tone for debate of the coming years. In a congressional hearing on that report, IT-security expert Winn Schwartau famously argued that government and commercial "computer systems are so poorly protected today that they can essentially be considered defenseless; essentially, an electronic Pearl Harbor waiting to occur" (U.S. Congress, 1991). This was the first use of the *electronic Pearl Harbor threat frame* that was used in many attempts of IT-securitization from the 1990s until the present day (Hansen & Nissenbaum, 2009; Dunn Cavelty, 2013a). This frame became generally prevalent in 2011, as a later chapter will show and thus it can be argued that it represents the master frame for

[105] "Security refers to protection against unwanted disclosure, modification, or destruction of data in a system and also to the safeguarding of systems themselves. Security, safety, and reliability together are elements of system trustworthiness—which inspires the confidence that a system will do what it is expected to do" (National Research Council, 1991, p. 2).

cyber-realism (see chap. 4.5.4 Discourse: Cyber-Doom and the Hegemony of Cyber-Realism).

Another burst of awareness happened between 1997 and 1999 with the Eligible Receiver Simulation that uncovered network vulnerabilities and the 1998 Moonlight Maze incident were, military maps and troop configurations were stolen from the Pentagon. These events had an impact on the discourse on critical infrastructure protection that tilted the Clintonian cyber-utopianism more towards realism, as a following chapter will show (see chap. 4.4.4 Politics: Turn to Realism - Critical Infrastructure Initiative (1996-1999)). This is the reason why this episode of the Clinton administration is described in this chapter and not the previous one.

Another major burst of awareness came between 2007 and 2008 with the first large-scale cyber-attack on the nation of Estonia and the first use of hacking in a military scenario in Syria (Israeli Operation Orchard). The Pentagon, too, received a wake-up call with the intrusion into their classified and highly secure internal network by a malware called "agent.btz" in 2008. In the same year, the "Conficker Virus" affected millions of users and caused huge financial damage. These events led to the creation of the US Cybercommand, as another chapter will show (see chap. 4.5.3 Practice: Professionalization of Offensive Cyber-War & Surveillance). With an Internet penetration reaching roughly 80% of the US, and 20% of the world population in 2007, it can be argued that the political elite and the general public realized the significance of cyberspace and cyber-security somewhere between those years (see appendix Quantifying the Internet and the Digital Revolution).

Finally, between 2010 and 2011, three hacking events made big news headlines: the so-called Sony hack, the actions of the hacktivists anonymous against Scientology, Defense Contractor Booz Allen Hamilton, VISA, Mastercard and Paypal after the Wikileaks affair. Finally, there was the revelation of the US-made Stuxnet virus that attacked Iranian nuclear enrichment facilities. These events lifted the former military discourse on cyber-security into the public domain. A more comprehensible table of events is listed in the appendix (see Table 9. List of Internet Milestones and Security Incidents).

Analytically, it can be argued that rather than one single shock moment, the continuity of cyber-security incidents had an additive, cumulative effect on the political awareness or problem recognition of these issues. This and the next chapters introduce some key events that led to the formation of the paradigm called cyber-realism, including the first political and technological responses to tackle the issue of computer insecurity. The ideational origins of this paradigm lie in the thinking about information warfare.

4.4.2 Ideas: Formation of the Information War Doctrine (1976-2000)

The origins of what we now call cyber-war lies within the broader military concept of information war, which was developed shortly after the Vietnam War. The fact that the world's most advanced military was not able to defeat its adversary in a jungle led to a general war-depression, the Vietnam syndrome. The US military began a soul-search, developing new strategies and ways of fighting war. Technology, automatization and modernization promised to reduce the duration and the human costs of war (Rid, 2016, p. 362). Electronics already played a huge role in Vietnam. General Westmoreland coined the concept of *electronic-warfare*, a war of sensors and disruption of communications (Westmoreland, 1969). In 1976, shortly before DARPA tested the first TCP/IP-based inter-network, DoD advisor Thomas P. Rona, developed the concept information war. He theorized a new strategy for defense based on the ongoing computerization of the military, driven by the Personal Computer revolution of the 1970s.

The strategy "aims at depriving the attacker of the essential information required to structure an effective offense" (Rona, 1976, p. 1). Key processes in this new information warfare are: to *disrupt* (prevent the enemy from transmitting or receiving signals), to *deceive* (send erroneous signals without the enemy realizing their true nature and to provoke false decision-making) and to *exploit* ("to secure and use information extracted from enemy information links in order to improve our own decision process" (Rona, 1976, p. 32)). The idea was to target the enemy's command and control chain of command, for example by disrupting the communication link of intercontinental missiles, resulting in faulty targeting. Systems like the SAGE radar could be "hacked" by inserting false signals, simulating an army where there was none, which would result in false decision-making. Rona highlighted that there is no real conceptual difference between *offensive exploitation* of enemy information links and the *defense* of one's own, because the technology used is essentially the same (Rona, 1976, p. 1). He also argued that *cumulative mass collection of enemy data*, driven by the aim to know as much about him as possible, while at the same time preventing the enemy's data collection, is central to IW (Rona, 1976, p. 43). A similar idea was developed by Pentagon scientist William Perry who coined the term "counter command & control warfare" around the same time (Kaplan, 2016, p. chap. 1)

In 1983, former DARPA director Eberhart Rechtin further defined IW as the war of "sensors and signature control, between codes and cryptoanalysts, between military security and intelligence" (Rechtin, 1983, pp. 28-31). Rechtin combined the idea of a computer network with military organization: different parts of the armed forces would be integrated into one communications network so that the commander would have the

knowledge and the ability to talk to individual battle-groups. This network could distribute the communication flow from the chain of command. Later thinking would call this concept the "system of systems" approach (Owens, 1996) or "network centric warfare" (Gartska & Cebrowski, 1998) and inspire the construction of intelligence sharing networks. However, he also was aware of the risk of his plans. This network could be attacked and information from it stolen or manipulated.

After this initial interest, the matter lay silent for a while or was probably hidden from the public's eye. The Gulf-War campaign against Iraq in 1991 is regarded by some authors as the facilitating condition for a renewed interest in IW and its underlying technology (Mazarr, 1994; Morgan, 2000; Bacevich, 2013, p. 164). Between 1992 and 1996, most documents on this issue were published. In the assessment of the war, two lines of thought developed. On the one hand, the Powell doctrine argued that overwhelming force was responsible for the success in Iraq. On the other hand, the alternative argument was that high-technology that facilitated the victory. The latter became a more convincing narrative because of the general techno-optimism of the time (see chap. 4.2.8 Norms and Key Ideas of Cyber-Utopianism). For the Joint Chiefs of Staff, Desert Storm "highlighted the increasing dependence of the US Armed Forces on information-based technologies and their powerful advantages" (Joint Chiefs of Staff, 1996a, p. 2). The Gulf War put into practice Rona's theoretical concept of digital counter-command and control warfare. For example, during Desert Storm, NSA Rear Admiral John Michael McConnell, a name that features prominently in the history of cyber-war,[106] directed his Joint Intelligence Center to penetrate the Iraqi command and control network. Because American firms had built the Iraqi digital infrastructure, NSA knew the positions of central network switches carrying large portions of enemy troop communications. For the first time, NSA proposed the practice of hacking to be a weapon of war. The idea that were conceived during Desert Storm initiated a process that culminated in a new military doctrine in 1998 (Joint Chiefs of Staff, 1998).

A lot of doctrinal papers that are of significance were written during that time by the armed forces. They present the official, published line of reasoning and are the carriers of early forms of the cyber-realist paradigm in Thomas Kuhn's terms (see Cyber-Realism Corpus). They educate the next generation of paradigm holders (see chap. 2.2 Paradigms and Norm-Change). The IW initiative was mostly driven by the Department of Defense and the military agencies. They pushed IW on the political agenda in order to draft an

[106] Since there are many names advocating cyber-war over the course of time, a full list of key-actors from the US intelligence community can be found in the appendix.

official military doctrine that matched the realities of a globalized, post Cold War security environment (Bacevich, 2002, pp. 131-136). The official IW doctrine documents (see appendix Cyber-Realism Corpus) give an overview over early cyber-realism, its ideas and norms. From the documents, I will extract problem definitions, core concepts, ideas and norms which will then be used to summarize the cyber-realist paradigm and its central elements.

The official or public history of IW began in 1992, the same year Microsoft released Windows 3.1. *Directive TS3600 Information Warfare* a policy memorandum was issued by General Colin Powell, chairman of the Joint Chiefs of Staff. The original directive is still classified but a modified version was made public in 2006.[107] The directive applies to most of the US military branches, the Joint Chiefs of Staff, the defense & intelligence agencies and orders them to implement it throughout the 1990s. For the first time, it gives crucial definitions of information war and related concepts, like *Information Operations (IO)*:

> "The integrated employment of core capabilities of Electronic Warfare (EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), Military Deception (MILDEC), and Operations Security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own" (Department of Defense, 2006, p. 1).

This definition clearly shows that IW originally was conceived as a broad meta-category of war-fighting that includes surveillance, espionage and intelligence operations as well as psychological operations, public affairs, propaganda and diplomacy from various sources. It included EW, such as the use of electromagnetic energy to jam enemy radar systems as well as the broad category of Computer Network Operations or what later is called cyber-war. CNO are different operations like *Computer Network Attacks* (CNA),[108] or what we nowadays call cyber-attacks, *Computer Network Defense* (CND)[109] and *Exploitation* (CNE).[110] This indicates that cyber-war should not be understood in isolation of those other concepts. CNA aims at the intrusion into enemy computers and computer networks

[107] Unfortunately, the difference between the first and later versions cannot be determined due to classification. However, it can be assumed that some core definitions and competencies are to be similar or even the same since they include concepts that can be traced back to Rechtin and Rona and other documents of that time-period. All further elaborations are based on the 2006 version (Number O-3600.01).

[108] "Operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves" (Department of Defense, 2006).

[109] "Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks. […] CND also employs intelligence, counterintelligence, law enforcement, and other military capabilities to defend DoD information and computer networks" (Department of Defense, 2006).

[110] "Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks" (Department of Defense, 2006).

in order to disrupt or destroy them, but also targets information stored in these systems. The directive is quite clear about the range and scope of those applications. The key goal of the DoD policy is:

> "[…] Full spectrum dominance by taking advantage of information technology, maintaining U.S. strategic dominance in network technologies, and capitalizing upon near real-time global dissemination of information, to affect adversary decision cycles with the goal of achieving information superiority for the United States" (Department of Defense, 2006, p. 2).

The central cyber-realist goal of *full spectrum dominance* is refined further in other military doctrines throughout the 1990s. It is defined as an operational advantage based on the ability to collect and process large amounts of information while denying adversaries the same, for example by obstructing the decision-making process. The doctrine aims to integrate various military services as well as intelligence agencies into one coherent military cooperative (called joint operations) and outlines responsibilities for implementation.

In sum, the *Directive TS3600 Information Warfare* is a rather legalistic and technical document that provides no contextual information, explanations or reasons why definitions are given or what necessities are driving the doctrine. It has a declaratory, commanding character. Because it is a rather complex doctrine, I subdivided the analysis into different chapters that follow the logic of paradigms. I start with a quick description of the initial euphoria in the face of of new digital weaponry that quickly turns into pessimism when the problems with interconnectivity are discovered. The problem definitions are central for cyber-realism since they influence and shape the goal formulation. After the problems I will discuss further concepts of the IW doctrine and then turn to its normative implications.

4.4.2.1 Optimistic Cyber-Realism: Revolution in Military Affairs (1992-2000)

When reading the early 1992 US doctrine on information warfare, one gets the impression of a great euphoria because new digital technologies promised to win wars easily by remotely manipulating the enemy's chain of command. This enabled the US to overcome the Vietnam syndrome. The euphoria was called a Revolution in Military Affairs (RMA), the competing line of thought to the Powell-doctrine of overwhelming force. This optimist military theory was formulated in 1992 with the Office of Net Assessment Report (Krepinevich, 1992). The report was a reaction to the Russian military thinking of the mid-1980s. Around the same time when Rona and Rechtin began to think about information war, Soviet military strategists theorized about a revolution in military affairs driven by

information technologies and precision-guided weaponry. Russians called the integration of the two "reconnaissance strike complex". They also predicted the possibility of "electronic fire operations" on enemy communication lines, which could be interpreted as cyber-attacks. The Office of Net Assessment Report tried to test the assumption whether such a revolution was indeed happening and thus it provides the larger, intellectual context and explanations of strategies and guidelines in the 1992 DoD Directive on information war.

The RMA-theory assumes that new technological advances, together with new military operational concepts and strategies that exploit these technologies,[111] can alter the conduct or nature of war itself (Krepinevich, 1992, p. 3). It is an argument based on technological determinism that positions technology as the driver for social change. RMA argues that two key technologies change the nature of war: information communication technology (ICT) and precision-guided weaponry like cruise-missiles (with satellite targeting). These played a crucial role in the First Gulf War of 1991.

Computer communications networks such as the early ARPANET and the Internet played a key role in this concept because they ought to be combined with military weaponry and their supporting infrastructure. In theoretical terms, this represents a new form of social embeddedness of computer networks (see chap. 2.3.5 Phase Model of Technological Diffusion) All military systems would be integrated into one "*network of systems" (or systems architecture*). These inter-networked forces would be able to exchange real-time battlefield information and thus would gain superior knowledge, overcoming the "fog and friction of war". In later military thinking, these ideas would result in military-built technical artifacts called "the Global Command and Control System" (Edmonds, 1996), "WARNET" (McCarthy, 1997) or the Global Information GRID (Department of Defense, 2007). The data stored in these networks would be accessible by all weapons platforms. Cruise missiles could acquire targeting information and the "soldier of the future" (Edmonds, 1996) on the field, equipped with electronic devices, could access real-time data from the battlefield from orbiting spy satellites or Unmanned Aerial Vehicles (UAV).[112]

The result would be a better organized and more efficient force projection, "to pierce the opponent's jugular vein on the first throw" (Owens, 1996, p. 4). The goal is to gain "a comprehensive understanding of a state as a political, social, economic and military

[111] A common example is the use of new tank technology within the operational concept of Blitzkrieg (rapid advances of armored forces) in WW2, which proved to be superior than the competing French military paradigm of defensive war based on the Maginot line.
[112] RMA concepts gave the development of Unmanned Aerial Vehicles a boost that led to combat drones such as the Predator (Blom, 2010).

organism" (Krepinevich, 1992, p. 12). This is not just about militarily relevant information such as troop size or status and position of enemy tanks, but goes much deeper:

> "Information dominance, as used here, is defined as a superior understanding of a (potential) adversary's military, political, social, and economic structures, to include their strengths, weaknesses, locations, and degrees of interdependence, while denying an adversary similar information on friendly assets" (Krepinevich, 1992, p. 22).

Information about all vital functions of an adversary state are to be collected, processed and analyzed in order to get inside the enemy's head (Harris, 2014, p. Prologue). This includes comprehensive knowledge of heads of states, close advisory circles and all information-links at the enemy's command and control decision-making infrastructure. The social and economic functions of a state are to be understood in order to determine exploitable weaknesses. A *comprehensive knowledge of all other states* is the core aim. The optimistic belief is that gathering as much information as possible will result in superior knowledge. If sufficient information is gathered, then the second component becomes active. In case of war, the center of gravity would then be hit by GPS-guided cruise missiles or drone-strikes on targets. That is one reason why information dominance includes knowledge about the physical whereabouts of state leaders (geo-location). The concept of "leadership decapitation" follows logically from RMA-thinking. In fact, the drone war is just a logical outcome of these developments that were started in the early 1990s and clearly exemplifies the political influence of RMA-thought.

Building upon this RMA narrative, Jon Arquilla and David Ronfeldt published a widely regarded RAND article called "Cyberwar is coming!" (Arquilla & Ronfeldt, 1993), a warning that has been uttered repeatedly until the present day. They too, argued that overwhelming force and military budget are irrelevant if the enemy's strikes against ones digital chain of command. With the ongoing information revolution, information would become a strategic resource. Those who control and posses as much information as possible, while denying the adversary the same, would be dominant in this age. Hierarchies would be inefficient compared to new network-centric forms of organization, which follow naturally from the information revolution. In their view, there would be two kinds of war: "'netwar'—societal-level ideational conflicts waged in part through internetted modes of communication—and 'cyberwar' at the military level" (Arquilla & Ronfeldt, 1993, p. 27). Netwar refers to psychological operations and propaganda by smaller, asymmetric enemies like terrorists. Cyber-war revolves around the destruction and disruption of the enemy's information systems, crippling the enemy's command and control. They argue that

"cyberwar may be to the 21st century what blitzkrieg was to the 20th century" (Arquilla & Ronfeldt, 1993, p. 31).

The appeal of this new mode of warfare was obvious, especially with the Vietnam syndrome in mind. The US was the technologically most advanced country in the world, so it seemed obvious, at least for a while that it would benefit from this revolution. It had advanced sensors and superior precision-strike capability. It also had information dominance with its vast array of satellites and its global spy network Echelon. In 1995, General Jay Garner brought the optimist RMA narrative into the public by giving an interview with Time magazine. He argued that because of new information technologies, war would be revolutionized. A war, theoretically, could be ended before it began, without the loss of human life, which was a major concern after Vietnam (Thompson & Waller, 1995). The prospect of winning a war by digital means by disrupting the enemy's command and control before an attack seemed promising (Rid, 2016, p. 371).

However, this optimism was only one side of the story that quickly vanished when NSA and others realized in secrecy, that the very same principles of information war could be turned against the United States. Over the course of the 1990s, optimism about the digital revolution turned into pessimism. The Internet quickly became a problem, especially for Signals Intelligence agencies like NSA. The next chapter will introduce the problem definitions that lie at the core of cyber-realism.

4.4.2.2 Problem Definitions of Cyber-Realism

This chapter analyzes the central ideas of cyber-realism and their evolution. Thomas Kuhn argues that one characteristic of a paradigm is that it defines what counts as a problem. What constitutes a problem for a paradigm is based on the perception of the world. The characteristics of the problem define appropriate solution strategies (see chap. 2.2 Paradigms and Norm-Change). This chapter identifies the core problems that the cyber-realism identifies with the unfolding Internet during the 1990s. These problems are the foundation for a cyber-realist technological frame that defines norms and policies in order to deal with the unfolding digital revolution.

Most of the analyzed doctrinal papers start with a diagnosis of the impact of new ICT on traditional military and state conduct (see appendix Cyber-Realism Corpus). Like their utopian counterparts, they diagnose a transformative power of the Internet that is indicated with terms like the "explosive proliferation of ICT" or "technological/information revolution" ushering in the "Information Age" or a "new frontier", which are widely used metaphors in these documents. For example:

> "The information age is here. Rapidly advancing information-based technologies and an increasingly competitive global environment have thrust information into center stage in society, government, and warfare in the 21st Century" (Joint Chiefs of Staff, 1996a).

This tech-deterministic argument serves as a diagnostic frame and is line with Kuhn's assumptions that new paradigms often turn to epistemology and ontology, defining what the nature of things are (Kuhn, 1970, pp. 73-88). A revolutionary character or a transformative power is attributed to the Internet and ICT in general (Feaver, 1998, p. 98). It is believed that the Internet will change everything, social order and the conduct of war and there is no escape from it. Technological progress is the driving force to which social reality has to adapt. In that regard it is similar to cyber-utopian thinking. That cyber-realists pick up utopian frames shows the discursive dominance of these. While this change is positive for utopians, it produces a set of problems for military impact constituencies (see chap. 2.3.6 Combining the Frameworks). The problems are directly related to the technical design of the Internet:

> "Within the last decade, personal computers, workstations, data bases, and mainframes have been interconnected into distributed information networks. This interconnection is continuing at an ever-increasing rate. Through the Internet and other data networks, government networks are interconnected with commercial networks, which are interconnected with military networks, which are interconnected with financial networks, which are interconnected with the networks that control the distribution of electrical power, and so on. It is now almost impossible to distinguish where one network ends and another begins in this extensive and complex information Infrastructure" (Joint Chiefs of Staff, 1996b, pp. 1-4).

The core logic of TCP/IP, linking networks together into a large inter-network, is perceived as problematic because all different kinds of networks (military, government, banking) are interconnected in one large, increasingly globe-spanning communication structure. *Interconnectivity*, one of the goals and norms of the engineering-paradigm, is seen as a problem. As I have shown in the chapter on technical affordances of TCP/IP, networks within the Internet are not aware of the overall structure and it is difficult to shield sub-networks like military nets from intrusion (see chap. 4.1.3.1 Artifact: Internet Protocols and Norms). Theoretically, it is possible to enter every network in the Internet, given that access controls and security measures (Firewalls etc.) can be circumvented. Computer researchers quickly reached the conclusion that the only way around this problem is "air gapping", to physically disconnected sensitive networks from the internet

infrastructure (Aitel, 2013). The problem definition has two major dimensions, *dependency* and *vulnerability*, which each produce a subset of minor problem definitions.

First, it is argued that the US Government, the economy and the military are *dependent* on this infrastructure.

> "The national security posture of the United States is becoming increasingly dependent on U.S. infrastructures. These infrastructures are highly interdependent, particularly because of the internetted nature of the information components and because of their reliance on the national information infrastructure" (Joint Chiefs of Staff, 1996b, p. 1).

Indeed, some observers estimated that even in 1996, 95% of military command and control communication was transmitted through public-switched networks, i.e. the Internet. (O'Neill, 1997). The *"internetted nature"* is perceived as a problem. This dependency spans across all societal sectors: military, economy, politics and society in general. Financial transactions are done electronically as well as maintenance and control of the electric energy network. The general gist of the argument is that an information- or network-economy such as the US requires the Internet to function.

The second problem dimension is that this new ICT infrastructure, and everything connected to it, is *vulnerable* to information war and CNO, as developed by the US. In other words, the US could become the target of the same techniques it wants to apply to others:

> "Today's concept of national security extends beyond military protection of of borders, and is based on connectedness. Disruption, denial, or destruction of government, commercial, utility, or social-service infrastructures is unthinkable; even the temporary loss of service due to a natural disaster can have effects that ripple throughout society. The use of information technologies to simplify, enhance, or speed operations has led to massive dependence and, consequently, critical vulnerability" (O'Neill, 1997, p. 189).

The structure of this argument stays the same during the whole cyber-war discourse, even until the present day (see chap. 4.5.4 Discourse: Cyber-Doom and the Hegemony of Cyber-Realism). This RMA-inspired idea of *strategic cyberwar* assumes that a strike on this internetworked infrastructure *could* cascade through the network and therefore *could* disrupt or destroy everything else connected to it. This is the worst-case scenario and at the same time the master frame for legitimizing the cyber-war doctrine. It is argued that a cyber-attack against a internetworked system X (where X could be replaced by any electronic system such as online-banking, air-traffic & transportation, communications

networks etc.) *could* (in theory) bring the entire operation of connected systems to a halt and therefore cripple a society depending on these infrastructures, causing death and physical harm.[113] In short, it is assumed that cyber-attacks can shut down an entire nation. In discourses, the clearest expression of this master-frame is the "digital Pearl Harbor" metaphor that was coined in 1992 and constantly reiterated by cyber-realist advocates such as Bill Clinton's national security advisor, and George W. Bush's "cyber-czar" Richard W. Clarke in 2002:

> "A coordinated cyber attack on the nation's critical computer networks. Such an attack could well succeed in shutting down 911 systems, shutting down telephone networks, and transportation systems. You black out a city, people die. Black out lots of cities, lots of people die. It's as bad as being attacked by bombs" (Bacevich, 2002, p. 120).

Besides the "crippling blow thesis", IW theorists deduce a whole range of other threats and dangers from the dependency and vulnerability argument. For example:

> "The lack of geographical, spatial, and political boundaries offers further anonymity and legal and regulatory arbitrage; this lack also invalidates previously established "nation-state" sanctuaries. Information warfare is also relatively cheap to wage, offering a high return on investment for resource-poor adversaries" (Joint Chiefs of Staff, 1996b, pp. 1-5).

One part of that vulnerability argument is for example "the availability and relatively *low cost of these technologies* in global markets that "increase the likelihood of an adversary buying and using IW technology (Joint Chiefs of Staff, 1996a). Since the 1991 Computers at Risk Study from the National Research Council (National Research Council, 1991), the argument is brought forward that a skilled individual can do more with a cheap computer than a terrorist with a bomb. Indeed, the history of hacking incidents (see Table 9. List of Internet Milestones and Security Incidents) indicates that skilled, young computer geeks indeed were able to infiltrate insecure communications systems. Individual and collective hackers became a threat figure during the 1990s, just as cyber-utopians predicted (see chap. 4.2.5 Framing Cyberspace as the Electronic Frontier (1990s)). Computers were becoming cheaper during the 1990s, which facilitated their massive diffusion. This availability of knowledge produced "rapid growth of a computer-literate population"

[113] A common feature of IW and cyber-war literature is the similar narrative structure. Articles first diagnose a revolutionary change, point to dependency and vulnerability and then typically provide a list of critical infrastructures that are interconnected and then include a threat argument that hypothesis a terror-attack or a critical failure. This discursive mechanism has been extensively researched (Deibert, 2003; Dunn Cavelty, 2007; Dunn Cavelty, 2013a; Hansen & Nissenbaum, 2009).

whose members "possess the skills necessary to conduct such an attack" (President's Commission on Critical Infrastructure Protection, 1997). This might be an implicit recognition of the "empowerment thesis" that is mostly brought forward by cyber-utopians (see chap. 4.2.8 Norms and Key Ideas of Cyber-Utopianism). In general, "threats include, but are not limited to, computer hackers, criminals, vandals, terrorists, and nation states" (Joint Chiefs of Staff, 1998, pp. I-15).

"*Easy access", "cheap hardware"* and "*knowledge diffusion"* to launch cyber attacks are seen as a key problem for the state. The argument here is that c*yber-war favors or empowers the weak* while making high-tech information economies more vulnerable (Lindsay, 2013, p. 375). It is argued that everyone could be an information-warrior because "much of the technology needed to attack information systems is low-cost (a computer, a modem), widely available (a willing hacker) and just as efficient (one phone call)" (Thompson & Waller, 1995). Why is this problematic? Because the cyber-realist paradigm sees ICT and information as a weapon, which will be elaborated on a little later. For now, the list of problem definitions needs to be completed.

Another perceived problem is the global nature of the Internet technology because, at the time, it became truly world-wide. Three problems are central: "*the lack of state borders",* the "*death of distance problem"* and *"the problem of international jurisdiction*". These problems were recognized in official government documents for the first time in 1996. It makes sense to discuss them together because they all have to do with the way TCP/IP was designed. The Inter-network has no intelligence of physical space and therefore it does not know what borders are. Packets randomly choose the most efficient route through a network and do not even notice that they travel through different networks or national jurisdictions. Therefore, packets do not recognize government borders. Dynamic routing is so fast that distance is ultimately reduced: packets or a message can reach the other end of the world in less than 3 milliseconds. Because of the norm of openness, there is no content or usage restriction. This means that all kinds of digital information (including malware, propaganda, pornography and cyber-attacks) can stream into a network in the form of packets. The openness norm is perceived as a dual-edged sword by cyber-realists:

> "The speed of information warfare attacks, coupled with near-anonymous offensive capabilities, makes it difficult to differentiate the nature and source of possible attacks. While information systems and network management tools (e.g., access logs, intrusion detection systems) offer possible sources for I&W, the government does not own or have complete access to these sources and does not have the authority to monitor them" (Joint Chiefs of Staff, 1996b, p. 106).

The result is that network operators (and governments) can no longer *control* what digital information enters the US Internet from the global outside. The IW doctrine clearly states that the government does not (yet) have the authority to monitor a nation's Internet.

Both the *speed of information* and the *sweeping nature of data transmission* produce two implications for actors concerned with national security, intelligence and law enforcement: first, an information war-attack can be launched from another jurisdiction and arrives at the target instantaneously. In other words, there is *no pre-warning mechanism* like with conventional attacks (Molander et al., 1996, p. xiv). Second, a target could strike *from everywhere on the globe*, as long it is connected to the Internet. Geo-strategic features such as oceans or mountains are non-existent in cyberspace. Distance does not protect anymore because in cyberspace, adversaries are virtually in close proximity to each other. This is what is meant by the death of distance metaphor.

The third problem is that of *jurisdiction*. The Internet is described as an infrastructure "over which the government has little control" (Joint Chiefs of Staff, 1996b, p. 1). Because of the decentrality of network design, large portions of the Internet operate outside the control of governments. 95% of the physical and digital Internet infrastructure is run by private entities over which the government has only indirect influence. The 1990s were dominated by economic deregulation, which gave government regulation, for example of Internet content, a bad reputation (see chap. 4.3.4 Artifacts: Privatizing Control over the Internet). Internationally the physical infrastructure is decentralized as well: it is located within different countries and jurisdictions. No government can simply super-impose control and regulation over the entire infrastructure, at least not as easily as in other areas of government regulation.

A closely related issue that was discovered during the mid 1990s is that TCP/IP provides a basic level of *anonymity*. The idea that "on the Internet, nobody knows you are a dog" was a common perspective in thinking about the Internet during the 1990s and was also adopted by cyber-utopians (see chap. 4.2.8 Norms and Key Ideas of Cyber-Utopianism). This also has implications for IW because it "offers a veil of anonymity to potential attackers" because they "can hide in the mesh of internetworked systems and often use previously conquered systems to launch their attacks" (Joint Chiefs of Staff, 1996b, p. 5). This problem would later be called the *attribution problem*. It is defined as "assigning a cause to an action […] identifying the agent responsible for the action (specifically, "determining the identity or location of an attacker or an attacker's intermediary") (Clark & Landau, 2011, p. 25). It describes difficulties of monitoring and

tracing what an actor (represented by an IP-address) is doing online. The IT-community was aware of this problem since the Morris worm of 1985 and intelligence actors began pondering the issue since the mid-1990s. Not knowing who is responsible for an action in cyberspace (like an CNA) has severe ramifications for the use of the Internet for war and surveillance, deterrence, coercion and retaliation, as scholars like Libicki (Libicki, 2009) and Rid (Rid, 2012) argue. The attribution problem is both a *technical* and a *social or political problem* (Landau, 2010, p. chap 3.7).

On the technical side, the problem has to do with how TCP/IP was designed because "typical computer network environments are not designed to support attribution of attackers" (Wheeler & Larsen, 2003, p. 4). TCP/IP was not designed to monitor what an actor does on the Internet (internal intelligence) and this is a logical obstacle for any actor who wants to determine this fact (see chap. 4.1.3.1 Artifact: Internet Protocols and Norms). For example, to trace a CNA or CNE to its original IP-address would require the log-protocols[114] of every intermediary node (router) through which packets of the attack were routed. As has been shown, one packet easily crosses several jurisdictions and most messages (depending on size) consist of hundreds, if not thousands of packets that are all routed randomly through different subnetworks and countries. Obtaining log files that (might) indicate which IP-address launched a cyberattack is difficult. Obtaining this logging information from foreign governments can be a huge legal and diplomatic obstacle. It gets particularly complicated if the packets are routed through failed states with weak law enforcement or a botnet of remote-controlled computers. This is what the Joint Chiefs of Staff paper means when it says that "the government does not own or have complete access to these sources and does not have the authority to monitor them" (Joint Chiefs of Staff, 1996b, p. 106).

Additionally, TCP/IP has no authentication mechanism built in that guarantees that a packet indeed originated from a source.[115] This weakness allows for a practice called "spoofing", the faking of an IP-address (Clark & Landau, 2011, p. 27). As a result, even if one could retrieve the source IP address for a cyberattack there is no guarantee that the attack really originated from this location. Another problem is interference with routing.

[114] Most computers and routers in a network produce log files that document every activity of that server. These files for example document incoming and outgoing packets, data flow in the network and general system activity. These logs are essential for system maintenance and security because they document time, date, and location of possible intrusion and sometimes even file access, or bandwidth use. They are therefore substantially important pieces of digital evidence to investigate cyber attacks (Chaikin, 2007).

[115] "The weakness in IP is that a source host itself fills the source address field in the header of an outbound IP datagram. In theory, any host can transmit an IP datagram with any source address. […] There is no guarantee that a datagram was actually sent from a given source" (Mutaf, 1999, pp. 18-19). In contrast, intelligent-network designs such as X.25 would allow easer network surveillance and therefore identification of packet-origins.

There are easy-to-use technologies available (such as Virtual Private Networks or Onion Routing) that allow artificial re-routing. An attacker can direct his attack through another country to give the impression that it originated there, increasing the possibility of false-flag attribution (Lindsay, 2013, p. 377). Finally, most cyber-attacks are multi-staged, as the Joint Staffs recognized. "Computer A penetrates computer B, which is used as a platform for penetrating computer C, which in turn is attacks computer D" (Clark & Landau, 2011, p. 1). Even if it were possible to trace the IP-address of the attacking computer D, this does not necessary mean that the attack really originated there.

Besides the problem of technical attribution, there is the problem of social attribution. An IP-address identifies a machine or in many cases just a local-area network, but not the human operator. How do we know who did it, if the origin-IP address is an Internet cafe with an open WIFI network, where every passing computer or mobile phone could get access to? To assess the identity of the originator, further sources of data are needed. In most cases, trace evidence from the application layer (for example login information of webservices or billing addresses) is used for that. To attribute Internet activity to an actor requires multiple kinds of data, or in other words – better more than less. This is a strong impetus for the idea of mass data collection. The attribution problem explains why most cyber-attacks can just be vaguely attributed and why political statements regarding state-sponsorship of CNA must always be critically evaluated. The possibility for false attribution and political instrumentalization is tremendously high.

It should have become clear by now that besides opportunities for interconnected systems of systems and the exploitation of the information space for military and intelligence actors, the Internet technology creates a set of core problems (dependency, vulnerability, geographic problems and the problem of attribution) for their own military operations, law enforcement and intelligence gathering. Thus, the Internet is predominantly seen in negative terms by impact constituencies tasked with national security. These problems can be, in most cases, traced back directly to how the Internet works and how TCP/IP was designed. This diagnosis is central because it provides the fundament for solution strategies which basically aim at solving issues such as traceability of cyber-attacks by exercising total control over the Internet. Before we turn to that, it is important to look at other ideas and norms that develop in the early information warfare doctrine. These other ideas further contextualize the perceived problems and create a coherent meaning network that frames the issue of computer security from a concrete, military security perspective.

4.4.2.3 Core Ideas: Information Weapons & Digital Battlespace

Before we turn to solutions to the aforementioned problems, it is necessary to analyze some of the key ideas of cyber-realism. The aim here is to show how ideas from the IW concept lay the foundation for the norm that the state, represented through its military, should exert control over information systems like the Internet. In this early stage, the norm is not clearly pronounced but it is implied in the logic of IW. These documents understand control as the ability to monitor information traversing the global information infrastructure. Control includes the ability to disrupt and alter information traversing the Internet on the content layer. This later gets expanded to include the workings and functionality of this very infrastructure at the physical layer.

As indicated before, *information* is the central concept in IW. Information is defined as "perceived phenomena (data) and the instructions required to interpret that data and give it meaning" (U.S. Department of the Air Force, 1995, p. 2). For the military, precise and timely information, for example knowledge of enemy positions, is crucial for war fighting. It is believed to mitigate the effects of the so-called "fog of war", a metaphor invented by Carl von Clausewitz describing uncertainty on the battlefield resulting from unclear information (Bacevich, 2002, p. 133). The Air Force (1996) and the Joint Chiefs argue that war is about the competition of information, which might be "as old as human conflict […] a defining characteristic of humanity" (U.S. Department of the Air Force, 1995, p. 1). This implies an instrumental character for gaining an advantage in a battle situation. A central element of the paradigm is a new relevance that is attributed to information: "Information itself is becoming a strategic resource vital to national security" (Joint Chiefs of Staff, 1996a, p. 19), a "strategic asset" (Schwartau, 1997, p. 49), or ultimately *a weapon* (Rechtin, 1983). This is a key element of cyber-realism:

> "Knowledge as a resource is not included in the current resource paradigm of manpower, materiel, money, forces, and logistics. Knowledge, the "ammunition" of information war, is inexhaustible. Once produced (at a cost), knowledge can be used repeatedly – it will not disappear. In fact, it only increases! Digital knowledge can be copied and never missed. It can be given away but still kept. Digital knowledge can be distributed instantly" (Fast, 1997, p. 12).

The idea of *information as a weapon* that can be exploited against adversaries whose societal functions depend on the distribution and processing of information (i.e. information economies) is one of the central ideas in the cyber-realist paradigm. This frame legitimizes and normalizes the mass acquisition of information by military actors. Weapons and the use of force seem to fall naturally into the domain of the military. In

other words, military actors position themselves as the appropriate actor for the job. The newly discovered relevance of information is presented as an utterly new element in military thinking. This idea is the fundament for understanding many related cyber-realist concepts like espionage, exploitation of information and disruption of communication flows. If information is valuable, then exploitation and espionage is a kind of theft. It is driven by the fear that someone uses this weapon against ones own infrastructure. It also legitimizes the military asserting a role as defender against these issues, which is its primary function in a state. It also explains the ultimate goal of IW: "We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same" (Joint Chiefs of Staff, 1996c, p. 16).[116]

The goals are to be reached with the instrument of Information Operations. IO, the use of computer hacking and exploitation are described as appropriate tools for the end of information superiority. IO directly target *information* (the content) as well as *information systems* (i.e. the delivery structure such as computers & networks) in order to affect an adversary's decision-making process. Again, if information is a weapon, then the destruction or disruption of that weapon or its supporting infrastructure, becomes an appropriate military goal. Computer networks that are used in command and control are of special importance here. Offensive IO, such as computer network attacks play a special role. The idea of intrusion into the digital infrastructure of an enemy in order to either passively monitor or actively alter information in data-bases resembles Rona's idea of digital deception. Therefore, CNA and CNE are twin-concepts or two sides of the same medal. Both attack and exploitation require first and foremost an infiltration of enemy systems via security weaknesses, backdoors or social engineering (Wilson, 2006, p. 5). Once inside a computer system/network, analysis is required to identify ways to shut down or disrupt a system which at the same time is exploitation and intelligence gathering. Only the end-product (the payload) of the operation differs – exploitation aims at data exfiltration or manipulation and tries to mask its presence, whereas disruption (CNA) produces visible effects. CNE is a logical precondition for CNA and CNE is the more valuable operation, because it extracts valuable information that is required for CNA (Lewis, 2002, pp. 7-9). For the key goal of information superiority, computer network exploitation is the far more important (policy) instrument (see chap. 2.2.3 Degrees of

[116] Bacevich argues that the aim is "to achieve something approaching omnipotence" (Bacevich, 2013, p. 133).

Change). In sum, although spectacular cyber-attacks dominate the news, it is very likely that the number of undetected CNE is way higher.

The official US doctrine is quite transparent about the designated targets of computer espionage (U.S. Air Force, 1998). The doctrine adopts the holistic or organic perspective that was outlined by the RMA theory (see chap. 4.4.2.1 Optimistic Cyber-Realism: Revolution in Military Affairs (1992-2000)). Targets include enemy heads of states as well as leading economic and social figures. It is a state-centric approach, another similarity to realism as an IR theory. All vital functions of a state are targets of IO – energy and financial infrastructure, manufacturing, telecommunications. It basically targets everything within a society and particularly *critical infrastructures* that guarantee the basic operation of a state.

It is furthermore argued that IO have the "greatest impact in peace and the initial stages of a crisis" (Joint Chiefs of Staff, 1998, p. viii). Intelligence gathering, CNA and CNE are to be conducted in peace and war and this somewhat makes sense from a military perspective. It is logical to be prepared, to have targeting lists and contingency plans in case of war. However, the idea basically transcends the notion of war having a clear-cut beginning and end. *IW is permanent*, in peace and in war. It need not be declared, which has severe legal implications, which are not discussed in the major doctrines (Bitton, 2014).

It is total in the sense that the distinction between offense and defense is blurred because "offensive IO also can support defensive IO […] because they are so interrelated […]" (Joint Chiefs of Staff, 1998, pp. 3-13-14). Other military thinkers would go as far and argue:

> "Traditional distinctions—public versus private interests, warlike versus criminal behavior—and geographic boundaries, such as those between nations as historically defined, are complicated by the growing interaction within the information infrastructure" (Molander et al., 1996, p. xiii).

The blurring of traditional dichotomies like war–peace, front–homeland, public–private, war–crime is a reoccurring theme in scholarly articles about the Internet of that time and is also articulated by cyber-utopians. This has to do with the way the Internet is perceived. Since the Internet transcends traditional geography and connects all mankind through one network, the distinction between homeland and front-line does not make sense anymore. It is quite interesting how the military actually perceives this infrastructure.

The military aligns itself partly with the idea of the Information Superhighway (see chap. 4.3.3 Ideas: Cyber-Utopia on the Information Superhighway (1993)). It talks about the so-called Global Communication Infrastructure (GII)[117] which includes the US National Infrastructure (NII) and the Defense Information Infrastructure (DII). This includes all communication channels that can store or transmit any kind of information (News, Media, Internet). The definition includes both the software (databases) and hardware of this information structure (like fiber-optic cables) and is therefore more precise than cyber-utopian ideas of a predominantly digital and virtual cyberspace. Cyberspace indeed has a hardware base that operates under different conditions than software protocols. With hardware, geopolitics and military force matters, because it can be physically destroyed. Most of the physical infrastructure of the Internet is located at dense metropolitan areas and diffused along areas with substantial economic relevance, whereas in remote areas no broad-band Internet can be found (Botnet, 2012). The physical infrastructure of cyberspace is not as space-less and immaterial as utopians assume. However, cyber-realism still has a somewhat metaphysical understanding of this global information structure. The Internet is understood as a *realm:*

> "In many respects, one can consider information as a realm, just as land, sea, air, and space are realms, information has its own characteristics of motion, mass, and topography, just as air, space, sea, and land have their own distinct characteristics. There are strong conceptual parallels between conceiving of air and information as realms. […] But the Information Age changed the information realm's characteristics so that widespread military operations within it became practical" (U.S. Department of the Air Force, 1995, p. 6).

Defining the Internet as an operational domain or realm is noteworthy because it implies that the military plays an appropriate role therein. The military asserts a role, it claims a stake or it begins to "colonize" cyberspace to use utopian frames (see chap. 4.2.5 Framing Cyberspace as the Electronic Frontier (1990s)). More so, based on the realist belief in the centrality of the state, it claims to be the dominant actor therein. Interestingly, the notion of the realm or domain implicitly builds upon the cyber-utopian metaphor of cyberspace as a distinct digital space that has certain properties. Cyber-realists and utopians frame the same thing, the Internet, in similar ways but reach different interpretations and conclusions. Cyberspace is said to have the aforementioned distinctive

[117] "The GII is the worldwide interconnection of communications networks, computers, data bases, and consumer electronics that make vast amounts of information available to users. It encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites and satellite ground stations, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more" (Joint Chiefs of Staff, 1998, pp. I-13f.).

characteristics (like the lack of borders, death of distance etc.). Cyber-realists assume that it functions similar to material realms, but is yet different because it is a man-made, digital construct. In sum it can be argued that cyber-utopian and realist ideas are two sides of the same coin. They operate with similar assumptions about the nature of this new technology and assign similar technological frames (such as the death of geography or the ideas of a distinct cyberspace). However, they perceive the same thing differently. Military actors focus, as it seems to be in their operational DNA, on the negative aspects and the potential threats to national security while utopians focus on the positive side of things.

Implicit in these ideas are certain norms, which will be distilled in the next chapter.

4.4.2.4 Analyzing Emerging Norms of Cyber-Realism

This chapter analyzes the normative implications of the IW doctrine. It shows how certain ideas and problem definitions construct certain imperatives for action that over time become normalized until they are seen as standards of appropriate behavior. In line with Kuhn, norms emerged out of the problem-solving practices of cyber-realists (see chap. 2.2 Paradigms and Norm-Change). Initially, these norms were not completely articulated, mature or even dominant outside the context of military and IC.

The first point is the *perceived chaos and lack of control of the Internet* that is seen as potentially dangerous for national security of the US. The Internet is said to enable small actors engaging in offensive attacks and no one knows what is going on because technical features of TCP/IP prevent visibility. The protocols create an artificial "fog of war" because no central watchtower is able to see what actors are doing on the Internet. Anonymity and the attribution problem prevent control. Exerting authority by states is complicated by TCP/IP because there is no central activity logging. From this perceived core problem follows a powerful imperative: the US should be able to know what is going on.

Second, IW claims that *the military should have information dominance*, i.e. awareness of information traversing the global information infrastructure. Because this is not easily possible, this dominance should be achieved through information operations, defined as computer network attacks, espionage and defense. Inspired by techno-optimism and the RMA tradition, new technological capabilities and strategies are seen as the solution to this problem.

Third, from this follows a kind of *strategic imperative for the mass accumulation of data*. Information is treated as a resource that should be collected and massively accumulated to gain information superiority over the enemy. Following from the

Clausewitzean notion of war, more information about the battlefield is always better. This includes a holistic approach and social, economic and political information.

Fourth, treating *information as a weapon serves to legitimize the military's role in cyberspace*, because the use of force and violence falls into the natural turf of the military. This is further extended by the rhetoric framing of hacking, i.e. the intrusion into foreign networks as an computer network *attack*. This militarized language legitimizes the role of the military, as Dunn Cavelty argues (Dunn Cavelty, 2013a). In theoretical terms, this framing represents an attempt to counter-signify the Internet, giving the technology a new meaning (see chap. 2.3.6 Combining the Frameworks). Framing the Internet as dangerous creates the need to defend the US from adversaries that develop computer network capabilities. During the mid-1990s, however, this language is contained within military discourses and not very public, thus it serves more the function of internal sense-making.

Fifth, defining *cyberspace as a distinct military realm or domain serves to assert this role*. It is an attempt to claim the stake that the military has a role to play in cyberspace. This is noteworthy because this infrastructure was created by academics (with military sponsoring) but is run by private enterprises. The Clinton/Gore administration specifically gave primacy to the private sector and now the military is claiming to be relevant as well (see chap. 4.3.3.1 The Hands-off Norm & the American Internet Governance Model). In theoretical terms, the military is structurally excluded from cyberspace and thus not in a natural position to make that kind of claim. Arguing that it is appropriate for the military to assert a role in cyberspace, guaranteeing its protection, resembles a counter-appropriation strategy to compensate for the perceived exclusion (see chap. 2.3.6 Combining the Frameworks). The IW doctrine itself elaborates on this issue that the military is in no natural position to control the Internet because it neither has the competencies nor the capabilities. "Legal arbitrage" as they call it, prevents this (Joint Chiefs of Staff, 1996b, pp. 1-5). In cyber-utopian terms, this is a kind of colonialization of cyberspace by force.

Sixth, the concept of *IW blurs the traditional dichotomy of war and peace*. The goal to achieve information dominance through computer network attacks is said to be most efficient in peace. Thus, the extraordinary practice of intruding into someone else's network via CNE is normalized. It is presented as an appropriate state practice, regardless of legal obstacles in form of the humanitarian law that sees peacetime espionage as highly ambivalent (Bitton, 2014, p. 1018).

Seventh, the death of distance and the argument of a *borderless cyberspace normalize the practices of exercising authority* over someone else's territory. Intruding into another nation's network to exploit information stored on a server located in another

nation's territory could be regarded as a hostile act, as is stealing information from the White House.

In sum, the *IW doctrine lays ou the foundation of the norm of control*, i.e. that the state, through its military and intelligence agencies, has the natural right to monitor the global Internet infrastructure. Control works on two levels. First, by being aware of the content or information that is exchanged over this medium (the content layer) and by being able to manipulate or alter this information. Second, by being able to control the very workings or functions of this infrastructure on the physical layer. We should not forget that the early IW doctrine explicitly mentions the concept of electronic warfare and the idea to disrupt the electromagnetic spectrum or the physical transmission of electrons. The IW doctrine claims that it is appropriate for states to disrupt the workings of the communications infrastructure of another country, i.e. shutting down the phone network or Internet, by utilizing CNA. What might be appropriate in times of war, is not necessarily so in peacetime. But IW intentionally blurs this dichotomy. The following graphic summaries the key ideas, norms and frames of early cyber-realism during the 1990s.

Figure 25. Cyber-Realism during the 1990s (own diagram)

Cyber-Realism	
problem → goal	- increasing technization and interconnection of military command and control (since 1976), impact of ICT on state conduct - possibility of computer exploitation (since 1976) - perception of an information revolution, and RMA (diagnostic frame) - Information age as a problem (1990s) - modern societies depend on Internet - interconnectivity creates vulnerabilities, CNA could bring an information society to a halt (crippling strike thesis) - availability of low-cost tech - Internet features as a problem: death of distance problem, transcendence of state borders and problems of jurisdictions, speed of CNA, no pre-warning - anonymity of the Internet is a core problem (attribution problem), lack of government control - protocol openness of the Internet is a problem - → Information Dominance/Superiority - → penetrate fog of war with information operations
anticipated use	- Internet for military command and control - used by adversaries for hacking U.S. critical infrastructure
social elements (norms, power)	- military as defender of cyberspace - counter-appropriating the lack of military control over cyberspace - it is appropriate for military to penetrate enemies networks, even in peacetime

It is important to state that the norm of control, at this stage, is only implicit in the doctrine. This represents the emergence of a norm within closed military circles (see chap. 2.1 Norms and Theories of Normative Change). The meaning of the Internet during that time is still dominated by cyber-utopian and liberal ideas. The chapter showed nicely how standards of appropriate behavior depend on problem perceptions and definitions and thus the standpoint of observation, i.e. the paradigm. The next chapter will explain how this

norm got expanded and diffused outside of military circles and inside into the political administration, which is an important condition for cyber-realist norms becoming dominant during the mid-2000s.

4.4.3 Setting the Path: The Institutionalization of Cyber-Realism

Whereas the last chapter introduced the ideational and normative content of the early cyber-realist paradigm, represented through the IW doctrine, this chapter discusses the process of institutionalization. As the result of the intellectual formative period since 1992, advocates and holders of the cyber-realism paradigm have been creating organizational structures. The institutionalization of the paradigm in military bureaucracies made the paradigm more permanent than its utopian counterpart, which was predominantly held by a loose actor coalitions without fixed structures or platforms. Institutions, such as military branches, also allowed the recruiting and socialization of new actors or paradigm advocates into cyber-realist thinking that would later serve within the administration and thus act as norm-entrepreneurs from within the government (see chap. 2.2 Paradigms and Norm-Change). This is a key explanation why cyber-realism could permanently influence US decision making and that it could become the dominant paradigm in the mid-2000s.

NSA established its Information Warfare Center in 1992. In secrecy, NSA began developing techniques for launching "information warfare attacks", breaking into computer networks and destroying them from the inside (Harris, 2014, p. chap. 3). NSA began collecting known and unknown security vulnerabilities (zero day vulnerabilities)[118] in Internet hard and software that could be exploited for infiltrating computers and networks (Harris, 2014, p. chap. 6). The US armed forces established several IW centers like the *Defensive Information Warfare Program (1992)* (Saalbach, 2015, p. 58) or the School for Information Warfare and Strategy at National Defense University in Washington D.C, and *NIWA, Navy Information Warfare Activity* (both 1994). In 1995, the Air Force established its first *Information Warfare Squadron* in South Carolina (Department of the Air Force, 2006) and the army established its *Land Information Warfare Center* in 1995. Before becoming director of NSA in 1996, Kenneth Minihan led the Air Force Information Warfare Squadron. Its official mission was to defend Navy networks from intrusion, but its secret other mission was to "threaten information systems of America's adversaries"

[118] "A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack [or exploit]" (Symantec, 2016). In theoretical terms, it is information about an entry-vector in a target system that can be utilized by an offensive malware. As such, zero days are the "most effective cyber weapon" (Harris, 2014, p. chap. 6) because there is no defense against it until the vendor fixes the vulnerability.

(Kaplan, 2016, p. chap. 7). Later, as head of NSA, Minihan set up the *Information Operations Technology Center* which gave NSA a more offensive posture. In 1996, the FBI formed the *Infrastructure Threat Assessment Center* to investigate cyber-crimes and the Data Intercept Technology Unit (DITU), a domestic signals intelligence operation, in 1997. The CIA created a top secret unit called Information Operations Center, designed for the more physical side of network attacks like planting agents inside an enemy's infrastructure to distribute malware in air-gapped systems (Kaplan, 2016, p. chap. 7).

The purpose of this short chapter was to show how cyber-realist ideas became institutionalized. These institutions play a major role during the politicization and spill-over of realist ideas into the political discourse of critical infrastructure protection and the Kosovo war. Institutions outlined in this chapter sponsored key personnel for presidential commissions and advisory panels, which allowed classified cyber-realist concepts such as IW to spill into the discourse of political elites and decision-makers. This will be discussed in the next chapter.

4.4.4 Politics: Turn to Realism - Critical Infrastructure Initiative (1996-1999)

This chapter explains the politicization of cyber-realist core ideas into a wider political discourse in the second half of the 1990s. This indicates a shift from early Information Superhighway cyber-utopia to critical infrastructure protection and technological pessimism. It also marks the shift from concepts developed in secrecy and inside the military sphere into policy discourse. I argue that although the Clinton administration initially adhered to a utopian, optimistic perception of the Internet (see chap. 4.3.3 Ideas: Cyber-Utopia on the Information Superhighway (1993)), its perception began to change due to a series of events in the mid-1990s. The causal mechanism explaining this subtle turn to realism is a *rapid succession of critical events that were used by cyber-realist advocates to push their agenda*. Cyber-realist problem definitions, particularly the problem of network-interconnectivity and ICT-dependency and vulnerability became embedded in the discourse on critical infrastructures. This is due to persistence and continuity of personnel: realist advocates held key positions in relevant commissions to diffuse their agenda. This led to a cumulative learning effect: the more incidents happened, the more public leaders were convinced of cyber-realist ideas (see chap. 4.4.1 Background: Growing Awareness of Computer Insecurity (1967 - 2011)). At the end of the millennium, euphoria had gotten replaced by a general anxiety and sense of vulnerability.

Since the 1991, Computers at Risk Study from the National Research Council (National Research Council, 1991) and various others (Office of Technology Assessment,

1990; General Accounting Office, 1996) have warned that computers are insecure (see chap. 4.4.1 Background: Growing Awareness of Computer Insecurity (1967 - 2011)). These expert opinions have been widely neglected during the Information Superhighway euphoria but became visible after the Oklahoma bombing on 19 April 1995. As a reaction to Oklahoma, President Clinton issued PDD-39 called "Policy on Counterterrorism" on 21 June 1995. President Clinton set up the Presidential Commission on Critical Infrastructure protection to identify and review the vulnerability of all critical infrastructure systems, including information and telecommunications networks. This commission uncovered a series of critical vulnerabilities and rang the alarm, which led to a *growing awareness of computer security.* The commission identified eight sectors of critical infrastructure: telecommunications, electrical power, gas and oil, banking and finance, transportation, water supply, emergency and continuity of government (President's Commission on Critical Infrastructure Protection, 1997).

Key members of this working group were outspoken cyber-realist advocates such as former Air Force expert on electronic warfare Tom Marsh, or NSA Director for information warfare Rich Wilhelm, who was the NSA White House liaison for the Clipper proposal in 1993 (Kaplan, 2016, p. chap. 3). He also became a national security advisor for Al Gore, probably because of his expertise and knowledge of NSA's digital capabilities. Previous governments dealt with critical infrastructure as well but they defined the threat-spectrum more in terms of civil accidents, natural disasters and thus physical disruption and destruction (Ackerman, Bale, & Moran, 2006, p. 35). Wilhelm argued that this understanding must be expanded to include digitals systems, i.e. computers and networks, upon which these sectors rely. Being a former information-warrior, he knew that computer networks could be penetrated by an outside force because the US was essentially doing the same (Kaplan, 2016, p. chap. 3). Wilhelm also made the case to keep the US cyber-attack capabilities top-secret, because complaining about other nation's and hacker's attempts to penetrate US networks while one does the same, certainly looks awkward. In other words, America was building in secrecy what it denounced publicly.

The President's Commission on Critical Infrastructure Protection released its report in February 1997 (President's Commission on Critical Infrastructure Protection, 1997). The commission identified the problem that in case of an emergency, no agency was formally in charge. Kaplan describes how several White House officials "were startled when more than half of its report and recommendations dealt with the vulnerability of computer networks and the urgent need for what it called 'cyber security'" (Kaplan, 2016, p. chap. 3). Although coming from the civil side of government, the report features a

rhetoric very similar to cyber-realist doctrines (see chap. 4.4.2 Ideas: Formation of the Information War Doctrine (1976-2000)). It also includes a chapter on information warfare. Take for example statements like "we must learn to negotiate a new geography, where borders are irrelevant and distances meaningless," and "cyber attacks could be combined with physical attacks, against facilities or against human targets, in an effort to paralyze or panic large segments of society, damage our capability to respond to incidents" (President's Commission on Critical Infrastructure Protection, 1997, pp. 1-18). This cyber-realist inspired military language is no coincidence because central realist advocates introduced it to the civil actors of the Commission, who of course had no idea about the state of military doctrine and technical capabilities. This shift marks the beginning politicization of cyber-realism.

On July 15, 1996, President Clinton signed the executive order 13010 – Critical Infrastructure Protection, to develop a national strategy for infrastructure protection (Ackerman et al., 2006, p. 35). It argues that:

> "Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats")" (The White House, 1996).

The narrative of the order is pretty much in line with cyber-realist thinking: dependencies on new technologies create new vulnerabilities, including to cyber-attacks. Note that the report does use military language like computer network attack or defense and introduces the word "cyber-attack". The inclusion of terrorism and cyber-threats in a presidential directive is a novelty. It is important to stress the temporal and cultural context of this order. It stands in the context of a growing awareness of computer-security issues and thus a growing perception of insecure computer systems. Pessimism began to replace optimism, a trend that accelerated with every network intrusion that was discovered by the US government. Nothing makes this clearer than what came to be known as Eligible Receiver.

On June 9th 1997, the NSA ran a military simulation called *Operation Eligible Receiver* in order to test the vulnerability of US networks in case of a foreign CNA. It simulated a cyber-attack against the emergency communications systems and military

communications networks in order to disrupt US command and control – a test of information warfare so to speak. In this simulation, an NSA red-team successfully penetrated DoD computer networks with CNA and extracted and altered data. The team only used commercially available, off-the-shelf technology for this intrusion, which is seen as key evidence for the vulnerability of governmental computer networks and the thesis that potentially everyone could launch such an attack (Bendrath, 2001). Eligible Receiver was initiated by the new director of NSA Kenneth A. Minihan. He drew this idea from a war-plan that had been created at the NSA Information Warfare Center (see chap. 4.4.3 Setting the Path: The Institutionalization of Cyber-Realism). The simulation was a success in the sense that it revealed shocking deficits in US network security. Kaplan describes the reaction by some military officials when they learned about the network intrusion:

> ""I don't trust my command-control." This was the ultimate goal of information warfare, and Eligible Receiver revealed that it was more feasible than anyone in the world of conventional warfare had imagined. […] Eligible Receiver revealed that the Defense Department was completely unprepared and defenseless for a cyber attack. The NSA Red Team had penetrated its entire network […] Everyone in the room was stunned, not least John Hamre, who had been sworn in as deputy secretary of defense at the end of July" (Kaplan, 2016, p. chap. 4).

Eligible receiver showed why cyber-attacks, information war and psychological warfare should not be seen in isolation. It showed that information dominance was fragile and could quickly turn into its opposite (Rid, 2016, p. 380). The psychological effect, the distrust in one's own computer system definitely increased the seriousness of the issue. For the Pentagon, the simulation resembled a shock, or a "wake-up call", as Healey argues (Healey & Grindal, 2013).

What made matters worse was the fact that in its direct aftermath, only four months later, a similar intrusion into DoD networks happened, but this time, it was not a simulation. The attack utilized a security vulnerability in Sun's Solaris operating system which is why the incident was called *Solar Sunrise*. Deputy Secretary of Defense John Hamre called this "opening shots of an authentic cyber-war, perhaps launched by Iraq– exactly the kind of 'electronic Pearl Harbor' that Pentagon analysis had been warning of for years" or as the fulfillment of Eligible Receiver's hypothetical threat, as he briefed President Clinton (Kaplan, 2016, p. chap. 5). Because of general geopolitical tensions, it was speculated that the culprit was either Iraq, China or Russia, which had begun their information warfare programs around the same time. In the end it turned out to be a 16 year old boy from San Francisco. However, Russia is believed to be responsible for

another hacking campaign called "*Moonlight Maze*". Over the course of the year 1998, huge quantities of sensitive military information were stolen from US military networks. At the time, it was the biggest CNE operation ever recorded, which showed for the first time what the attribution problem actually *meant*. FBI forensic experts investigated over a year, including diplomatic procedures, to find the source of the attack, which probably was a Russian intelligence agency (Rid, 2016, pp. 391-404). Due to diplomatic difficulties the issue was never really resolved. As a reaction, a Joint Task Force for Computer Network Defense (JTF-CND) was founded at the DoD. In April 2000, the Joint Task Force was given a broader mandate to include CNO, operations and hence was renamed JTF-CNO.

All of this indicates a spill-over of cyber-realist ideas from the military into the political sector. This trend continues with the 1998 the Presidential Decision Directive 63, which called for "a National Plan to protect America's critical infrastructures, especially cyber systems, from deliberate attack and disruption" (The White House, 1998a). It assigned roles and lead agencies, as well as private sector liaisons for the management of infrastructures (Ackerman et al., 2006, p. 35). In May 1998, Clinton created a National Coordinator for Critical Infrastructures and began lobbying for an increased year 2000 investment in cyber-security programs with the "protecting cyber-security" initiative. There, the White House:

> "Proposed a Fiscal Year 2001 budget which allocates $2.01 billion to defend against this emerging threat, up by over $250 million from the actual FY 2000 budget, and double the FY 1998 budget" (The White House, 1998b).

Another instance of idea spill-over was the 1998 Kosovo conflict. US secretary of defense John Hamre called this conflict the first "cyber-war" (Bendrath, 1999). According to Kaplan, a joint group consisting of NSA and the Navy's Information Warfare Squadron fed false information to Serbian Air-defense systems, using a demon dialer technique that had been devised, but never been executed, for an operation in Haiti in 1994 (Kaplan, 2016, p. chap. 7).[119] American hackers also sent messages to enemy leaders and even made Milosevic's phone ringing (Kaplan, 2016, p. chap. 7).

Kosovo was the first instance of *politicization of hacking* because different international hacking groups engaged in low-impact CNA against Serbian and NATO-websites. Most of the attacks were "distributed denial of service" (DDoS) attacks that

[119] The aim was to disrupt Haitian Air-defense, which was connected to the telephone system. By utilizing a well-known known technique called Demon Dialing, made famous by the hacker Captain Zap in the early 1980s, communications of the radar could be disrupted by flooding the phone network with fake calls – a crude version of a distributed denial of service attack (Kaplan, 2016, p. chap. 4). The mission was called off but the attack-plan was kept.

simply disrupted websites. There were also several incidents of *web-site defacement* – taking control of a website to smear it by posting propaganda. These so-called cyber-attacks had more the character of digital sit-ins and did not alter the course of war, they just changed its medial representation (Bendrath, 1999). Stil, Kosovo set the path for conflicts to come. Russia and China were certainly watching and taking notes on how to utilize IW and cyber-attacks as new means of warfare that ultimately led to the concept of hybrid warfare (Wirtz, 2015).

In October 1999, the USSPACECOM was designated as the lead agency for CND for the DoD and, via another executive order, a National Infrastructure Assurance Council was created. In 2000, this capacity was expanded to include CNA as well. In January 2000, the first ever "National-Plan for Information Systems Protection" was published. The FY 2001 budget included an $8 million program to create the Federal Intrusion Detection System (FIDNET) to protect non-DoD federal agencies (The White House, 1998b).

After the Kosovo war, the Clinton Administration included cyber-threats into its official "National Security Strategy for a New Century". It argued that America faces threats to its critical infrastructure, for example in form of cyber-attacks, sabotage by terrorists or hostile states (The White House, 1999, p. 2). Cyber-threats rank second place following regional or state-centered threats. The wording resembled the standard narrative of the cyber-realist paradigm or the cyber-revolution thesis (Lindsay, 2013, p. 370). Proposals included closer collaboration between law enforcement and the creation of an intrusion detection system. This official strategy is key evidence for the argument that cyber-realism spilled over from a military doctrine into the overall national security strategy of the US.

Let’s sum up. The turn to critical infrastructure protection was a turn to cyber-realism that increasingly replaced the utopian perception of the Internet during the late Clinton administration. This represents an instance of political learning. This process initiated a path-trajectory that led to the creation of the Department of Homeland Security under the Bush administration, which subsumes cyber-security and the protection of governmental networks under one authority. At the same time, it must be stated that these operations that have been called the "first cyber-war" – Eligible Receiver, Solar Sunrise, Moonlight Maze, the NATO operation in Kosovo – were classified for a long time. Only political elites such as the Secretary of Defense and military circles knew about these. But one particular incident introduced cyber-realist arguments and frames to a wider general public: the Y2K or "millennium bug" discourse, which is the topic of the next chapter.

4.4.5 Discourse: Y2K and Critical Infrastructure Failure

The Y2K-panic of the late 1990s is an interesting juncture in the history of cyber-security because it introduced key realist arguments into the public discourse and led to growing pessimism about the digital revolution.

For reasons of cost-effectiveness, early computer programmers used a shortcut for the date in their computer applications: 1964 became 64. In the past, computer storage was expensive so this shortcut actually saved storage capacity and thus money (The United States Senate Special Committee on the Year 2000 Technology Problem, 1999, p. 7). Since around 1984, computer experts speculated that this might create issues once the year turns to 2000, which the computer would interpret as 00. It was not regarded as a problem because no-one expected that in this fast moving software business, code would be used for longer than a few years (Computerworld, 2000). This "millennium bug" turned into a potential problem at the moment when large systems became internetworked and mutually dependent. It was a problem of path-dependency, an uncorrected mistake made in the past and causing future troubles. Around 1996, some firms began to report anomalies in their applications when the date turned to 00, which some applications misinterpreted as being 1900. This was particularly an issue for corporations with long-term processes, such banks calculating interest rates.

The President’s commission on critical infrastructure recognized the problem when doing a thorough analysis of US IT-systems (The United States Senate Special Committee on the Year 2000 Technology Problem, 1999, p. 12). This institutional embeddedness set the frame for the discourse: Y2K was framed as a matter of critical infrastructure vulnerability and thus fell in the domain of cyber-realist advocates.

It is nearly impossible to collect all the predictions of what consequences the millennium-bug would have before 2000, so I focus my short analysis on an interesting Retro Report by the New York Times in 2013 called "Y2K Bug: Much ado about nothing?". This report gives a short overview over different predictions made by IT-experts and cyber-realists. Voices range from "nothing or little will happen", to "the Y2K bug will be an international disaster", "threaten nearly every aspect of modern life", "could cripple the nation" because a potential "failure of Uncle Sam’s computers would be chaos". Planes were said to be falling from the sky, nuclear power plants could meltdown or the nuclear stockpile could be launched by accident. A Senate estimate circulated through the media where it was claimed that "40% of the country could be hit by power failures on New Year’s 2000" (The New York Times, 2013). A cover of Time Magazine in January 1999 was titled "The End of the World!?! Y2K insanity! Apocalypse Now! Will computers melt

down? Will society? A guide to MILLENNIUM MADNESS" (TIME Magazine, 1999). Even policy-makers chimed into the crippling-blow narrative that is pretty similar to the cyber-war narrative. United States Deputy Secretary John Hamre, who in the past repeatedly warned about the immediate crippling blow to American infrastructure by cyber-attacks, dubbed the Y2K problem as "the electronic equivalent of the El Niño and there will be nasty surprises around the globe" (CNN, 2006). Senator Dodd is quoted in the official report with a statement pretty much in line with the cyber-war narrative: "the question is not will there be disruptions, but how severe the disruptions will be" (The United States Senate Special Committee on the Year 2000 Technology Problem, 1999, p. 12).

The general narrative should have become clear. It is striking that the Y2K bug is deeply inspired by the discourse on critical infrastructure protection and features narratives developed within the context of the IW doctrine. Especially, the core problem-definition of *interconnectedness* stands out. Because everything is interconnected by the Internet, potentially everything could come to an end. To assess the impact of Y2K, the Senate set up a special committee "Investigating the Impact of the Year 2000 Problem". The official report released in March 1999 describes the problem as follows:

> "Y2K is about more than the failure of an individual's personal computer or an incorrect date in a spreadsheet. As one examines the multiple layers of systems and technologies that support our everyday lives, the potential Y2K problems increase exponentially. The interdependent nature of technology systems makes the severity of possible disruptions difficult to predict" (The United States Senate Special Committee on the Year 2000 Technology Problem, 1999, p. 1).

The problem described here is remarkably similar to the *crippling-blow* and *cascading-effect* thesis of the cyber-war narrative developed within the IW-doctrine (see chap. 4.4.2.2 Problem Definitions of Cyber-Realism), the interconnectedness of computer-systems in networks and the potential of a cascading effect. Because these systems are mutually interdependent, no one knows what happens if a few of them produce an error. Even the threat representations are similar: shutdown of the power grid, nuclear meltdown, loss of life and potential failure due to computer blackouts.

But there is more spill-over from the cyber-war narrative. The report states: "hackers and other criminals might see Y2K as a prime opportunity to attack pieces of our infrastructure. Or they might use Y2K-induced infrastructure failures as cover for theft, arson, bombings" (The United States Senate Special Committee on the Year 2000 Technology Problem, 1999, p. 12). The difference between Y2K and the cyber-war

discourse is the global reach of the issue. Best argues that Y2K shows the potential weakness of a globalized, interconnected world order and is thus seen as the first crisis of globalization: "We have never gone through a global event like this in which all the world is affected by one thing at the same time, something that has the potential to disrupt commerce" (Best, 2003). In other words, the crippling-blow and cascading effect thesis is not just limited to US territory, as in the cyber-war narrative, but is predicted to be global. At the same time, Y2k presented an anomaly for utopianism since the potential for catastrophic failure due to the connectedness of systems was not expected by this paradigm. Cyber-realism predicted a possible Y2k outcome while utopianism was blind to that.

To provide leadership and to counter the media-frenzy, President Clinton appointed the Deputy Budget Director John Koskinen to be to chair the "Year 2000 Conversion Council" guiding the governmental efforts to make a secure transition to the year 2000. According to Koskinen, his job description given by the President was "do not let the world end" (The New York Times, 2013). A $50 million Y2K coordination center was created, involving government and private industry like Microsoft (The Washington Post, 2003). Microsoft released Windows 98 Special Edition, including a fix for the Y2K bug and computer manufactures sold Y2K-proof certified systems. In sum, the entire US spent an enormous amount of money, roughly $100 billion, on Y2K fixes in software and hardware (Reuters, 2000). Roughly $9 billion came from the Federal Government. Global spending is estimated between $300 and $500 billion (Manjoo, 2009). While some argue that this was government overspending, the general consensus seems to be that it was money well spent and that this effort prevented a major incident. It also helped to reduce public anxieties over the severeness of the Y2K issue, as a Gallup Poll from 1999 showed: "the number of Americans who think Y2K-related computer mistakes around the world will cause "major problems" dropped to 21%, down from 34% in December [1998]" (Saad, 1999).

The Y2K scare is interesting because it received so much public and media attention, although little actually happened. No planes crashed and the world did not end. There were only minor disruptions and probably more people died of firework injuries on New Years Eve 2000. The Y2K scare coincided with a general "end of the world fear" around the new millennium and therefore made the issue of cyber-security more tangible for a large audience. It revealed

> "a sense of urgency and a fear of loss of control over the state of affairs in the world. Y2K was a revelatory eye-opener about the fragility of the digital economy and the world in general. It was the definite negation of the promises of ICT and cyber-utopianism and a reminder that technology could break loose and turn on its creators, and thus possibly have unforeseen negative consequences for society" (Pärna, 2010, p. 152).

The problem of network-interconnectivity and dependence on these systems that military and intelligence experts had warned about in secrecy of the National Security Council, suddenly became common knowledge.

4.4.6 Preliminary Summary

Since this is the longest chapter in this thesis, I decided to split the description of the causal mechanism into two-parts. The second part is presented in the final summary (see chap. 4.4.10 Summary).

First, the *technological mass diffusion of both the personal computer in the 1980s and the Internet* in the 1990s led to a greater interconnectivity of military and civil computer systems (part 1). With this technical diffusion, the number of actors experimenting with hacking and computer network intrusions (deviant use of technology) increased. The result of this was an *increase of computer security incidents*, both in quantity and quality. The more computers spread, the more incidents happened which ultimately raised awareness of the issue of computer insecurity (necessary condition). The bigger the perceived incident, the stronger the political response was.

The most prominent trigger in the early days were the 1983 War Games revelation and the Morris Worm of 1989 that shut down large portions of ARPANET and thus affected military command and control. This led to *the slow growing political perception and problem recognition* (part 2). Actors with the greatest know-how of computer and technical matters, i.e. the intelligence and engineering community, realized the problem first. Technological literacy is a key explanation in the entire history of cyber-security. Network intrusions presented themselves as a problem that no-one had thought about before, which means that no existing standard operating procedures within the bureaucracy existed. However, the problem was not necessarily perceived to be urgent in the mid 1980s because there was no other country technologically as advanced as the US. The issue was dealt with in secrecy. Only a hand full of actors knew about this issue in political circles at the time.

The *salience of the topic inside military circles increased with the Gulf War* that showed military planners the importance of computers and superior information about the

battlefield (part 3). This trigger led to an initial euphoria about the possibilities of new information technologies and the expected revolution in military affairs it could bring. This process can be described as *sense-making or soul-searching process,* which marks the beginning of the construction of a coherent paradigm as a general roadmap to make sense of the emerging Internet. National security actors began to research the issue and turned to the existing literature on the matter, for example the work of Rona (Rona, 1976) or Rechtin (Rechtin, 1983). What followed was the *development of the military doctrine of information war*. To make sense of the Internet and computer security, advocates established a set of technological frames or sense-making devices that helped them to understand the issue from a national security perspective. New ideas regarding the nature of these new information technologies were developed (for example the concept of information weapons) or partly picked up from cyber-utopian media discourses (the concept of cyberspace as a distinct space). Military actors began to understand cyberspace as a chaotic, borderless, anonymous and potentially anarchic medium that was lacking state control and order. The Internet began to be seen as a challenge to national security with predominantly negative attributes. The decentralized logic of TCP/IP, as well as the security and control issues it introduced became the core problem definition of cyber-realism. These stayed the same the entire time, even until today. What we see here is a coherent problem definition within this process of paradigm or doctrine-building. In contrast to the other paradigms, realism is the most problem-driven.

The answer to these perceived problems was the *state-centric norm that the military and intelligence community should exert control over this new medium cyberspace*, particularly in terms of information dominance and being able to disrupt and exploit information flows of other countries, even in times of peace (part 4). Institutions were set up to fulfill this function. This lead to the realization of a classical security-dilemma: while the IC developed computer network attack capabilities, it realized that others could potentially do the same to the US. Other countries in turn began to mimic US practices.

The *institutionalization of information warfare in military organizations* was a crucial causal factor for the success of the paradigm (part 5). According to Kuhn, paradigms have to be carried by actors that are socialized into this belief system. Military training and Information Warfare centers served the function to educate the next generation of paradigm holders which entered political offices during the Bush and Obama administration. The continuity of personnel, for example in the case of former NSA director Mike McConnell (1992-1996), who later served as Director of National Intelligence, pushing pretty much for a similar agenda, is a key explanation for the

persistence of cyber-realist ideas. This created a relatively steady and stable path trajectory and permanence that cyber-utopianism was lacking. This is particularly the case during the turn to critical infrastructures in the second Clinton administration, when many trained information warriors were placed into the presidential commission on critical infrastructures. In these positions, cyber-realist advocates acted as norm-entrepreneurs, diffusing their ideas to a non-military political audience.

In terms of the advocacy coalition framework, *cyber-realists got access to political power to spread their message* to political elites. The salience of their ideas increased with the terrorist attacks of the mid 1990s while the Eligible Receiver Simulation uncovered the vulnerability of large portions of US command and control systems, followed directly by the Moonlight Maze intrusion. The rapid succession and perceived severeness of these issues further increased the salience of cyber-realist ideas. These events led to the *spillover of the military concept of information war into the political sphere* (part 6). Ideas, discursive frames and norms developed, in secrecy, within the military concept of IW appeared in the political discourse on critical infrastructure. Particularly the cyber-realist narrative of a crippling blow that could cascade through the network and shut down the entire US economy (or the power grid) had a certain narrative fidelity that became obvious during the Y2K Panic at the end of the 1990s. In other words, ideas, norms and frames that were first developed within the military doctrine of information war now suddenly featured prominently in non-military policy documents.

The Y2K panic (a shock in theoretical terms) *elevated cyber-realist lines of thought and frames into the public discourse and decreased the salience of cyber-utopianism* (while not dismantling it completely). This is in line with the theory (see chap. 2.2.4 Explaining Change). Compared to the utopian paradigm, the explanatory power of cyber-realism was greater. For utopianism, Y2K presented an anomaly (or a blind spot) that was not conceived within the optimist narrative of a better technological future. Cyber-realism simply had the better explanation for what was going on because the Y2K bug had fit perfectly into its narrative of critical vulnerability and dependency of digital infrastructures. In other words, Y2K was a commensurable manifestation of the problem that cyber-realist had been warning about all along. This crippling-blow narrative had a high degree of fidelity, was shared by many civilian and military experts and was even actively promoted by President Clinton. This increased the external credibility of cyber-realism in front of the general public. For first time, it presented itself as a viable alternative to utopianism that was still dominant during the mid of the 1990s. This also has to do with the fact the that military doctrine of IW was in the public domain. Y2K was the

first instance where the utopian narrative got contested and lost some of its salience. The second major disruption was the burst of the dot-com bubble that again presented itself as a phenomenon that was not perceived by utopians.

Table 5. Causal Mechanism of early Information War

Context	Growing computer security instances during the 1980s.
Part 1	Technological mass diffusion of both the personal computer in the 1980s and the Internet in the 1990s lead to a *greater interconnectivity of military and civil computer systems.* Deviant use by hackers creates security problems.
Part 2	War Games as trigger. Intelligence Community begins to *recognize* the problem of vulnerable computer systems during the 1980s, but attributes no urgency.
Part 3	Increased *salience* of technology, information and computer insecurity for conduct of war in the context of Gulf War. Military begins sense-making and *drafting* a new doctrine utilizing information technology.
Part 4	Cyber-realists *develop* a negative perception of cyberspace that is driven by problems that derive from shortcomings in TCP/IP and their concern for national security. They *develop* the norm that it is their appropriate role to exercise control in cyberspace (norm emergence) in order to wage information war.
Part 5	Institutionalization of cyber-realist lines of thought in new information warfare institutions leads to a socialization of a new generation of paradigm holders and a persistence of ideas.
Part 6	Cyber-realist advocates *diffuse* their ideas regarding critical infrastructure protection and the Kosovo War among political elites.
Outcome	Y2k Panic leads to a spillover of cyber-realist ideas and norms into the public discourse and helps to disenchant the cyber-utopian narrative.

The table summarizes the findings of the causal process that unfolded during the late 1980s and 1990s. However, this marked only the beginning of the growing dominance of cyber-realism. The paradigm was by no means dominant yet. The Bush administration picked up the path that had been laid out before and systematically began to fuse cyber-realism with counter-terrorism, giving it a new direction and accelerating its development. This will be the topic of the next chapter.

4.4.7 The Politicization of Cyber-Realism with the War on Terror (2000 - 2008)

This chapter analyzes how the military cyber-realist paradigms got further transferred into the political domain (politicized) and how it could become dominant within the Bush administration. The weeks after the tragic terrorist attacks of 9/11 present a critical juncture where multiple causal pathways come together (equifinality) and form a coherent trajectory. This and the following chapters describe the broad changes in terms of ideas, norms, strategies, policies and technology that were set in motion only within a few weeks after the attacks. Since this is a complex matter, I subdivided the chapters thematically to deal with conceptually different topics like policies or technologies. The reader has to keep in mind that these different chapters cover more or less the same time period.

In January 2001, the newly elected republican administration of George Walker Bush entered the oval office and with it a whole bunch of strong advocates of RMA and information warfare. Bush himself affirmed the RMA concept in his first speech on foreign policy (Kellner, 2002, p. 1). Other advocates were Secretary of Defense Donald Henry Rumsfeld, his deputy Paul Wolfowitz, as well as Vice President Richard "Dick" Cheney. The idea of RMA, information warfare and particularly cyberspace control is one of the key concepts within the neoconservative (neocon) agenda. In 1997, Project for the New American Century (PNAC), a neoconservative think-tank, which advocated RMA-thinking was formed. Many PNAC members later occupied positions in the Bush administration (especially in the field of national security).[120] Three months before Bush took office, the think tank released an influential paper, outlining neoconservative military reform (Kagan et al., 2000). The goals were to achieve a "pax Americana", a peace based on global US dominance and supremacy. Three technological instruments are key for this: global missile defense, the control of cyberspace and the exploitation of the RMA (ICT & precision strike technology such as drones). Neoconservatives argued that control of cyberspace, "the new international commons", is "a key to world power in the future" (Kagan et al., 2000, p. 51). Offensive capabilities (to disrupt or paralyze the military or the commercial sector's computer networks), would be an invaluable source for power to maintain US supremacy (ibid). In general, neoconservative thinking outlined in this paper is basically identical with the cyber-realist paradigm outlined in military documents that were analyzed in previous chapters.

Other core ideas and principled beliefs were first, the norm of military omnipotence and power (Griffin, 2007) and the perceived appropriateness to use it as a main instrument

[120] Among them Elliott Abrams, John Bolton, Eliot Cohen, Paula Dobriansky, Zalmay Khalilzad, Richard Perle, Peter W. Rodman, James Woolsey, and—most significantly—Cheney, Libby, Rumsfeld, and Wolfowitz, became central members of the new Bush administration (Kagan, Schmitt, & Donnelly, 2000).

of international affairs (including new forms of IW). Second, the perceived appropriateness of unilateral action and a distrust in international organizations such as the UN (Ikenberry, 2007) based on the idea of American exceptionalism and concepts of benign hegemony (Monten, 2005). Third, the idea of pre-emptive war, "to confront the worst threats before they emerge" (Bush, 2002) that became, for the first time ever, part of the official *National Security Strategy* (2002). The belief that it is possible to deterministically predict how a chain of events will play out and be able to intervene with correct measures before it manifests itself, is one of the key driving forces of Internet control and mass surveillance or what neoconservative agenda calls "21st century surveillance" (Halper & Clarke, 2004, p. 273). Neoconservatism can be seen as the conduit that brought military concepts into the political domain.

The early Bush security policy, outlined in his election campaign, was relatively moderate, arguing for a "humble foreign policy" (Onea, 2013, p. 121) and was not particularly predisposed towards neoconservatism and cyber-realism. Bush was not that much interested in the Internet either. He is described by observers as technologically ignorant. Bush himself said that he used "the Google" only occasionally (CNBC, 2006). It was Dick Cheney, David Addington and CIA Director George Tenet who turned Bush towards Internet surveillance. They used the window of opportunity to present the neoconservative ideas as the appropriate response to the terror attacks. They framed neocon ideas and policies as solution strategy to the 9/11 shock, which is in line with theory (see chap. 2.2.4 Explaining Change). Internet control, espionage and surveillance programs had been in development before 9/11 and were taken out of the drawer and reformulated as an appropriate 9/11 response strategy (Buckley & Singh, 2006). Observers close to the President (Clarke, 2004, p. 243) confirm that both Cheney and Rumsfeld exerted a great deal of influence on the (inexperienced) President. This changed with Bush's second term, but during the crisis days after 9/11 the national security decision-making process was dominated by neoconservative voices (Renshon, 2009, p. 63). Bush gave broad orders what had to be done, but had no interest in the details (Starr-Deelen, 2014, p. 110). This gave his close advisory circle more influence to shape policy. The hawks repeatedly sidestepped the moderate forces, namely National Security Advisor Condoleezza Rice and Secretary of State Colin Powell (Risen, 2006, p. chap. 3).

Richard Cheney transformed the representative function of the Vice President into an effective Co-President. No other Vice President in history had as much influence (Onea, 2013, p. 106) and indeed, many of the controversial post 9/11 responses, like the NSA mass surveillance program, can be traced back to him. Cheney is described by colleagues

as "the most radical conservative" (Clarke, 2004, p. 19). He served in the government during the Watergate scandal (where illegal domestic surveillance played a role). Since then, he was an advocate for a strong executive, working in secrecy, unchecked by other branches of government. He was also a proponent of mass surveillance. He repeatedly stressed that the limits that were put onto US domestic intelligence gathering with the Foreign Intelligence Surveillance Act (FISA) of 1978 led to an "erosion of Presidential power and authority" (Cheney inMiller, 2008, p. xvi). Since 1978, FISA had to authorize domestic surveillance. Before 9/11, FISA rejected more domestic surveillance requests of the Bush administration than it had during the four administrations before. This just increased Cheney's negative attitude towards legal checks & balances (Bamford, 2009, p. 113). To cut back FISA was one of his and David Addingtons personal goals. Addington said before 9/11: "We're one bomb away from getting rid of that obnoxious [FISA] court" (Addington inBamford, 2009, p. 112). The two are said to be the chief designers of the idea "that the President, as Commander-in-Chief, has the authority to disregard virtually all previously known legal boundaries, if national security demands it" (Mayer, 2006). This controversial legal paradigm, called *unitary executive theory*, served as the legal framework for many controversial programs that were often legitimized by secret Presidential directives.

Among these are the CIA extraordinary rendition program "Greystone" (Risen, 2006, p. Chap. 1), the reclassification of terrorists as "illegal enemy combatants" (Ralph, 2013, pp. 2-3) and the CIA "enhanced interrogation" practices like water boarding in secret prisons all around the world (Sanders, 2012). The NSA's domestic surveillance program was also legitimized with this interpretation of the law, but more about that later (see chap. 4.4.7.3 Artifacts: NSA and the Full-take Norm of Internet Control (2001 -)). The noteworthy point here is that all these programs were established within a few weeks after 9/11, without any public discourse or opposition from Congress. The composition of the close circle of decision-makers in the White House (sometimes called the War Council) and group-think phenomena are a key explanatory factor for the post 9/11 dominance of cyber-realism (Badie, 2010). Besides Addington and US White House Counsel Alberto Gonzales (also a strong advocate of the Bush policy), no-one had a legal or even law enforcement background, which is rather unusual in the US political system (Mayer, 2006).

This explains the declaration of a global *war* on terrorism (GWOT) only a few days after the attacks (Starr-Deelen, 2014, p. 125). This is a result of the neoconservative norm that war is a legitimate/appropriate instrument of statecraft (Halper & Clarke, 2004, p.

281). Whereas the Bush Senior and Clinton administration responded to the terror attacks of the 1990s with a "law-enforcement paradigm" (Starr-Deelen, 2014, p. 88), members of the Bush administration favored a war-paradigm. Why? Because war could be used to legitimize the use of all available means and granted the President executive powers as commander-in-chief (called Article II powers), thereby enabling the key neoconservative ideas such as the idea of a unitary executive. A state of emergency (Ralph, 2013) could serve to "justify classifying everything associated with fighting it" (Priest & Arkin, 2012, p. chap. 1), like targeted killing of terrorist suspects and domestic mass surveillance. Key evidence for this is a memorandum written by John Yoo, one of the Department of Justice (DoJ) top lawyers that legalized the NSA warrantless Internet surveillance, arguing that such intrusive measures are *now* justified because of the attacks and that the Fourth Amendment had no application for military operations, even in the homeland (Bamford, 2009, p. 116). A leaked letter from Yoo to judge Kollar-Kotelly indicates that Yoo was aware that domestic Internet surveillance was illegal, but tried to convince the judge anyway, arguing that national security is the higher good compared to the constitution (Humpenöder, 2016).

In sum, the shock that was 9/11 and neoconservative norm-entrepreneurs within the administration lifted the former military cyber-realist paradigm and the norm of control into the executive. Controlling the Internet was presented as a solution to the terror attacks. The following chapters will analyze the socio-technological system that was put into place to enable control over vast portions of the Internet traffic. This system has three dimensions: First, the strategic side, explaining how to fight terrorism, second the legal side that enabled extraordinary measures and third, the technological response in forms of actual technical systems (NSA surveillance program and the DARPA's Total Information Awareness program) which perfectly illustrates the workings of cyber-realism. The next chapter introduces new ideas and the evolution of cyber-realist thought within the context of the war on terror that ultimately led to the fusion of information war and surveillance.

4.4.7.1 Ideas: Cyber-Realism and Counter-Terrorism (2001 - 2007)

This chapter analyzes the impact of 9/11 and counter-terrorism policy on cyber-realism. It argues that elements of the new counter-terrorist policy (Starr-Deelen, 2014, p. 103) got fused together with the cyber-realism. "Laws and policies in the area of cybersecurity are combining and interacting with those in the antiterror realm" (Deibert, 2015, p. 77). This gave cyber-realism a new direction. For this analysis, major US strategic documents, counter-terrorist policy, are analyzed for content relating to the Internet (see appendix

Cyber-Realism Corpus). It will summarize the main ideas and shifts that came after 9/11. This chapter will focus on problem definitions that are developed within these strategy papers, whereas the following chapters will look at legal, technical and institutional solutions to these problems.

The core problem that was diagnosed quickly after the attacks and that shaped most of the US response, even to the present day, is the simple realization that terrorists were able to live in America, hidden within the general population (The White House, 2001a). The enemy "lurks in the shadows" (Office of Homeland Security, 2002, p. vii) and is "invisible against the backdrop" of an open society (Office of Homeland Security, 2002, p. 15). The problem is that an open society "presents an almost infinite array of potential targets" that can be attacked with various methods. The identity, intention and location of the enemy are unknown, in contrast to nation-state threats.[121] Additionally, the attackers are framed as a new kind of enemy, "a challenge as formidable as any ever faced by our nation" (Office of Homeland Security, 2002, p. vii).

From the beginning, the connection between terrorism and technology is drawn. According to Bendrath, this started before 9/11 (Bendrath, 2003) and has to do with the network-character of terrorism (The White House, 2002, p. 1). Like computer networks, Al-Qaeda is said to resemble "loosely interconnected, semi-independent cells that have no single commanding hierarchy" forming a "network of networks" (Jackson, 2005, p. 410). Signifiers from the engineering and utopian paradigm are used to describe the enemy which connects computer-science terms with terrorism, thereby changing meaning (Nissenbaum, 2005). There is an interesting oxymoron here. Although Islamic terrorists are generally framed as barbaric, inhuman and uncivilized (Tsoukala, 2008), they are described as technologically potent, using satellite communication and the World Wide Web for recruiting and information war (spread of propaganda). Arquilla and Ronfeldt, some of the initial proponents of the term cyber-war, argue that terrorists could use the Internet to launch a net-war (Arquilla & Ronfeldt, 2001). The cyber- and information war threats become systematically connected to the counter-terrorism discourse.

On the 9th October 2001, the Department of Homeland Security (DHS) is created and new "*Counterterrorism and Cyberspace security positions"* are announced. Richard Clarke becomes the President's Special Advisor for Cyber-security ("cyber-czar"). He highlighted that the future security of the US depends on cyberspace: "America has built

[121] This changed the intelligence requirements, as one analyst explains: "If you're talking Russia, Humint is really important. If you're talking about al-Qaeda, Humint ought to be important, but Sigint turns out to be more important" (Haseltine inBamford, 2009, p. 143). Humint refers to human intelligence, contacts and spies.

cyberspace and America must now defend its cyberspace" (The White House, 2001b). In his first speech, he presents most of the elements of the cyber-war narrative that have been shown before. These positions then become gradually implemented into national security policy (The White House, 2003). For example, "the gravest danger our nation faces lies at the crossroads of radicalism and technology" (Office of Homeland Security, 2002, p. 2). Initially, the focus was on nuclear proliferation, but over time it shifts to cyberspace issues: terrorists "exploit information technology and the Internet to plan attacks, raise funds, spread propaganda, collect information and communicate securely" (Office of Homeland Security, 2002, p. 7). Sooner or later they might start cyber-terrorism to "cause widespread disruption and damage, including casualties" (Office of Homeland Security, 2002, p. 7). In 2006, a new *National Strategy for Combating Terrorism* introduces the term *cyber safe havens*, which frames the Internet as an:

> "Anonymous, geographically unbounded and largely unregulated virtual haven for terrorists. Our enemies use the Internet to develop and disseminate propaganda, recruit new members, raise and transfer funds, train members on weapons use and tactics to plan operations" (The White House, 2006, p. 17).

The similarity to the description of the Internet in the information warfare doctrine is striking (see chap. 4.4.2.2 Problem Definitions of Cyber-Realism). Because of the Internet core norms such as openness, decentrality and anonymity, it can be used by all kinds of actors for a variety of purposes, even terrorism and propaganda. From a counter-terrorist perspective, the Internet becomes a *problem* and a target in the war on terrorism. At the same time, it is seen as an opportunity for exploitation for example by providing counter-messages to terrorist propaganda. The official *goal* becomes to "deny the Internet to the terrorists" (The White House, 2006, p. 17).

These broad problem definitions set out the general strategic goals that are similar in most of the documents and resemble many elements introduced in the IW-doctrine. The first priority is *prevention*.

> "The United States must take every appropriate action to avoid being surprised by another terrorist attack. To secure the homeland, we must have an intelligence and warning system that is capable of detecting terrorist activity before it manifests itself in an attack so that proper preemptive, preventive, and protective action can be taken" (Office of Homeland Security, 2002, p. viii).

The national security[122] strategies show that the major themes of the counter-terrorist policy are highly compatible with and even reinforce cyber-realist ideas: First, the belief that more information could lift the fog of war and theoretically uncover or *prevent* hidden terrorist plots ("the more we know about our enemy, the better we are able to defeat that enemy" (Office of Homeland Security, 2002, p. 7)). The assumption is that the goal of prevention can be achieved with the instrument of better intelligence. The belief goes so far that even terrorist intentions should be detected, if one has enough information. Therefore, "intelligence and information has become a priority of the highest measure" (Office of Homeland Security, 2002, p. 15).

The second major theme is the *need to share, or the fusion of various sources of information* (all-source intelligence) together in databases. The database becomes the core technology of the 21st century:

> "Databases used for federal law enforcement, immigration, intelligence, public health surveillance, and emergency management have not been connected in ways that allow us to comprehend where information gaps or redundancies exist. […] To secure the homeland better, we must link the vast amounts of knowledge residing within each government agency while ensuring adequate privacy" (Office of Homeland Security, 2002, p. xi).

The idea here is to fuse intelligence databases together into one an accessible network. The issue is described by the 9/11 Commission in 2004 as the problem to *"connect the dots"* (9/11 Commission, 2004). The Homeland Security strategy outlines the general mission to integrate information sharing across the federal government, across the state and local governments as well as private industry and citizens, to develop a common meta-data standard for electronic information to homeland security (Office of Homeland Security, 2002, pp. x-xi).

These themes become more refined in the 2005 *National Intelligence Strategy* that argues that the Intelligence Community (IC) must be able to "penetrate the thinking" of leaders and therefore must make "the best use of all-source intelligence, including from open sources [such as the Internet]" (Director of National Intelligence, 2005, p. 9). Since information is a resource, it follows that it must be "*mined"* from all sources, even the Internet. This is the origin of the term data-mining. In sum, the intelligence strategy describes a paradigm change from need-to-know to *need-to-share*, removing the ownership of data by agency (Director of National Intelligence, 2005, p. 14). In a nutshell, every

[122] Starr-Deelen argues that the National Security Strategy of 2002 resembles a neoconservative key document called Defense Planning Guidance, written in 1992 by Cheney and Wolfowitz (Starr-Deelen, 2014, p. 141).

piece of collected data must be accessible by agencies with sufficient authorities. At the same time, the number of agencies with data access is dramatically expanded. The *National Strategy for Information Sharing* (2007) outlines the norm that information sharing should be the rule, not the exception. All these documents indicate the increased relevance of intelligence gathering in the war on terror, being perceived as the first line of defense (Director of National Intelligence, 2005). This of course implies the upgrading of all intelligence functions and agencies, giving them more resources and reducing legal hurdles for surveillance and espionage.

The third major theme is the *expansion of the battle space* in several dimensions: physically, spatially, digitally and temporally. The national security policy states that "the war against terrorists of global reach is a global enterprise of uncertain duration" (The White House, 2002, p. 1) and therefore it argues that the distinction between domestic and foreign affairs is diminishing. The 2007 renewed *National Strategy for Homeland Security* summarizes:

> "In order to uncover terrorists and terrorist activity against the backdrop of our highly mobile, dynamic, and diverse society, we must attain domain awareness of the actions, events, and trends that occur throughout our land, maritime, air, space, and cyber domains" (Homeland Security Council, 2007, p. 5).

The language is very much in line with IW documents of the mid 1990s and frames cyberspace as a military domain with the goal of total battle-space awareness (see chap. 4.4.2.3 Core Ideas: Information Weapons & Digital Battlespace). The Internet becomes a central battle space in the war on terrorism. The strategy papers repeatedly stress "the War on Terror is a different kind of war, which requires a paradigm shift and the application of all elements of our national power and influence" (The White House, 2007, p. 1). Especially the homeland security strategy systematically connects the cyber-war narrative (US dependency on vulnerable critical infrastructure) with the threats of terrorists and hackers. Terrorism in fact becomes the more dominant threat to cyber-security within these documents (Homeland Security Council, 2007, p. 28). But not just IW and counter-terror problem definitions become integrated, but also the solution strategies. Many of these strategy papers are inspired by cyber-realism: they are full of RMA assumptions and IW goals, for example the demands for the development of remote sensing and precision strike capabilities together with the need to conduct information operations (The White House, 2002, p. 30).

These three themes, *all-source information gathering to prevent terrorism*, the *fusion of this intelligence in accessible databases* for law-enforcement, military, intelligence and

the private sector and *the expansion of the battle space in the global war on terror* are repeated and refined in various documents throughout the Bush administration. These general ideational components extend the cyber-realist paradigm: they introduce new enemies (hidden terror cells), a new battle space (the domestic homeland and global cyberspace), and legitimize the use of all sources of national power, like surveillance or other military-grade technologies domestically, digitally and preemptively. Counter-terrorism becomes the dominant frame for understanding the Internet, thus shaping the meaning of the technology itself. This is a fundamental shift: whereas the older IW doctrine was clearly outward-facing, to target enemy *states*, the new strategy is also inwards-facing, looking for individual enemies within the homeland. In sum, these documents reinforce the norm of Internet control: it is appropriate for states to use all available means to fight terrorism. This norm inspires many policies, such as the Patriot Act and the NSA warrantless Internet surveillance program. The following chapters will analyze the effects produced by this new cyber-realist paradigm in terms of technological artifacts and policies.

4.4.7.2 Policy: The Patriot Act and Intelligence Reform (2001 - 2004)

The theory assumes that paradigms influence policy and technological design. In other words, they can change socio-technical systems. One part of this change is legal, the other technological. This chapter focuses on the legal paradigm-change that happened with 9/11 and that lay the legal groundwork for expanded Internet control. Cyber-realist ideas of Internet control became embedded in policy.

To understand the scale and size of the paradigm change that took place after 9/11, it is necessary to provide a bit of background. In the 1970s it was revealed with the Pike and Church Committees that NSA, FBI and CIA, ordered by Presidents, repeatedly engaged in warrantless domestic surveillance of American citizens. Thousands of Americans, who are protected by the constitution from such practices, were monitored and profiled.[123] The Foreign Intelligence Surveillance Act (FISA) of 1978 was a bipartisan reaction to prevent that Presidents could order the secret surveillance of citizens without court or congressional approval (Lerner, 2003, p. 496). FISA was intentionally designed to deter a rogue executive from bypassing legal checks and balances. The aim was to prevent the

[123] For example under Operation SHAMROCK, the executive forced telecommunications carriers to cooperate with NSA to allow access to continental telegraph and telephone cables. The NSA was potentially wiretapping most incoming and outgoing traffic to Europe and the Pacific region. FBI's COINTELPRO program was designed to infiltrate civil rights and anti-war movement groups and to discredit their leaders (Martin Luther King) and to spread dissent (Schwarz, 2008).

fusion of intelligence and law enforcement in an almighty secret police like the "Gestapo" or "KGB" (Turner, 2004, p. 52).

Therefore, it created a logical separation between foreign intelligence collection done by CIA and NSA and domestic law enforcement (FBI). Because law-enforcement intelligence should be usable in the court of law, a domestic surveillance warrant required higher legal standards. For example, an FBI warrant application had to include probable cause,[124] the nature of information sought had to be described and it had to be certified that the information could not be obtained by other means. FISA, de jure, did not prohibit domestic surveillance by outward-facing intelligence agencies, but established a regime of court oversight to prohibit abuse of powers. If NSA wanted to monitor a foreign suspect inside America, it needed a warrant from the FISA court (FISC). Warrantless domestic surveillance of US citizens protected by the 4th amendment was illegal under this regime (Seamon, 2008, pp. 130-132). FISC warrant applications just needed to show that the target is somehow connected to criminal activity and that useful intelligence will be the result of surveillance. Compared to crime investigations, FISC warrants have a much lower standard which is the prime reason why evidence obtained under a FISC warrant should not be used in the court of law. Also, FISC warrants and procedures are normally classified (Landau, 2013, p. 55). FISA also granted an attorney the authority to authorize *pen registers*, trap and trace devices that collect caller-IDs of phone calls (Donohue, 2008, pp. 229-233). However, FISA initially did not grant the executive the right to obtain business records (such as customer records or data stored on company servers), which was changed after the Oklahoma bombing.

FISA, de facto, ended NSA's domestic surveillance and since then the FBI became the primary agency under this legal regime (Risen, 2006, p. chap. 2). Between 1978 and 1995, FISC granted around 500 warrant applications per year, with the number growing slowly until 9/11, when it doubled. Out of 16,450 applications between 1978 and 2003, FISC denied only 3 (Donohue, 2008, p. 232). FISC supporters see this as evidence for the high legal standards of the FISA warrant-applications, whereas critics argue that FISC is not independent and just a "rubber-stamp" (Lerner, 2003, p. 498). For some neoconservatives and the intelligence community, FISA was "an impediment for intelligence gathering and presidential authority" (Cheney inMiller, 2008, p. xvi). After 9/11, the neocon reading became dominant and increased pressure for reform.

[124] Probable cause "exist[s] where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found" (Congressional Digest, 2016).

The most significant changes to the legal regime came with the PATRIOT Act that passed Congress on 25 October 2001 (with 98 to 1 votes). Even the Democrats jumped the 9/11 bandwagon without many questions. Observers describe the bill as a paradigm change, it abandoned the *law enforcement paradigm to terrorism* (of the Clinton and Bush Senior administration) and substituted it with "an intelligence [or military/war] paradigm that seeks to secretly gather all information that might turn out to be useful" (Podesta, 2002). With it came a norm change – the norm of the separation of law enforcement and intelligence agencies was discarded (Turner, 2004, p. 53). This agenda was driven by the principled beliefs outlined in the previous chapters: first, the idea "to prevent another 9/11" and second, to do so without restrictions to the unitary executive, which should use *all* available means, unbound by legal or congressional restraints. The Patriot Act included many high-detail items that had been on the neoconservative and intelligence community wish-list before 9/11, for example lower FISA standards and more executive powers (Rovner & Long, 2005, p. 617). The following sections are of particular relevance for Internet control.

Section 218[125] and 203[126] effectively dismantled the wall between foreign intelligence agencies such as the CIA or NSA and domestic law enforcement such as the FBI, thereby sweeping away 30 years of fundamental FISA norms (Donohue, 2008, p. 234). The FISA process (with its lower standards) could now be used for domestic intelligence more easily. These lower standards of FISA warrants are part of the reason why since 2002, "the Department of Justice requested more wiretaps under FISA than under ordinary wiretap statutes – a circumstance suggesting a significant shift in the government's strategy for gathering information" (Donohue, 2008, p. 232).

Section 206 expanded the concept of a "roaming wiretap". Not a device, but a person itself is wiretapped, meaning that the warrant roams between different devices (phones, computers, Fax). The act removed the legal requirement that the target had to actually use the device. This means that all public phones or routers in a neighborhood could theoretically be tapped into just based on a suspicion (Podesta, 2002). It also authorizes the "the installation of devices to record all computer routing, addressing, and signaling information" (Podesta, 2002). This theoretically legalizes wiretapping into the routing infrastructure of the Internet. This is noteworthy because it seems to be designed to counter-appropriate the effects produced by dynamic routing within the TCP/IP protocol

[125] Section 218 reduced requirements for a warrant from previously demanding that *the* (primary) purpose of the investigation was to obtain foreign intelligence, whereas in the new version it was reduced to "*a* significant purpose", but there could be others (Lerner, 2003, p. 505).
[126] The key idea in Section 203 is that foreign intelligence (which is defined quite broadly) gathered during criminal investigations (court evidence) can be shared with the intelligence community.

(see chap. 4.1.2.1 Ideas). Section 216 mandates Internet service providers to maintain logs of a target's Internet-surfing and E-mailing behavior like the IP addresses of external hosts a computer connects to (so-called Internet metadata) and this data must be shared with law enforcement *and* the IC. Metadata plays a huge role in the NSA programs that will be discussed afterwards.

Section 215 allows the collection of business records that could be relevant for any investigation. It significantly expanded the type of intelligence that can be gathered, defined broadly as "tangible things". This basically means everything: books rented, billing records, documents, data and other items. With this paragraph the government can force private companies to hand over all kinds of customer data, like IP-address tables. It also includes so-called gag-orders, which means that the company is not allowed to disclose this seizure publicly and cannot initiate a judicial appeal. This paragraph was used to legalize the NSA PRISM program (see next chapter).

Accompanying the practice of the gag orders are the *National Security Letters* (NSL). Those letters are a kind of subpoena, initially designed to collect customer transactional records, and were expanded for other types of (meta) data: "historical information on telephone calls made and received from a specified number; billing records; subscriber information including name, address, and length of service; and e-mail addresses associated with an account" (Greenlee, 2008, p. 188). Critiques argue that these letters are a method to bypass warrant requirements for law enforcement. In 2004, the FBI issued 56000 of these letters, compared to 8500 in the year 2001, before 9/11 (Donohue, 2008, p. 238). In 2003, Attorney General Ashcroft issued a guideline that data from these letters can be stored indefinitely and should be shared with *any* other federal agency. In 2004, the Bush administration expanded executive powers quietly with the Intelligence Authorization Act for Fiscal Year 2004. This order enabled that more agencies could issue NSL on a broader range of targets[127] (Donohue, 2008, p. 241).

In sum, legal provisions within the Patriot Act fit nicely to the idea to gather as much data as possible from different sources and to make this data available to different agencies. It is very much in line with the idea of information dominance. The Patriot Act thus is a clear expression of cyber-realism and an often-citied instance of the securitization of the Internet, expanding national security politics beyond the established rules of the game within a liberal democracy (Nissenbaum, 2005, p. 70). The act *blurs* the boundaries

[127] Like "banks, credit unions, thrift stores, brokers in securities or commodities, currency exchanges, insurance companies, credit card companies, dealers in precious metals, stones, or jewels, pawnbrokers, loan or finance companies, travel agencies, any business that transfers funds, telegraph companies, car, airplane, and boat sellers, real estate agents, the US Postal Service, state and local government entities involved in the preceding, and casinos" (Donohue, 2008, p. 241).

between domestic and international. It turns the outside in: instruments of international relations (intelligence gathering) were used domestically. In a nutshell, the act lowered the standards for intelligence gathering and reduced judicial oversight while expanding surveillance functions to more parties and maintaining a broader definition of what information could be gathered and must be shared with other agencies. At the same time, 4th amendment rights were restricted – "information about individuals not subjected to a criminal investigation" (Priest & Arkin, 2012, p. chap. 7) could be collected without their knowledge and the need to inform suspects after an operation, to allow an appeal in court. Lawmakers realized the controversial nature of the act and introduced so-called sunset provisions – clauses that had to be reauthorized by Congress in 2005. However, controversial elements such as the NSL would not be designated to sunset.

What other changes were there? One was the creation of the Department of Homeland Security (DHS) in 2002 and the idea of local intelligence fusion centers.[128] The DHS was meant to address the problem of terrorists inside the US. As mentioned before, the need-to-share norm requires the creation of databases that store intelligence. To this day it is hard to grasp a complete picture of how many counter-terror and crime databases exist, what kind of information is stored therein, who has access[129] to what kind of data and what kind of privacy safeguards exist. Only a snapshot can be provided. In 2007, the DHS reported that its Homeland Security Information Network (an integrated network of several classified databases) had expanded to all 50 states. This network allowed multi-directional sharing of counter-terror information between government and industry.

Another change was the Intelligence Reform and Terrorism Prevention Act (IRTPA) in 2004, which implements the reshuffling of the intelligence agencies. It was a response to the 9/11 commission report and represents the "most sweeping changes in the intelligence world since the National Security Act of 1947" (Priest & Arkin, 2012, p. chap. 5). It created the position of the DNI, Director of National Intelligence (John Negroponte) whose job it is to coordinate all 17 intelligence agencies (as of 2015). IRPTA added the so-called "lone-wolf clause", which authorizes FISA warrants "for individuals involved in international terrorism, but not affiliated with a known terrorist group" (Collins, 2004, p. 14), thus broadening the scope for potential surveillance targets. In 2004, the FBI asked the FCC to expand the scope of the 1994 CALEA to include Internet and VoIP

[128] Fusion centers combine intelligence from various agencies (intelligence community, military) with information from the local level (police reports, crime & other incidents). It is unclear how many of these centers exist. Even the DHS has no numbers how much it spends annually on these centers and what the money is used for. The initial budget in 2003 was $31 billion (Priest & Arkin, 2012, p. chap 7).

[129] According to Arkin, there are around 4000 federal, state and local organizations with counterterrorism responsibilities and jurisdictions (Priest & Arkin, 2012, p. chap. 7).

communications (see chap. 4.3.5.2 Policy: Wiretapping the Internet with CALEA (1994)), which was denied because of privacy concerns when the bill was signed (Landau, 2010, p. chap 4.4). Between 2004 and 2007, the phone wiretap volume grew 62% and that of digital communication like email 3000% (Singel, 2007).

Additionally, there was a dramatically increased intelligence budget. Directly in the aftermath of 9/11, Congress granted a blank-cheque of $40 billion to counter the attack and another $40 billion were approved a few weeks later (Priest & Arkin, 2012, p. chap. 1). Both intelligence and defense spending doubled since 9/11, a dramatical increase compared to the the Clinton administration. It is possible to reconstruct this, because the intelligence budget was declassified in 2007, following a recommendation from the 9/11 commission. In this year, the National Intelligence Program (NIP) was worth $49.25 Billion, and the Military Intelligence Program (MIP) Budget was $22.64 Billion, totaling an intelligence spending of $71.9 billion. The budget increased during the Obama administration in 2011 to a total $83.26 billion and then began decreasing to $73.16 billion in 2013 (Erwin & Belasco, 2013).

Summing up the legal and structural changes that were adopted after 9/11, there is one theme: bigger/more is better. Everything grew in scale: money (intelligence budget), personnel, competencies, data gathering skills and intelligence private-public partnerships. New agencies were formed,[130] the outsourcing of surveillance functions to private companies and overall secrecy[131] increased. The only thing that did not grew was legal oversight and staffers.[132] The post 9/11 security apparatus grew so substantially that even those tasked to coordinate it had no complete picture. When Robert Gates replaced Rumsfeld as Defense Minister in 2006, he wanted to track all the DoD secret programs. The conclusion was: "the complexity and lack of accountability made it impossible to tell whether the country was safer because of all this spending […]" (Priest & Arkin, 2012, p. chap. 1).

These cyber-realist policies were the necessary condition for the creation of technical artifacts that aimed to control cyberspace. The next chapter analyzes how the NSA and other agencies constructed technical artifacts to realize the goals of total information dominance or awareness that would potentially enable the tracking of terrorists in cyberspace.

---

[130] Journalist William Arkin counted 1074 new federal government organizations concerned with counterterrorism in the year 2009 (Priest & Arkin, 2012, p. chap 4.)

[131] The number of classified documents tripled to over 23 million, bringing the classification system to its limits (Priest & Arkin, 2012, p. chap. 1).

[132] The amount of congressional staffers with intimate knowledge of the intelligence community, controlling their programs actually declined (Priest & Arkin, 2012, p. chap. 1).

4.4.7.3 Artifacts: NSA and the Full-take Norm of Internet Control (2001 -)

This essential chapter introduces the counter-artifacts developed by NSA that aim to realize the goal of total information awareness and to collect as much intelligence as possible. These programs are intentionally designed by cyber-realists to counter the effects of the original Internet – namely anonymity and privacy and other obstacles introduced by TCP/IP. They are the technical side of the large socio-technical change that was introduced after 9/11 (but began before), the other being the legal and structural reforms of intelligence gathering described in the previous chapter. Before we turn to the changes, a bit of background is needed.

The NSA was established in 1952 and since then had an *outward-looking mandate*, to monitor Soviet targets (Bamford, 2009, p. 13). Domestic surveillance was not its original mission description, but the Watergate scandal showed that NSA, in secrecy had expanded its mission to monitor actors inside the US as well.[133] Initially, NSA was intended to be a small agency with a supporting role. It was tasked by lead agencies such as CIA to collect certain types of SIGINT for them (Rovner & Long, 2005, p. 619). With the primary eavesdropping target (Soviet Union) gone, the importance of NSA gradually declined during the 1990s. General Michael Hayden, Director of NSA between 1998-2005 (see appendix Table 14. Intelligence Community Directors) comments:

> "NSA downsized about one-third of its manpower and about the same proportion of its budget in the decade of the 1990s. That is the same decade when packetized communications – the e-communications we have all become familiar with – surpassed traditional communications" (Hayden inBamford, 2009, p. 47).

This indicates the problems the Internet produced for intelligence agencies, because dynamically routed communication was harder to intercept (Kaplan, 2016, p. chap. 8). Other problems for a SIGINT included that "communications were being encoded with powerful new commercial encryption that was proving virtually impossible to break" and "the exploding volume of global communications as more and more messages were moving through hard-to-tap fiber-optic cables" (Hayden, 2016b, p. chap. 1.). In other words, the digital revolution was perceived as a problem for a downsized and marginalized agency whose job description is intercepting and interpreting information. Packet-

[133] "Between 1967 and 1973, the NSA intercepted communications of Americans thought to be associated with drug trafficking, terrorism, threats to the President, and civil disturbances such as the anti-war movement" (Sanders, 2012, p. 273).

switching made NSA's job more difficult. "Technology has moved from being the friend to being the enemy" (Hayden, 2016b, p. chap. 2.).

For Hayden, 9/11 was a window of opportunity to address this problem and to increase NSA's standing vis-à-vis the IC in general. In fact, 9/11 would transform NSA into the biggest and technically most sophisticated intelligence agency on earth.[134] The change began directly a few days after the 9/11 attacks. In early October 2001, Hayden (for the first time ever) met with President Bush and Cheney. In an interview, Hayden recalled that Cheney said: "What would you like to do that you cannot already do that would help prevent another 9/11?" (Kirk, 2014). At least since 1999, Hayden had several experimental R&D programs in place that aimed at domestic telecommunications surveillance (Harris, 2014, p. chap 2.). Hayden argued that he cannot legally use them under the FISA regime and thus uttered concerns over the lawfulness of these programs. According to Hayden, Bush said: "[…] there are some things we are going to have to do, and I think I have the authority to authorize you to do the things" (Kirk, 2014). The underlying rationale behind this blank cheque was that in times of emergency the "gloves come off" (Risen, 2006, p. chap.1). In the following days, Hayden, together with CIA director George Tenet, basically drafted a surveillance wish list.

On October 4th, Cheney issued a secret signing order, under which the President authorized "the program". The order was written not by the President's legal aid (who would be legally in charge), but by Cheney's, David Addington, which is unique in US intelligence history (Kirk, 2014). This underscores the role of the Vice President in enabling the largest spying operation known to date. The program would operate *outside the FISA regime* for domestic surveillance. It would only be legitimized by the President's article 2 powers, based on the unitary executive theory. The combination of these necessary conditions, the blank cheque and the shared interests of Cheney and Hayden in terms of surveillance, immediately after the 9/11 shock, explain the form and severity of surveillance measures taken. A non-influential Vice President with no grudge with the FISA court and less radical neoconservative views probably would have adopted less severe measures.

What did "the program" do? Because of secrecy there is an ambiguity whether it was indeed one program or several smaller ones that later were combined and renamed. Its origin was a 1999 program called Trailblazer, which Hayden described as the agency's

[134] With failure to connect the dots at 9/11 and the Iraq WMD intelligence blunder of 2003, the CIA's role was downgraded with the Intelligence reform of 2004 (Russell, 2007). At the same time, NSA became upgraded dramatically. In 2008, NSA had 40% more workforce compared to pre 9/11. Whereas in 2001, NSA had around 55 contracts with external companies, that number grew to 7197 in 2005 (Bamford, 2009, p. 199).

future (Gorman, 2006). Trailblazer was designed to fuse all kinds of information that NSA gathered with different techniques (SIGNT, HUMINT, Reconnaissance Intelligence) from various listening-posts (like the Echelon satellite surveillance system) all around the world into one, centralized and searchable database. The problem that this technical artifact was going to address was that even before the intelligence expansion of 9/11, NSA collected more data than it could analyze, thereby suffering information overload. In his memoirs, NSA director Hayden describes a blackout of NSA systems in early 2000 where "the sheer volume of collection had overwhelmed the capacity of our networks as they had been configured" (Hayden, 2016b, p. chap. 1). In 2002, NSA collected 200 million pieces of intelligence per day but could only analyze 1 percent of it (Lee, 2015, p. 28). Additionally, with the digital revolution, the digital haystack was potentially doubling in size each year. [135] Trailblazer was designed to be the solution to all of NSA's "information management problems" (Gorman, 2006), to store and analyze intelligence in "the largest database of every call ever made" (Cauley, 2006).

Data like audio (intercepted messages in a plethora of different languages), video and images and all different kinds of records like financial and Internet traffic, had to be transcribed (to be computer-readable) and stored. To get this data, in early 2001, *before* 9/11, NSA allegedly began approaching US Internet- and telecommunications carriers, in secrecy, to obtain two kinds of data: First, customer records such as caller-ID and Internet meta-data.[136] Second, NSA began to collect Internet content data (in some instances) by physically tapping into communication networks that handled the majority of the nation's phone-calls, text- and E-mail messages as well as Internet traffic.[137] Later, the Snowden leaks would call this full-take of Internet data the UPSTREAM program (see chap. 4.5.5 Artifacts: The Snowden Leaks). Initially, some of the ISP denied, but the later Patriot Act required them by law to hand over this kind of information (Harris, 2007).

[135] Hayden: "mobile cell phones increased from 16 million to 741 million, an increase of nearly fifty times. […] Internet users went from about 4 million to 361 million, an increase of over ninety times. Half as many landlines were laid in the last six years of the 1990s as in the whole previous history of the world. In that same decade […] international telephone traffic went from 38 billion minutes to over 100 billion. This year [2002], the world's population will spend over 180 billion minutes on the phone in international calls alone" (Hayden, 2016b, p. chap. 4).

[136] Metadata like: who calls whom, when, how long, with which phone number from which geolocation. The Snowden leaks (2013) repeatedly stressed the important role of metadata that is used as a first instance of intelligence. Metadata is used as a filter-device in order to manage the vast amounts of stored content data. To analyze metadata, NSA set up a special Metadata Analysis Center (Harris, 2014, p. chap 2.). According to Snowden leaks, 250 people work there (Ewen MacAskill et al., 2013).

[137] Estimates by Minnesota Internet Traffic Studies suggest that during 2000, the amount of data that the internal US internet-network handled was between 20000 and 35000 Terrabytes/Month. In the year 2011, this grew to around 3 million TB/month (Minnesota Internet Traffic Studies, 2017). According to Forbes, 12 billion E-mails were sent in 2000. (Chiang, 2009).

To gather data, NSA would install "what's normally foreign intelligence, outward-facing equipment" (Drake inKirk, 2014) on domestic networks. Splitters would be installed at fiber-optic cables at the central US Internet Exchange points (IXP), for example those which physically connect the North American continent with Europe or East-Asia (see following figure).

Figure 26. Map of Internet Data flows, Source: (Landau, 2010, p. chap. 4.6)

Since the privatization of the Internet backbone (see chap. 4.3.4 Artifacts: Privatizing Control over the Internet), these are operated by private service providers and handle large amounts of *both* domestic and global Internet traffic.[138] Splitters use a prism to copy *everything* that is transmitted through that fiber optic cable (The Washington Post, 2013a). They basically copy the Internet. We know all this because in 2003, AT&T technician Mark Klein became aware of secret NSA rooms (room 641A) at large AT&T Internet-switches. Through these rooms, international and domestic Internet data-streams were routed, copied and then fed into NSA's data analysis programs. Former NSA analyst and Trailblazer developer William Binney declared (under oath) in 2012 that the agency had between 10 and 20 intercept centers all over the US (Lee, 2015, p. 153). Hayden once called this the "gold of the program" – the agency could "spy on the world without leaving home" (Harris, 2014, p. chap. 2).[139] Klein filed a law-suit, together with civil liberty groups, and lost in 2006. However, this process revealed the existence of the NSA

[138] Large portions of the physical Internet infrastructure are located in the US, which means that a large amount of global traffic is routed via the US. Additionally, many services like Google or Facebook are American, which means that the 90% of people around the globe who use "Google search", contact servers within the USA, which means that their traffic potentially gets collected (Risen, 2006). Insiders testified that NSA even encouraged the telecommunications industry to increase the capacity so that even more global data is handled by US switches (Harris, 2014, p. chap. 2).

[139] This creates a legal ambiguity. Because of dynamic routing, an E-mail between two 4th amendment protected American citizens, from Washington to Austin may be routed via Pakistan, and therefore become international communication. Since these switches carry both international and domestic communication, it becomes harder (if not impossible) to distinguish between foreign and domestic communication, as the FISA law requires (Risen, 2006, p. chap. 2).

warrantless surveillance program in late 2005 (Risen & Lichtblau, 2005) and President Bush was forced to acknowledge its existence on December 17, 2005.

From a technical perspective, this is a remarkable program because it is a logical way to circumvent many of the wire-tapping issues introduced with the TCP/IP protocol and fiber optic cables – namely dynamic routing, packet-switching, the end-to-end principle that created limited degrees of anonymity (see chap. 4.1.3.1 Artifact: Internet Protocols and Norms). Several intelligence officials repeatedly stressed the challenge of TCP/IP for eavesdropping:

> "Today you have no idea where that information is being routed […] You don't know how it's being routed, it's going through all kinds of switches, the information is not where you think it is, and that's what created the complexity and that's what we have to figure out how to deal with" (Bamford, 2009, p. 162).

This statement is key evidence (see chap. 3. Methodology & Research Design) that the Internet's core technologies like fiber optic cables and dynamic routing represented a core nuisance for actors engaged in SIGINT, because it made wiretapping harder. In theoretical terms, it is an anomaly or puzzle that the paradigm of cyber-realism tried to solve with all available means, which explains why NSA, the impact constituency, spent a lot of resources circumventing it (Harris, 2014, p. chap. 1). The goal of these artifacts was to reinstate intelligence in a network that was designed to have none.

This becomes evidently clear with one of Trailblazer's companion programs called Thinthread. It sorted and analyzed metadata and then correlated it to content data and thereby basically acted as a filter. It could "detect meaningful traffic via the metadata of a massive communication stream (e-mail or voice)" (Hayden, 2016b, p. chap. 2). The metadata was analyzed for patterns, frequency and length of calls and thereby pointing the analysts to communications whose content should be explored (Hayden, 2016b, p. chap. 2). It included E-mail analysis and was directly designed to address one of the core problems of NSA: packet-switching. According to Hayden, Thinthread "could assemble the individual packets that comprise e-mail messaging" which "enabled it to put communications back together from the individual packets" (Hayden, 2016b, p. chap. 2). The problem of Thinthread was that it could only handle small portions of data. It could not be scaled up to support bulk-data collection. The problem of Trailblazer was that it was bulky and slow and was highly cost-intensive – over $1 billion in a decade (Kaplan, 2016, p. chap. 8). Eventually, Trailblazer and Thinthread were merged to address the problem of

scalability and to create one of the first big-data systems within an intelligence agency.[140] It was renamed Stellarwind, which since 2005 is known to the public as the Terrorist Surveillance Program (Bush, 2005).

The "Upstream" data collection at large intermediary nodes of the physical Internet infrastructure that handle the majority of packets allows to intercept many of these. Packets would be reassembled with the help of supercomputers and special Deep-Packet-Inspection Software.[141] In theory, if one would have all the packets sent over the Internet, one would be able to sort them out and combine them, just like in a large jigsaw puzzle (given enough computing power and as long as they are not encrypted). In the post card metaphor used to describe packet switching before, the equivalent would be collecting and photocopying all post cards passing through a postal office (see chap. 4.1.3.1 Artifact: Internet Protocols and Norms). However, this data alone is too complex. To make sense of it, meta-data (data about this data) and customer records are needed. Customer records allow to correlate an IP-address with a human operator, which eliminates all anonymity and so it becomes transparent what each Internet connection does on the web. In other words, meta-data collection on a massive scale is one way to solve the attribution problem (see chap. 4.4.2.2 Problem Definitions of Cyber-Realism).

If this practice was repeated internationally at other large IXP,[142] this would statistically allow to analyze large portions of global, unencrypted Internet communications. With the Snowden leaks of 2013, we became aware of similar programs conducted by the Five-Eyes intelligence partnership (including US, UK, Canada, Australia, New Zealand). Under the Tempora program, the British GCHQ applied the splitter and DPI technique to European fiber-optic cables, intercepting "more than 40 billion pieces of content a day", or 25% of the Internet traffic (Gallagher, 2015b). Because of the geographic structure of the large transcontinental Internet-cables, most of the European traffic to the US physically crosses British territory, which allows for interception of

[140] According to Hayden: "we had the theoretical ability to access a significant percentage of the calls entering or leaving the United States" and "We also gathered large volumes of metadata. In the first six months of the program we built up a bank of billions of domestic call events in addition to an even larger number of foreign ones. We used contact chaining from known or suspect "dirty numbers" to see if there were connections that suggested terrorist ties to the United States" (Hayden, 2016b, p. chap. 5).

[141] Deep Packet Inspection (DPI), was initially designed by ISP for billing purposes and can read a packet's content data while it passes an Internet router (Parsons, 2013). According to Bamford, NSA used a technology from an Isreali Company called NARUS to analyze the copied data-streams. After 9/11 NARUS began to sell its NARUS STA 6400 Semantic Traffic Analyzer and its Intercept Suite to intelligence agencies around the world. The suite can reassemble packets, based on their identifier number, flowing through a network from a remote location (Bamford, 2009, p. 192).

[142] Another method would be installing splitter under the ocean, directly at the cables. In the month before 9/11, reports surfaced that NSA was repurposing submarines for this end (Jr, 2001). Other nations most likely do the same (Huddleston, 2015). Physical control of fiber-optic cables would be one way to disrupt global communication in case of war.

continental communication directly at the British shorelines. The Tempora program, with its aim of "Mastering the Internet" became operational in 2011 (Shubber, 2013). Operation Eikonal by German Bundesnachrichtendienst (BND) seemed to serve a similar purpose at the largest central European IXP, DE-CIX (although BND denies this). Most likely, other partners conduct similar operations (there are reports from Mexico, India, Afghanistan and Iraq, Canada, UK, Australia, New Zealand), thereby creating a global wire-tapping network (Bamford, 2009, p. 221). Mastering or "owning" the Internet, which means awareness and total control of all information transmitted therein stands in stark opposition of the initial norms that were embedded in the system, namely a certain degree of privacy and anonymity and the idea that only the end-points of the network have intelligence. In total, the whole NSA-program can be characterized as a global dragnet data collection that tries to collect every piece of information that traverses the global ICT infrastructure and to circumvent the Internet's initial anonymity features.

The intentional design of the program is to gain as much data as possible and potentially, in the long run, collecting and storing the *entire* Internet and communication traffic, both content and meta-data for weeks or even months. In 2014, a large $1.5 billion NSA data-center was completed. It is said to have a storage capacity for several zetta or even yottabytes of data[143] and is equipped with Cray supercomputers to sift through the data (Bamford, 2012). In other words, the ultimate aim is to store and analyze all information transmitted over the global Internet infrastructure, hence the name "full take approach". To this present day we cannot be sure how much of this data is actually stored and analyzed. Nevertheless, it is the most expansive data collection in the history of mankind, although only a quick snapshot could be provided.

Although we are aware of intelligence *collection*, we have limited insight on *analysis* or what is done with the data. To shed light on this, we can analyze another, non-classified program called Total Information Awareness Program (TIA) that was launched in August 2002 at DARPA under the lead of Navy Rear Admiral John Poindexter. When Congress cancelled TIA in 2003, many of its components went to the NSA. This is the reason why I elaborate on this. The following is based on a report to Congress in 2003 (Stevens, 2003) and other secondary sources. The aim of TIA was quite similar to NSA's program – to prevent another 9/11 and therefore to find "terrorists in the world of noise" (Poindexter, 2002). The problem is not just connecting the dots, but "to know which dots to connect" (ibid.). The ultimate aim is, as the name suggests, total information awareness or to create

[143] Cisco estimates that the global Internet traffic has a size 1.1 ZB per year (Cisco Systems, 2016). This includes video content. Excluding the video, a data-center of 1 ZB storage capacity could store several years of Internet traffic.

an "information weapon", as Harris called it (Harris, 2006). The seal of the TIA program was therefore the freemason pyramid with the all-seeing eye and the slogan "scientia est potentia", knowledge is power. For that purpose, TIA aimed at building an integrated, unified software platform that could "data mine an indefinitely expandable universe of databases" (Stevens, 2003). Because of the sharing norm, external databases would be provided by other law enforcement and intelligence agencies (for example the plethora of new counter-terror databases after 9/11, such as the DHS database), but could also come from the private sector.[144] In turn, they would get access to the system.[145] The major functions of TIA were machine-translation of languages, data mining and patterns of life analysis. Let's take a look at some subcomponents:

The $44.6 million *Evidence Extraction and Link Discovery program* was intended to analyze social relationships of people, organizations and places. It analyzed who would go where, when and how long and search for patterns. Similarly, the *Scalable Social Network Analysis module* ($7.4 million) analyzed patterns in communications metadata to draft social networks of people (who speaks with whom, who is the central broker in a network). Social network analysis is particularly powerful and based on the idea of affiliation. If you affiliate with a terrorist (even without knowing), you belong to that network and thus potentially to a terrorist cell. The NSA allegedly stores social network information of targets up to three hops (or degrees of segregation), which mathematically increases the number to millions of people. If anyone in these is a terrorist, and you have a random link to him/her, you therefore are suspicious (Gallagher, 2013). The *HumanID module* ($32.2 million) aimed to identify humans at a distance based on their body features. The *Next-Generation Face Recognition program* ($17.1 million) would implement automatic face- and biometric recognition of stored images and videos (Stevens, 2003). In sum, TIA brought together many state-of-the-art Big Data analysis algorithms that were designed to find patterns in large quantities of data. These quantities came from the NSA wiretapping activity described before.

When Congress discovered the plans and ambitions behind TIA in late 2003, a public outcry followed. The executive initially simply renamed the program *Terrorist Information*

[144] "Transactional data for the TIA database could include financial (e.g., banks, credit cards, and money transmitters, casinos and brokerage firms), educational, travel (e.g., airlines, rail, rental car), medical, veterinary, country entry, place/event entry, transportation, housing, critical resources, government, and communications (e.g., cell, landline, Internet) data. Biometric data for the database could include face, finger prints, gait, and iris data. The TIA system could seek access to databases to discover connections between "passports; visas; work permits; driver's license; credit card; airline tickets; rental cars; gun purchases; chemical purchases – and events – such as arrest or suspicious activities and so forth" (Stevens, 2003, p. CRS 2).

[145] Harris argues that in its first year of testing in 2003, more than 250 agencies and entities had access and used the TIA prototype. In August 2003, there were 320 agencies connected to it (Harris, 2006).

Awareness to eliminate concerns, but in the end, Congress decided to stop funding. John Poindexter, partly because of his controversial role in the Iran-Contra affair, had to resign (Harris, 2006). Theoretically, that was the end of TIA, but there is evidence that some of the subcomponents I just described were renamed *Research Development and Experimental Collaboration*, "to erase any connection to its past" (Harris, 2006) and were moved to different contractors and to NSA's own research program (Shorrock, 2009, p. chap. 6). When Congress asked Hayden whether TIA *really* closed in 2003, he responded "I'd like to answer in closed session" (Harris, 2006). Indeed, many of the NSA programs leaked by Snowden clearly resemble TIA components (see chap. 4.5.5 Artifacts: The Snowden Leaks).

On a theoretical level, what the NSA and TIA did with the programs was to reestablish intelligence in the Internet, by building, within a legal grey-zone, on top of the existing physical infrastructure. As such, it represents a form of reconstitution (Pfaffenberger, 1992a) of the Internet infrastructure without altering its protocols (see following figure). The surveillance infrastructure that was put in place is a counter-artifact, aiming to compensate deficiencies perceived by cyber-realist advocates, namely norms of privacy and anonymity. Anonymity, and tools that provide it (like encryption or the Tor Network), are "the bane" of every intelligence agency (Harris, 2014, p. chap. 5). The idea of end-to-end was that the network is dumb – no central authority is aware of the Internet's content. By tapping into the physical Internet infrastructure and analyzing data streams with software, NSA reintroduced intelligence into the network, becoming aware of every packet and its content. The different legal and technical parts of the program made it possible to circumvent anonymity and to see which IP-address communicates with whom, where and what they talk about. Thus, NSA reversed the logic that on the Internet nobody knows that you are a dog (see chap. 4.2 The Evolution of Cyber-Utopianism). The following graphic depicts the interplay of cyber-realism and the technical artifacts it constructed.

Figure 27. Cyber-realist paradigm reconstituting the Internet via NSA programs (own diagram)

Cyber-Realism during 2000s	
problem → goal	- same problem definitions as IW doctrine: death of distance problem, transcendence of state borders and problems of jurisdictions, speed of CNA, no pre-warning, anonymity of the Internet is a core problem (attribution problem), lack of government control - New problems: terrorists hidden within society, SIGINT downscaled after Cold War, rise of packet-switching and digital communication - → Information Dominance/Superiority, bulk data collection - → penetrate fog of war with information operations - → terrorist prevention and preemption - → all source-intelligence gathering and sharing
anticipated use of Internet	- Internet for military command and control - used by adversaries for hacking U.S. critical infrastructure - Terrorists use the Internet as safe-havens and to plan attacks, recruit followers - U.S. could use Internet for pax Americana
social elements (norms, power)	- military/IC as defender of cyberspace - Counter-appropriating the lack of state control over cyberspace - it is appropriate for military to penetrate enemies networks, even in peacetime - War on Terror justifies expansion of Internet surveillance powers & secrecy (unitary executive theory) - turning foreign spy-apparatus inside: full-take data gathering norm

Construction

NSA Programs	
material dimension	**social dimension**
- obtaining meta-data and certain content data from ISP - wiretapping & copying Internet data streams at IXP, domestically with splitters - global wiretapping at key IXP with 5 eyes partners (Upstream) - Deep Packet Inspection Software - server-access of Internet Providers (PRISM) - breaking encryption (Bullrun) - big-data data analysis (Trailblazer, Stellarwind) - Data-centers - pattern of life analysis, social network analysis, biometric recognition (TIA) - datacenters, storing portions of the Internet	- full-take principle - mastering the Internet: total control of all packets traversing the net - total information awareness - supporting legislation (Patriot Act) - Prevention Logic & Intelligence Sharing - upgrading of NSA - intelligence sharing between 5 eyes and other partners (exploiting legal loopholes) - everyone is suspicious - reestablishing intelligence in a dumb-network

In retrospect, even national security officials acknowledge that the NSA warrantless surveillance program was a "sea-change" or "a major shift in American intelligence gathering practices" (Risen & Lichtblau, 2005) that altered 30 years of intelligence regulations, established with FISA. "Stellarwind was a departure from normal" (Hayden, 2016b, p. chap. 5). Legitimized during the shock situation of 9/11, without any public discourse, the Bush administration turned the NSA inwards while sidestepping fundamental checks and balances. At the same time, the scale and magnitude of intelligence gathering was expanded. "Everybody's a target, everybody with communication is a target", as one senior intelligence officer told author James Bamford (Bamford, 2012). Over time, this extraordinary practice, contesting many liberal norms, became the new normal. Tech-enabled mass surveillance initiated a path-trajectory.

The reader might ask, what does this have to do with cyber-war? The answer is: the very same infrastructure used for intelligence collection also is a valuable platform to launch offensive cyber-attacks. In the digital age, wiretapping is no longer a passive activity, sitting at the wires and listening in. It is an active procedure that requires breaking into computer-systems and networks with the help of special malware. Hacking into the global Internet infrastructure and sifting through global data-streams technically is a form of computer network exploitation. The network "exploited" is the global Inter-network. Thus, Internet surveillance with the aim of information awareness and/or dominance in

cyberspace is logically connected to computer network attacks or cyber-war. In other words, surveillance involves a great deal of hacking, as will be shown in the next chapter.

4.4.7.4 The Fusion of IW, Surveillance and Cyber-war (2003-2008)

Whereas the previous chapter highlighted additions to cyber-realism that came with the anti-terror policy immediately after 9/11, this chapter analyzes the continuity and institutionalization of information operations within the US Military and IC. Thus, it adopts a longer timeframe describing the general storyline (see chap. 3. Methodology & Research Design) and focuses predominantly on the evolved literature on Information operations. The central argument is that IW and Internet surveillance became fused together to create a nexus.

As indicated before, Secretary of Defense Donald Rumsfeld was one key advocate of IW and CNO, even before 9/11. Beginning with his swearing-in ceremony, he placed the issue of IW on the agenda as the second most urgent threat after weapons of mass destruction (Rumsfeld, 2001). In June 2001, at a NATO council meeting, he warned allies of "attacks from cyberspace", thereby diffusing the threat perception of the Internet as a dangerous place globally (Bendrath, 2003, p. 57). During his tenure, Rumsfeld began to implement RMA and IW concepts within the organizational structure of the US military and IC in order to reform the US defense policy and strategy. In 2002, he wrote an op'ed in Foreign Policy, arguing that the revolution in military affairs must be used to fight against new enemies such as terrorists and to defend US information networks from cyber-attacks (Rumsfeld, 2002). The roadmap for this transformation argued that information operations[146] should become a core capability of the US military: "the Department must be prepared to fight the net" (Department of Defense, 2003, p. 6). The norm of control is clearly outlined in plans for "seizing control of adversary communications and networks", even in peace-time. When implemented, this roadmap will transform the military into an "information-centric force" and would "jumpstart a rapid improvement of CNA capability" (Department of Defense, 2003, pp. 6-7). The fusion of the intelligence reform and military strategy becomes obvious in statements such as that "the IO battlespace should be prepared through intelligence" because "intelligence is a fundamental prerequisite for full spectrum IO." Computer network operations should "capitalize on newly acquired authorities provided by the Patriot and Homeland Security acts" (Department of Defense, 2003, pp.

[146] "Information operations (IO) are described as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own" (Joint Chiefs of Staff, 2006, p. ix).

18-22). In other words, the bulk-data collection should be used to prepare the battlefield for cyber-attacks.

In February 2003, President Bush issued the classified presidential directive 16, which intended to clarify under which circumstances the US would engage in offensive cyber-attacks and who would have the authority to conduct those. It also included the notion of a pre-emptive cyber-attack, for example against China and Russia. The directive was also the result of a larger "national strategy to secure cyberspace" (The White House, 2003) that had been in development since the Clinton administration. It adopts a lot of the critical infrastructure rhetoric of the Clinton administration and surprisingly includes liberal norms that acknowledge that the government alone cannot and should not secure cyberspace. However, this strategy seemed to be relatively marginalized in the general IO context.

Counter-terrorist terminology and ideas also became embedded within the reformed Doctrine for Information Operations (Joint Chiefs of Staff, 2006).[147] There is a heavy focus on the notion of intelligence support for IO. IO "requires intelligence on relevant portions of the physical, informational, and cognitive properties of the information environment" (Joint Chiefs of Staff, 2006, pp. III-1). Informational properties are "specification, capacity, configuration, and usage" as well as "technical design of information infrastructure", in other words the structural composition of Internet nodes and networks in other countries, as well as *content* and context of communication networks. It should become clear that these intelligence demands fit nicely with the NSA mass surveillance programs that targeted international IXP for bulk data collection.

In January 2005, IO including offensive network warfare authorities were given to US Strategic Command (STRATCOM) and one of its functional components called Joint Functional Component Command for Network Warfare (JFCC-NW). The new director of NSA, General Keith Alexander (2005-2014), became director of JFCC-NW and was "responsible for deliberate planning of network warfare" (Wilson, 2006, p. 8). NSA became responsible for CNE *and* CNA. General Alexander, in contrast to his predecessor Michael Hayden, is described as a "technical wizard" or engineer, one who actually understands the technical backgrounds of cyber-war (Kaplan, 2016, p. chap. 9). Alexander worked at Army Intelligence and Security Command after 9/11 where he developed

[147] Whereas the 1998 doctrine explained the concepts of information war, the 2007 doctrine replaces the term with Information Operations and aims to "provide joint force commanders (JFCs) and their staffs guidance to help prepare, plan, execute, and assess IO in support of joint operations." (Joint Chiefs of Staff, 2006, p. ix). The general problem definitions and narrative and goals stay the same. The 2013 updated Information Operations doctrines continues the trend to assign authorities and responsibilities and also focuses on multinational IO.

similar ideas to NSA, like to conduct traffic and pattern analysis in large volumes of Internet data. Whereas NSA built Trailblazer, a one-size-fits-all system that was costly ($1.2 billion) and bulky, Alexander favored a distributed, decentralized approach of multiple smaller programs and databases talking to each other. Smaller systems interacted and backed each other up while specializing in certain aspects (Kaplan, 2016, p. chap. 9). One component was called *Turbulence* and began in 2005 (see chap. 4.5.5 Artifacts: The Snowden Leaks). Although Turbulence is similar to Trailblazer in the sense that it, too, analyzes Internet data on the packet-level by sifting through the data looking for suspicious patterns, it also included several offensive cyber-war components. Whereas Trailblazer was more of a passive eavesdropping system (CNE), Turbulence was designed to be active or even offensive (CNA). Turbulence included a series of interconnected hacking techniques for CNA, such as man-in-the-middle attacks, DNS-injection, packet-spoofing and more.[148] These will be analyzed in more detail in a later chapter (see chap. 4.5.5 Artifacts: The Snowden Leaks).

In general, these technical artifacts manifested the fusion of surveillance and cyber-war. JFCC-NW was tasked with both disruptive and destructive CNA, espionage or CNE and, since 2008, computer network defense of military networks (whereas the DHS is responsible for the CND of civilian critical infrastructure). Its operations are classified and the US never admitted to be responsible for any known cyber-operation. Because of this dual-hat structure, the director of NSA can utilize intelligence support (from the overall IC) for computer network operations (Lin, Dam, & Owens, 2009, p. 166). This functional overlap is effective because complex cyber-attacks require actionable intelligence of adversaries' computer systems and are functionally similar to CNE. Nothing showed this more than the war in Iraq.

During the year 2007, several noteworthy cyber-incidents happened (DDoS Attack on Estonia and Israeli hacking of Syrian air-defense called Operation Orchard). The military operation in Iraq is often forgotten in books on the history of cyber-war (Healey & Grindal, 2013). During the "surge" of 2007, JFCC-NW's new toys and skills were put to the test. It was former NSA director (1992-1996) and now DNI (2007-2009) Mike McConnell who convinced G.W. Bush to authorize operational cyber-war with CNE elements in Iraq in April 2007 (see appendix Intelligence Community Directors). As

[148] All these are hacking techniques are often used by criminals in order to insert malware into a system. According to Kaspersky, a man-in-the-middle attack "requires only that the attacker place himself between two parties that are trying to communicate and that he be able to intercept the messages being sent and further have the ability to impersonate at least one of the parties. For example, in the offline world this could involve someone creating fake bills or invoices, placing them in a victim's mailbox and then intercepting the checks that the victim attempts to mail back as payment." (Fisher, 2013). By faking to be a trusted party, hackers can insert malware into the senders system without him/her knowing.

former NSA director and a fierce advocate of cyber-war (see chap. 4.4.2 Ideas: Formation of the Information War Doctrine (1976-2000)), McConnell's goal as DNI was to put cyber-security on the President's agenda (Kaplan, 2016, p. chap. 10). In order to do that, McConnell framed offensive CNA in terms of a digital 9/11: "if the capability to exploit a communication device exists, we have to assume that our enemies either have it or are trying to develop it" and if successful, such an attack could have the physical effects of 9/11 (Kaplan, 2016, p. chap. 10). He had a powerful argument. In March 2007, DHS tried to answer the question of whether a cyber-attack could cause physical destruction. During the so-called Aurora Generator Test at Idaho National Laboratory, the emergency circuit-breakers, designed for preventing a power-surge, were digitally manipulated. The 2.25 megawatt generator exploded (Kaplan, 2016, p. chap. 10). McConnell briefed Bush on the experiment. According to insiders, Bush got furious and said "We'll do another Manhattan Project if we have to" and gave McConnell "thirty days to fix it" (Harris, 2014, p. chap. 8). Of course, a highly complex issue such as cyber-security has no easy fix to it. Meanwhile, General Alexander and General Stanley McChrystal, head of Joint Special Operations Command (JSOC), the American Special Forces, already had their own plan.

They fused Special Forces and NSA hackers together to hunt down Iraqi insurgents. The problem at the time were roadside bombs, often detonated via cellphone calls (Kaplan, 2016, p. chap. 9). NSA got access to the large Iraqi telecommunication switches that handled Internet and cellphone data and was able to copy meta- and content data of all Iraqi communication (Nakashima & Warrick, 2013).[149] Correlating phone-call meta-data with maps allowed to detect self-made explosive devices. In other words, the US exported the technical artifact of UPSTREAM data collection and used it in another context (see chap. 4.4.7.3 Artifacts: NSA and the Full-take Norm of Internet Control (2001 -)).

American hackers from NSA's Tailored Access Operations[150] and CIA's Technology Management Office developed cyber-attacks to infiltrate computer networks, websites, servers and E-mail accounts of Al-Qaeda (its internal network was called Obelisk) and

[149] NSA struck a deal with Iraqi telecommunication carriers which gave it access to the fiber optic cables. "[…] by the time the 2007 surge began, NSA had put in place the spying infrastructure to collect every piece of electronic data going in and out of the country—every phone call, every text message, every e-mail and social media post" (Harris, 2014, p. chap. 1). According to one agreement, the carriers also had to implement an Internet kill switch: a technology to shut down all communications travelling through the countries. This kill switch technology is based on tampering with the Border-Gateway-Protocol that manages data transmission between two large IXP. According to insider reports, in 2010 DHS tested such an internet kill-switch in California but it remains unclear, whether the US has working Internet kill switches in place (Saalbach, 2015, p. 59). Shutting down a nation's internet would be one of the most intrusive cyber-attacks.

[150] TAO is said to be NSA's hacker elite, tasked with getting inside adversary networks, steal or crack passwords, implant spyware and backdoors. According to the Snowden files, TOA has implemented spyware in at least 85000 computers in 89 countries during 279 operations, as of 2010. (Harris, 2014, p. chap. 4). This organization is the physical manifestation of the fusion of cyber-war and surveillance.

other insurgents, tracking Internet activity of terrorists. With the help of metadata, analysts drafted social networks of insurgents that were communicating frequently with each other, just as envisioned with TIA. NSA hackers sent fake messages to known suspect phone numbers, arranging meetings just to arrest (or kill) the people who would show up. JSOC Special Forces planted electronic surveillance equipment such as key-loggers and other malware at suspects computers for further surveillance (Priest & Arkin, 2012, pp. 236-245). Offensive cyber-war tools also played a role in the assassination of targets with drone strikes, as Hayden (2014) once admitted by accident: "We kill people based on metadata" (Ferran, 2014). In other words, JFCC-NW, TAO, JSOC and other organizations were physical manifestations of the fusion of cyber-war, surveillance and kinetic wars.

But DNI McConnell successfully advocated for three other famous initiatives that marked the start of operational cyber-war, its fusion with surveillance and the rise of the cyber-realist paradigm (representing another instance of equifinality). The first is called Olympic Games (or Stuxnet), the second the FISA-Amendment Act of 2008 and the third the creation of US Cybercommand, which was completed under Obama. Stuxnet und US CYBERCOM will be discussed in more detail in the following chapters (see chap. 4.5.3 Practice: Professionalization of Offensive Cyber-War & Surveillance).

A key trigger or catalyst for these initiatives was an intrusion into classified, air-gapped DoD networks by an allegedly foreign malware, a self-replicating worm dubbed "agent.btz" in June 2008 (Brown & Poellet, 2012, p. 131). The fact that for the first time a classified and highly secure DoD network got hacked represented a shock that rang the alarm bells. Like with Solar Sunrise in 1998, the question was "who is in charge?" (Kaplan, 2016, p. chap. 10). NSA General Alexander saw an opportunity to "make NSA the military's new leader in cyberspace" (Harris, 2014, p. chap. 9). General Alexander lobbied that NSA was put in charge. He told a congressional committee that incident showed that offensive and defense capabilities should be brought together and that NSA would be best positioned to do the job, if he got more personnel and budget.

NSA's TAO was tasked with the defense operation called "Buckshot Yankee" to remove the malware and trace its origin. That NSA, and not DHS or any other organization was put in charge is described by insiders as an NSA "power grab" (Harris, 2014, p. chap. 9). In fact, the malware was well-known among private cyber-security companies and relatively benign. Malware analysts pointed to the fact that agent.btz also infected systems of the greatest adversaries (Russia and China) and was probably not a targeted attack at the Pentagon (G Data, 2015). This episode shows the imbalance of knowledge that is visible in the entire cyber-war discourse – because of classification and secrecy, many attacks and

practices cannot be analyzed independently and critically, which gives those agencies who maintain those secrets an advantage in proposing their message. The IC in that sense acts as "an institutionally distorting prism" (Herman, 2004, p. 345). In theoretical terms, the technical side of national security policy is a highly closed policy subsystem where only a few actors have access and insight. These actors sit in a special position of power and work as norm-entrepreneurs from within the executive. NSA Generals Hayden and Alexander and other cyber-advocates like DNI McConnell systematically framed this incident as an existential threat to the US (Harris, 2014, p. chap. 9). But this could not be critically evaluated by non-tech savvy decision-makers.

What followed was comprehensive a national plan by President Bush to increase cyber-security, announced in January 2008. Bush signed NSPD-54, which includes a language highly inspired by IW and cyber-war doctrine documents:

> "The electronic information infrastructure of the United States is subject to constant intrusion by adversaries that may include foreign intelligence and military services, organized primal groups, and terrorists trying to steal sensitive information or damage, degrade, or destroy data, information systems, or the critical infrastructures that depend upon them" (The White House, 2008).

To address this problem, all governmental agencies (and not just military ones) should focus on increased computer network defense. It defines CNA, CNE, cyber-security, cyberspace and much more. Formally, it designates the DHS as the lead agency which shall set-up a cyber-security center coordinating the various US CERT teams. Congress approved a budget of $17,3 billion, but most of this budget went directly to NSA because DHS neither had the resources nor the know-how. There were only a handful of network-security experts at DHS compared to NSA, which at the time, already had hundreds if not thousands of analysts charged with CND, CNE and CNA (Kaplan, 2016, p. chap. 10). This is more evidence for the power-grab thesis and shows how national security actors positioned themselves as dominant in cyberspace, thereby excluding civil or non-military responses to cyber-security issues.

Although the directive focused on CND, General Alexander began advocating for a broad interpretation of "defense". Narrowly defined, defense could mean Firewalls and intrusion detection systems, such as the DHS Einstein-2 program, a network-defense system designed to detect malicious code entering government networks. Alexander instead advocated for "active defense: penetrating an adversary's network to see what kinds of attacks he was planning, so that NSA could devise a way to disrupt, degrade, or defeat them preemptively" (Kaplan, 2016, p. chap. 10). The idea of active defense is a clear

fusion of the preemptive war doctrine, developed during the GWOT and the idea of information dominance, developed in the 1990s in the IW doctrine.

The last outcome was the reform of the FISA-system with the FISA-Amendment Act (FISAAA), adopted in July 2008. Again, it was DNI McConnell who took the initiative. The leak of Stellarwind in 2005 had sparked controversy over the legality of the NSA programs, collecting large portions of world Internet-traffic as it was passing through networks-switches inside the US (Lichtblau & Risen, 2005). Differentiating between foreign and domestic communications in the vast amounts of Internet packets – as FISA required – was technically and legally challenging, if not impossible. There was no sound way of guaranteeing that there were no domestic data-packets in this vast data-collection and thus 4th amendment rights of US citizens were not violated. With TCP/IP, it is virtually impossible to differentiate whether a packet is foreign or not (see chap. 4.1.3.1 Artifact: Internet Protocols and Norms). DNI McConnell convinced Bush of the necessity of the "full-take" data-collection of global Internet-data streams at domestic switches and urged him to "fix" legislation (Kaplan, 2016, p. Chap. 11).

As a result, Republican leaders in the Senate brought forward a bill that adjusted the FISA system with the new full-take surveillance practice in the digital age. McConnell adopted the "death of geography in cyberspace" frame to argue that the distinction between foreign and domestic could not be made anyway and therefore was too restrictive (Kaplan, 2016, p. chap. 11). FISAAA specified that electronic surveillance of American citizens would not be illegal (and not be called surveillance anymore) if it was aimed at a person "reasonably believed to be located outside the US." The clause "reasonably" is intentionally kept broad. A warrant request from now on would not need to specify the "specific facilities, places, premises or property" where intelligence collection would take place (U.S. Congress, 2008, p. section 701). This, again, widened the set of surveillance targets.

The bill also prohibited law suits against telecommunications providers and other companies (such as AT&T) facilitating the data-collection on behalf of NSA, giving them post-hoc legal "immunity from civil and criminal liability for any persons and companies" (Shorrock, 2009, p. chap. 9). The only legal protection of US citizens was the requirement to "minimize" data of US citizens discovered within the bulk-data collection, meaning the data had to exclude names of targets and the content of communications. Whereas under the old FISA law, data could be obtained and stored only if it was relevant for an investigation and if it could be shown that the target is a foreign power, the new law lowered standards again. Now, under section 702, it must only be shown that the target is a

"NON-USPER [non US person] located outside the United States" (Landau, 2013, p. 58).[151] It inverted the logic and the burden of proof: the bill defined everything as potentially relevant but in order to assess that, the data had to be collected first. Before, it was the other way around: relevancy had to be shown first before data collection could be initiated. It enabled NSA to collect the whole haystack of data; it legitimized the full-take principle and the norm of cyberspace control. It also inverted another legal principle in democracies: government practices have to be compatible with the law. In this case, the law was made compatible with NSA practices. Besides the usual civil liberty groups, few recognized this subtle, but massive change to the FISA system. There was not much of a public discourse. The Senate debated this bill only for two days until was adopted as law with a 60-28 vote (Kaplan, 2016, p. chap. 11).

In sum, during the second Bush presidency, domestic surveillance, foreign SIGINT and cyber-war capabilities became fused together, forming a coherent assemblage or a nexus that is hard to disentangle (mostly because of secrecy). Not only were the ideas of counter-terrorism with its focus on prevention and electronic surveillance (CNE) compatible with concepts of IW, especially CNA, but also were the policies and organizational structures similar and thus allowed convergence. The new intelligence gathering capabilities created with the PATRIOT Act were potentially useful for offensive CNA. The organizations doing counter-terrorism and CNA, like NSA, overlapped. Since electronic surveillance and offensive cyber-war are two coins of the same medal, it is no surprise that the creation of a powerful surveillance apparatus lead to the creation of a powerful cyber-war machinery, too. This enabled the fusion of the IW doctrine and counter-terrorism to form a coherent cyber-realist paradigm of the Internet. This also happened in the economi sphere, which can only be mentioned here briefly. Private intelligence contractors and cyber-security firms such as Northrop Grumman, SAIC, General Dynamics and Booz Hamilton saw a dramatic rise in revenue since 2001 (Shorrock, 2009, p. chap. 1). To further indicate this fusion, between 2005 and 2007 the term "information war" was replaced by the term "cyber-war" in military doctrine and other policy documents (Wilson, 2006). When Obama entered office in 2009, DNI McConnell instantly met with the President to lobby for the continuation of his plans, to which Obama agreed (Harris, 2014, p. chap. 3). Before we turn to that, we need to analyze the underlying norms and summarize the findings of this lengthy chapter.

[151] In contrast to European Charter on Human rights which grants privacy for every individual regardless of citizenship.

4.4.8 The Norm of Internet Control

Taken together, the epistemological and ontological ideas and problem definitions of cyber-realism led to a *definition of standards of appropriate behavior for state-actors with a national-security identity to engage with the Internet primarily through a militarized security logic.* This cyber-realist norm states that this new, uncontrollable medium *must be controlled*. This follows directly from the logic how IW was perceived in the 1990s and extended in the early 2000s: "Whereas the world wars used attrition (WW I) and maneuver (WW II), information age war emphasizes control" (Fast, 1997, p. 12). The Air Force argued in 1995 that: "Information is the next realm *we must control* to operate effectively and with the greatest economy of force" (U.S. Department of the Air Force, 1995). The technical and political measures put in place after 9/11 materialize this norm and thus are an instance of path-dependency.

Who should control cyberspace? In contrast to cyber-utopianism, cyber-realism is a state-centric paradigm: *the state ought to be a dominant actor in cyberspace,* controlling and monitoring it. This contests norms of the original Internet, which was designed to keep the state out. It was designed to be a decentralized, global infrastructure representing open commons that essentially belong to no single entity and to which no single actor has exclusive access or privileges, at least for now. Now, state actors claim special privileges such as the intrusion into another nation's information infrastructure and to exploit someone else's information.

Additionally, with cyber-realism *the Internet is predominantly understood as a national security problem* and less as an opportunity for democratic or economic development. The exhaustive problem definitions have shown this (see chap. 4.4.2.2 Problem Definitions of Cyber-Realism). More so, if information is perceived as a weapon, therefore it becomes a *means of power*: "power in the information age depends more on the ability to influence access and interconnection than on the capacity to enforce borders" (Fast, 1997, p. 10). The argument assumes that the more information one possesses, the more power can be accumulated. It is no accident that the seal of the Total Information Awareness Office had the slogan "knowledge is power". Here it becomes clear why the paradigm is called cyber-realism. Realism as an IR theory predominantly operates with an understanding of power as a resource – the more resources (i.e. tanks, military personnel, GDP or even CNA-capabilities) a nation has, the more powerful it is compared to those who have less (Baldwin, 2012). Cyber-realism assumes a direct correlation between information and power. If information is perceived as just another resource or weapon category, the ultimate aim becomes to gather more information. The general logic of this

paradigm is – the more information,[152] the better the command and control, the more powerful one gets, the higher the chances of winning a war. ICT and computers play a crucial role in this logic because they elevate the aforementioned functions to a new level.

The norm of Internet control defines the *appropriate action as the preemptive, "full-take" data collection*. Mass acquisition of information is a means to the end of information superiority. The key idea of "bulk data collection" or in other words, the "full take principle" or "big data"[153] is conceived as early as the mid 1990s but becomes dominant in the GWOT. The GWOT added the notion that mass data collection should happen preemptively, to prevent a potential terrorist attack. The full-take principle can be conceptualized as an emerging norm within Internet governance that is highly taken for granted and many countries are trying to replicate it.[154] It presumes that, *because of national security concerns, it is appropriate for states to gather all kinds of data* (that might belong to other states or private actors such as intellectual property, patents or private communication) of the global Internet traversing its physical territory and beyond, regardless of whether this data is of domestic origin or not. A consequence of that is that data accumulation will have no logical end. Cyber-realism strives for *total* information awareness and as such includes totalitarian aspects.

But there is another aspect of the norm of control. The fusion of intelligence and cyber-war leads to another definition of appropriate action: states claim the appropriate right to not just monitor, but alter, manipulate or destroy data and information stored in another country's networks. Cyber-realist advocates argue that this is appropriate behavior. It is also a taken-for-granted, unquestioned belief.

At the same time, the norm of Internet control is a dark norm because it contests several other norms in liberal democracies that were established to prevent abuses. First, it contests the norm that a severe measure such as surveillance requires a probable cause or a concrete suspicion before it is initiated. It turned the traditional legal principle *mens rea* upside down. This is the legal principle that "criminalization must be based on a specified criminal act" (Amoore & de Goede, 2008, p. 67). Instead, counter-laws are "'laws against law' or 'zero-law', by which legislation pursues harms that are *finus reus*: they act against a mere possibility of harm and explicitly undermine conventional legal principles" (de Lint & Kassa, 2015, p. 361). With the norm of control, suspicion is generated after intelligence is gathered and analyzed for terrorist affiliation patterns for example. Second, mass

[152] Rona mentioned in 1976: "The value of the exploitation is therefore cumulative; once we have extracted data to the opponent's information channel, further exploitation is facilitated" (Rona, 1976, p. 35).
[153] Colonel Fast speaks about "the value of "big information" as the source of power" (Fast, 1997, p. 18).
[154] In the years since Snowden, France, the United Kingdom, Russia and Germany have adopted laws that allow full-take collection of fiber optic cable content and metadata.

surveillance without suspicion contests the norm that severe surveillance measures should be targeted and that data of innocent individuals should be protected. The "full-take" surveillance approach necessarily catches data of innocents. Third, the "full-take" principle harms the distinction between foreign and domestic surveillance targets (which are protected by civil-liberties). Fourth, the unitary executive theory and the FISAAA reversed the idea that intelligence agencies had to follow the law. Instead, it established the precedent that the law was altered to legalize controversial practices post-hoc. Fifth, Internet control of both domestic and international data blurred the separation of powers and checks and balances that were put in place to prevent the formation of an almighty secret police. With the post 9/11 legal changes, NSA became judge, jury and eavesdropper at the same time (Bamford, 2009, p. 119) and with cyber-war, even a combatant in war. Additionally, no probable cause can be given when monitoring the entire Internet – potentially everyone becomes a target without any prior suspicion. NSA once was a marginal intelligence agency and now it is the most powerful agency in the world.

It is important to state that the norm of control developed out of a particular idea of cyber-realists, namely "that more information characterizes better judgment, and that therefore *more raw information to fill their gaps is their greatest need*" (Honig, 2010, p. 54). This *particular* interest of intelligence agencies became reformulated and framed as a *general* strategy in the war on terror that encompasses all sectors of society, which represents a hegemonic practice in terms of discourse theory. The intelligence reform of 2004 reshuffled the entire security apparatus and the 2008 FISA Amendment Act fulfilled the goal of making make data from the lowest to highest levels of society accessible. This also indicates a shift in actors: whereas IW was coined by the military, now the IC became positioned as the dominant cyber-realist actor.

It is important to note that cyber-realism could become dominant only because of the state of emergency directly after 9/11, pretty much in line with the predictions of the securitization framework. Total control of Internet data streams originally was an extraordinary measure adopted in an emergency situation after 9/11. However, over time this extraordinary measure became reified and normalized within the practices of the intelligence community. To monitor global data streams is now deeply taken for granted. This might be problematic, as the next chapter will show.

4.4.9 Critical Analysis of Cyber-Realism

Like with the other paradigms before, a critical discussion of the ideas is in order. The developments described in the previous chapter introduced several legal and political

dilemmas. For example, the goal to prevent human suffering in form of terrorist attacks is clearly understandable. It is also quite logical that more and better intelligence is needed to prevent attacks. The question is where legitimate needs cross a line and become too radical. That cannot be easily rectified. Therefore, this chapter introduces a critical discussion of some of the developments outlined in the previous chapters.

Cyber-realism is based on a simplistic understanding of knowledge generation, namely that having all the facts matters and that the facts speak for themselves. However, scientists know that "facts never speak for themselves" because data must be interpreted, analyzed and enriched with theory. The central problem here is bias. There is strong empirical evidence that intelligence failures often happen not because of lacking data, but faulty, biased analysis, like for example the political instrumentalization of intelligence estimates like with the WMD in Iraq 2003 (Rovner & Long, 2005). Bar-Joseph shows that in numerous cases, from Operation Barbarossa, Pearl Harbor, the Korean War to the Iranian revolution, "the source of the problem is not insufficient information about the looming threat, but rather the misinterpretation of the meaning of the available information" (Bar-Joseph, 2010, p. 24). Reporters counted that in many major terror attacks within Western countries in the last 10 years (from Paris to Boston), the suspects were already known to intelligence and law-enforcement agencies (Gallagher, 2015a). Even without new data-collection powers to sift through the entire Internet, intelligence already was available. Intelligence experts convincingly argue that too much information can lead to overload and perception biases, which result in faulty interpretation (Jervis, 2011). As it was shown, the dilemma of information overload was NSA's problem number one that led to the inception of Trailblazer in the first place, even at a time where it could not wiretap the Internet (see chap. 4.4.7.3 Artifacts: NSA and the Full-take Norm of Internet Control (2001 -)).[155] NSA collected 200 million pieces of intelligence per day in 2002 and could only analyze 1 percent of it (Lee, 2015, p. 28). According to the Snowden files, NSA now collects 97 *billion* pieces of intelligence in a 30 day period both domestically and globally (Greenwald & MacAskill, 2013). It is unclear how much of it NSA can analyze. Even with more data, the problem of biased interpretation, however, is not going away. The higher the complexity and quantity of data, the higher the chances for intelligence failures (Rovner & Long, 2005).

This problem increases with automated information processing techniques. Mathematician Kurt Gödel argued that any mathematical model representing reality (and

[155] Knightley shows that information overload is in fact the reoccurring theme with most intelligence agencies (Knightley, 2003, p. chap. 16).

trying to predict the future) would be either incomplete (perfect information is an illusion) or have paradoxes, or both. Every model is a reduction of reality and therefore incomplete by design, which is the reason why information systems cannot be perfect (Hables Gray, 2003, p. 206). Total information awareness is probably not possible. The "father" of the modern general computer, Alan Turing, showed that Gödel's law applied to computing machines in general. The perfect computer and the perfect algorithm predicting future behavior is also impossible, but cyber-realists believe in this very idea. There is another factor that makes prediction impossible and which is an explanation for the fact that even with the large intelligence apparatus, US agencies are rarely able to prevent attacks like the Boston marathon bombing or other amok incidents. The so-called fog of war, that total information awareness wants to eliminate, cannot be lifted because it is not a physical problem, but a logical one. Uncertainty, or to know the enemy's intention or where an attack might happen is generated by three complex components that are always present: the antagonists' behavior, one's own behavior and random chance (or nature). These problems are unpredictable and not controllable by current mathematics (Hables Gray, 2003, p. 205)

More so, automatic systems of information processing can be intentionally overloaded with false information by enemies, generating many false positives, a problem that indeed did plague Thinthread: "there were too many false positives, indications of something of intelligence value when that wasn't really true" (Hayden, 2016b, p. chap. 5). Besides internal errors, "a potential attacker could deliberately spew out large amounts of information to overload the opposing system and thus create confusion and delay in decision-making" (Knightley, 2003, p. chap. 15). This possibility lies at the very core of the information warfare doctrine and is practiced with great success by current day Russia with its hybrid warfare (Geers, 2015).

A question that is always hard to answer is how effective this bulk data collection is. It is in an important question considering that the costs of the entire US terrorist prevention operation are estimated at annually $80 billion, or $1 trillion between 2001-2015 (de Lint & Kassa, 2015). De Lint and Kassa argue that in terms of a cost-benefit analysis that was demanded by the 9/11 commission report, the GWOT and the counter-terrorism policy in general is a failure and the question arises whether the little gains in security are worth the enormous spending (de Lint & Kassa, 2015, p. 358). In contrast to law-enforcement, in the intelligence world there are no single smoking-gun indicators linking a piece of data to a crime, but more often intelligence is "like a tapestry with multiple threads woven into a beautiful whole" (Hayden, 2016b, p. chap. 5). This makes it hard to pinpoint the effectiveness of one single tool. However, IC officials regularly argue that these programs

are effective, necessary and legal. For example, when Stellarwind was on the brink of being canceled in 2004 after the DoJ discovered it, Hayden repeatedly called it an indispensable and "most effective tool in our arsenal" while unofficially acknowledging that without it, NSA would only loose 20% of its overall effectiveness (Hayden, 2016b, p. chap. 5).

Another component of this norm is naive *technological determinism*, i.e the "view by some that more technology will always make 'better intelligence collection'" because it is believed that data mining and Big Data algorithms can be used to identify "footprints of a terrorist in the data ahead of an attack" (Walsh & Miller, 2015, p. 9). While Big-Data algorithms indeed hold some promise, it can result in the blind belief in data. However, Big Data also has its limits because human behavior always has a random component that cannot be programmed in advance. More so, the over-reliance on electronic forms of surveillance often leads to a downscaling of human intelligence – the use of agents and informants in different regions (Russell, 2007, p. 75). Human intelligence is necessary to make sense of signals intelligence (Rid 2013, chap. 6). It is also necessary to capture hard to reach targets. One of the reasons why it was so hard to find Osama bin Laden in his hideout in Pakistan was that he did not use any form of electronic communication at all but relied on human carriers. History is full of examples where SIGINT was blind because human carriers were used.[156]

While terrorist prevention might be a legitimate goal, the practice that was introduced by the Bush administration after 9/11 is somewhat radical and potentially totalitarian in its approach.[157] The goal of total information awareness cannot logically be reached. However, "full-take" surveillance practices nevertheless try to reach this goal. The quest for more information has no logical end. It also implies that intelligence agencies will always lobby for more and more capabilities. But these capabilities clash with legal principles.

The general disregard of the unitary executive against legal checks and balances (such as the FISC in the early days of the NSA program) and the weakening privacy and civil-liberty safeguards is a problematic trend have become normalized since 9/11. Cyber-realism has the tendency to contest central norms that were taken-for-granted within democratic systems, such as the distinction between law-enforcement and foreign

[156] Lyman Kirkpatrick, a former British intelligence officer argues "If the Soviets ever decided to go for broke, they wouldn't put anything on electronic communications or do anything visible by satellites. All the orders would go by officer couriers, which was what Hitler did at the Battle of the Bulge and caught us totally unprepared. We were relying too heavily on communications intelligence" (Knightley, 2003, p. chap. 15).

[157] If we define totalitarian ideas consisting of seeking control over all aspects of public and private life of a society by a state.

intelligence gathering and the implementation of congressional and/or court oversight. It is important to remember that these legal checks and balances that are contested by cyber-realism were put in place to prevent the abuse of power, to prevent an all-powerful secret police like the Gestapo or Russian KGB that could be exploited by an authoritarian president (Heller et al., 2012). These checks and balances also are what differentiates intelligence agencies in Western democracies from those in authoritarian regimes. With the dismantling of many of these safeguards, authoritarian and democratic intelligence agencies became a bit more similar to each other.

This is particularly problematic when these intelligence agencies become judge, wire tapper and combatant at the same time within the field of cyber-war. As was shown, the official US Doctrine is actually surprisingly transparent about the designated target of information and cyber-war (U.S. Air Force, 1998). Targets include enemy heads of states as well as leading economic and social figures, but in principle, all vital functions of a state are targets of IO – energy and financial infrastructure, manufacturing, telecommunications. This is another totalitarian idea because it basically targets everything within a society and particularly critical infrastructures that guarantee the basic operation of a state. It is noteworthy that both original thinkers of IW, Rona and Rechtin, warned of the implications of the IW concept for democratic states (see chap. 4.4.2 Ideas: Formation of the Information War Doctrine (1976-2000)). Rona asked, "how does an "open" society, with its emphasis on freedom of information and public scrutiny, protect its interests in a hostile world suffused with long-term moves and countermoves of the information war?" (Rona, 1976, p. 4). For Rechtin, it was not a surprise that a totalitarian country such as Soviet Russia would firstly discover IW because of their "pervasive use of information control" (Rechtin, 1983, p. 31). A report to Congress highlights the ambiguity of this trend and asks for the development of a legal framework for information war (particularly psychological operations) against the own population (Wilson, 2006).

In sum, cyber-realism includes some controversial ideas that actively contest standards within liberal democracies but also in terms of international law and best practices.

4.4.10 Summary

The Bush administration, upon entering office, initiated another instance of paradigm-change via regime change. Had Gore won the presidency, we most likely would have seen a continuation of the Information Superhighway agenda. The *structural composition of the Bush administration* is a necessary condition for the dominance of cyber-realism (part 1).

Several proponents of information war and mass surveillance occupied key positions within the administration, thus shaping the post 9/11 political agenda with cyber-realist ideas. The role of Vice President Cheney and path dependency is important here, because Cheney had a personal policy agenda regarding the FISA court. 9/11 presented a shock that was framed as an extraordinary circumstance that allowed the expansion of presidential power as commander-in-chief and potentially the contestation of liberal norms (Heller et al., 2012). Controversial ideas and policies that existed before 9/11 were reformulated as solution strategies to the problem, including expansion of the executive authority, restricting oversight over surveillance activities, more secrecy and generally the use of extraordinary measures such as suspicion-less mass surveillance. Reframing 9/11 as a war-situation could legitimize that "the gloves come off". This is a classical example of securitization. This was possible because the crisis situation represented a window of opportunity producing a rally-around-the-flag effect that limited political resistance to legal measures such as the Patriot Act. The 9/11 attacks represented the central shock moment and trigger that initiated a completely new path trajectory for cyber-realism. This has two interlinked components.

First, it allowed the expansion of cyber-realist ideas. Besides this regime change, there also came a gestalt switch, a replacement of dominant paradigms with the war on terror. The *GWOT and national security became the dominant narrative and (technological) frame of reference for understanding the Internet (part 2).* Over time, it replaced the utopian or economic perspective of the previous administration. The diagnosis and the sense-making of the terrorist attacks uncovered a central problem definition: finding an enemy hidden against the backdrop of civil society that also used the Internet to coordinate the attack. The problem of domestic sleeper-cells legitimized the idea that the foreign intelligence and information-gathering apparatus had to be turned inwards. This *resonated* with the IW belief that more information could be used to lift the fog of war.

These ideas got amplified by the increased focus on *preemptive* action and terrorism-*prevention*, a new key goal derived from the aforementioned problem definition. The desire to predict actions of individuals, to penetrate their thinking, as it was called, also resonated well with the idea of information superiority. A key means to realize this goal was the need-to-share norm that intelligence agencies should make their databases available to each other, sharing information per default, instead of a need-to-know basis. The definition of the "*war"* on terrorism expanded the battlefield. The Internet itself became defined as a problem, because it was perceived as a safe-haven for terrorists and an amplifier for radical propaganda and recruitment. It became a target and battle-space, the

fifth domain in the war on terrorism. In sum, the new counter-terrorist doctrine and the IW doctrine were highly compatible in their goals and means to achieve these.

Cyber-realist ideas became central to the counter-terrorism strategy of the US and became embedded into politics and technology (part 3). The Patriot-Act, the Intelligence Reform of 2004 and the FISA-Amendment Act of 2008 are instances of cyber-realist inspired policies that defined new instruments and settings to realize the aforementioned goals and thus represent a third order policy change. These laws also include (legal) norm change, dismantling the separation of intelligence and law-enforcement agencies, expanding their surveillance or information gathering powers by giving them broad access to new data-sources such as telephone and Internet communication streams. These laws were designed to gather as much domestic and international information as possible and to allow the sharing of this information between agencies.

Cyber-realist ideas led to the *creation of new technical artifacts.* NSA, one of the main impact constituents of the Internet, used the window of opportunity to lobby for new powers and to present itself as the first line of defense in the war on terror. For NSA, packet-switched Internet communication over fiber optic cables presented a major problem for its global SIGINT capacities. This diagnostic frame drove the problem solution in terms of Internet and communications data collection on a large scale, a plausible way to overcome surveillance issues introduced by TCP/IP. NSA accelerated the development of new surveillance technologies that it deemed to be illegal under normal circumstances, but appropriate within the extraordinary context of the war on terror. The goal of these programs resonated well with the goal of information superiority and the concept of Total Information Awareness program. The aim became to "master" or "own" the web, piercing through the veil of anonymity or the fog of war created by packet-switching and thus becoming aware of information transmitted over, or stored in these networks, just as the IW doctrine envisioned it in the 1990s. In theoretical terms, NSA *engaged in the technical reconstitution of the Internet*, building new technical counter-artifacts to address the problem of packet-switching. These artifacts tried to establish control and centralized intelligence in a network that was designed to have none. With this practice, NSA materialized the norm of Internet control with technological artifacts, i.e. the multiple surveillance programs. The norm states that it is appropriate for states to monitor and control potentially all information (full-take principle) traversing the global Internet infrastructure, regardless of foreign or domestic territory, origin, time (peace and war) and without the need for probable cause or prior suspicion. This represented a major norm change in American intelligence practices since the creation of FISA, which had actively

prohibited broad, suspicion-less full-take surveillance in the past. The executive framed this as appropriate because the war on terror legitimized such extraordinary measures, but chose to keep it secret nevertheless. The creation of these artifacts increased their staying power and initiated a path-trajectory towards offensive cyber-war.

While this originally was a passive SIGINT collection, *the offensive value of this information became relevant in the context of the war in Iraq 2007 (part 4)*. Particularly Secretary of Defense Rumsfeld systematically began to fuse the new counter-terrorist and intelligence-strategy with the older concept of IW, arguing that information operations and computer network attacks should utilize the vast SIGINT collection. The fusion of SIGINT or surveillance and cyber-attacks can be explained with the technical similarities of these functions. In other words, once capacity A exists, B follows logically. Personal continuity of cyber-realist advocates that had been socialized either within the Intelligence Community or in one of the IW centers in the 1990s (like General Alexander or DNI Michael McConnell) also played a role in this fusion. They developed IW ideas further. This included the notion of pre-emptive attacks, the idea to destroy physical objects with cyber-attacks (Aurora Generator) and the fusion of SIGINT with kinetic or signature-strikes from UAV. The war in Iraq showed the utility of these concepts, which increased their staying power.

In 2008, a shock situation happened inside the national security apparatus that accelerated the already established trajectory. The agent.bz malware penetrated secure DoD networks and caused a certain anxiety within military circles. NSA lobbied heavily to be put in charge by framing this cyber-attack as an existential threat to the US that potentially could worsen in the future (security master frame). Because national security is a relatively pre-structured and closed-off policy subsystem with little transparency, NSA could plausibly argue that no other agency had the same skills and computer-literacy. This points to an under-theorized factor: turf-battles between political bureaucracies are a key explanation here. NSA had several advantages compared to other agencies like DHS. NSA already had institutionalized cyber-security procedures and thus skilled personnel since the mid-1990s. Cyber-security and cyber-war developed as a military or intelligence practice, which means great secrecy and classification. This excluded non-military actors (like the later DHS) from the turf and increased the standing of NSA within the intelligence community. *NSA used this upgraded standing to lobby the White House for a more aggressive posture in cyber-space, arguing for active defense and thus an expansion of the global surveillance and hacking of foreign IT-systems to preempt cyber-attacks* (part 5). G.W. Bush lacked computer literacy and was uncritical towards these suggestions. Policy

reforms were by advocated former information warrior DNI McConnell, including the suggestion to retrospectively legalize the full-take surveillance effort, which led to a minor policy scandal in 2004/2005 with the FISA Amendment Act of 2008. McConnell also argued for an increased cyber-security spending and the creation of a unified command structure, the US CYBERCOM, which Bush acknowledged. This part of the mechanism shows how path-trajectories initiated during the IW era of the 1990s (institutionalization, continuity of personal, ideas, procedures), became relevant at a later point in time.

Timing, again, is an important conditional factor. In the last years of the Bush presidency, and particularly with major computer network incidents like Estonia 2007, Operation Orchard 2007 and Georgia 2008, the whole issue of cyber-attacks and the general notion of cyber-security and hacking got a greater salience among policy-makers and the general public. This has to do with increased Internet penetration and the beginning smartphone revolution, giving even more people access to the Internet and enough literacy to comprehend the issue, at least to some degree.

It can be argued that the legitimization of offensive hacking and surveillance with GWOT became a meta-narrative that quickly became dominant in the years after 9/11. Extraordinary measures such as intruding into another country's networks or copying data-streams and potentially the entire Internet were legitimized with the 9/11 shock and then got normalized over time. But these practices are extraordinary since they contest central liberal democratic principles such as the separation of powers and civil-liberties (4th amendment). Terrorism has been used as the key legitimization figure for enhanced securitization in many countries, representing a global normative impact or the partly diffusion of some of these norms, including the norm of Internet control. In other words, the *outcome of this mid-2000 process is the stabilization of the norm* that the state, through its intelligence apparatus, has the legitimate right to sift through Internet data streams, even in other countries beyond their jurisdiction. While President Nixon got impeached during the Watergate scandal for using intelligence agencies for domestic surveillance, we nowadays take it for granted that intelligence agencies from around the world might monitor Internet surfing. The norm of Internet control is closely tied to the war on terror narrative, which is one of the most influential policy narratives of our time. It has a great interpretative flexibility (there are numerous ways how to fight terrorism), commensurability (there is an enemy to pin-point), and narrative fidelity (the civilized West vs. "barbaric" radical Islam) and this is likely to stay this way.

But there might be another argument for the stabilization of the norm. Once technology and supporting laws are put in place and bureaucracies are built, they have an

enormous staying power. This creates strong structural incentives to maintain the technology, policy and the narrative. To abandon the GWOT and dominance of the IC with its technical artifacts to fight terrorism would mean to waste a lot of money (Trailblazer and similar programs had cost billions) and to lose available tools of state power that might be useful in scenarios other than terrorism (inter-state espionage for example). In other words, the constructed technological artifacts to fight terrorism create a structural mechanism that increases the likelihood of their continuation (path-dependency). This is also facilitated by a whole industry of private intelligence contractors, security providers (like Blackwater) or arms-manufacturers that earn well with fighting terrorism. Cyber-realism in a sense, created its own economical side arm much like cyber-utopianism spread into economics and business in the 1990s.

Table 6. Causal Mechanism of Cyber-Realism during the 2000s

Context	9/11 shock and the failure of cyber-utopianism with Y2k and dot-com crash.
Part 1	Election of Bush administration with its structural composition of cyber-realist hawks plus 9/11 emergency situation *enable* controversial cyber-realist ideas to be put on the post 9/11 agenda.
Part 2	Cyber-realists *frame* the Internet predominantly in national security terms and *lobby* for policy and technical changes to counter perceived problems. Advocacy for the norm of Internet-control which strongly resonates with the old IW doctrine.
Part 3	PATRIOT Act and other policies *materialize* cyber-realist ideas and enable the *goal-oriented construction* of controversial Internet surveillance programs designed to counter problems created by TCP/IP. This enables a path-trajectory.
Part 4	*Fusion* of new post-9/11 mass-surveillance (CNE) capacities, technologies, policies and ideas with offensive computer network capabilities and IW, particularly in Iraq 2007.
Part 5	Rapid succession of cyber-security events (Estonia 2007, Buckshot Yankee) accelerate the cyber-realist path-trajectory and increase salience. Constant advocacy of socialized cyber-realists for new competencies and institutionalization.
Outcome	Further legal (FISAA) and organizational (USCYBERCOM) changes *establish* the NSA as the dominant state-bureaucracy in cyberspace. Idea that states ought to control/monitor global Internet data streams becomes *normalized* and unquestioned over time (norm stabilization among elites).

The next chapter will introduce changes during the Obama administration. This episode is interesting because Obama was initially skeptical about these new surveillance powers and during the election it looked like he might alter the over-extensive practices of the Bush administration. Once in office however, he kept most of the new surveillance and cyber-war technologies created by his predecessor.

4.5 From Cyber-Utopia to Cyber-War: The Obama Presidency (2008-2013)

"I could have added that the cyber domain has never been a digital Eden. It was always Mogadishu."
General Michael Hayden

This chapter exemplifies the normative change this thesis is about: From digital Eden to digital Mogadishu, as NSA General Hayden frames it. It is the culmination of the paradigm competition and the finalization of norm change from cyber-utopia to cyber-war or realism. The Barack Obama administration can be seen as a critical juncture where the future path of the norm of control was decided. The options were continuity of cyber-realism developed under Bush (which probably would have happened if Republican candidate John McCain had won the 2008 election), or an abandonment or correction of this path, which Obama indicated in his utopian election campaign. Thus, the Obama victory opened up the possibility of changing the established path-trajectory, reducing the impact of cyber-realism.

The analysis again focuses on the political level, analyzing political documents such as national strategies, election campaign material, official communications and speeches done by different parts of the administration. However, it also includes the military side of things in order to assess which paradigm is dominant within this administration. Methodologically, I screened key Internet-related documents of this administration, checking for congruence with cyber-realist or utopian ideas. This was not an easy task, since the Obama administration shows a duality between utopianism and realism.

The general temporal succession of the chapter is congruent with the rest of the thesis. The Obama administration is a hybrid-presidency, where both realist and utopian ideas overlap. I explain this in the next chapter (see chap. 4.5.1 Background: The Hybrid Presidency). This demands a slightly different chapter structure that emerged inductively out of the empirical analysis. Because of this hybrid-nature, I first focus on utopian *ideas* that Obama developed during the election campaign and that became partly realized in the Internet freedom agenda (see chap. 4.5.2 Ideas: Cyber-Utopianism under Obama and Clinton). Then I argue that the cyber-realist *practice* of this administration does not fit 100% with this cyber-utopian campaign. To keep the chapter structure simple and to highlight the duality between utopian rhetoric and realist practice, I talk about cyber-realist inspired policies, strategies, artifacts and institutions in one single chapter (see chap. 4.5.3 Practice: Professionalization of Offensive Cyber-War & Surveillance). This is justified because all of these form a tightly knit nexus. This is a crucial chapter because it shows the professionalization and normalization of cyber-war.

There is another novelty. For the first time, this section will introduce a distinct chapter on discourses to highlight the dominance of cyber-realist thought in the public domain (see chap. 4.5.4 Discourse: Cyber-Doom and the Hegemony of Cyber-Realism). This further indicates the normative change that is taking place under Obama. Observe that I do not conduct an individual discourse analysis, but mostly rely on summaries of discourse analyses done by other scholars. The function of this chapter is simply to show the overall societal impact of cyber-realist frames in public discourses.

Then I turn to another juncture, the leaks of Edward Snowden, which actually spans two chapters. First, I focus on the technical artifacts that NSA and others constructed in the war on terror to reach the aim of information dominance, developed within the context of IW (see chap. 4.5.5 Artifacts: The Snowden Leaks). The structure of this chapter follows the analysis of other technical artifacts, looking at goal-oriented construction, embedded norms and technical affordances at a handful of leaked programs. This is a technical but important chapter because it shows what the norm of control technically entails and means. The other chapter focuses on the outcome of the Snowden leaks in terms of political reform (see chap. 4.5.6 Juncture: The President's Panel on NSA Practices). This chapter addresses the President's panel that was tasked to evaluate the Internet mass surveillance practices and to formulate reform ideas. I will analyze this report in high detail, focusing on critical arguments and suggested reforms. My argument is that Obama did only follow a few minor recommendations of the report, which is smoking-gun evidence for the dominance of the cyber-realist norm of Internet control that now has become fully established. Like before, the chapter concludes with a critical discussion (see chap. 4.5.8 Critical Analysis) and a summary of the causal mechanism (see chap. 4.4.9 Summary).

4.5.1 Background: The Hybrid Presidency

The purpose of this chapter is to characterize the Obama administration and to understand the structural constraints and background that facilitated its policy decisions. This is important because the Obama administration cannot be as easily described as the Clinton/Gore administration (which clearly was cyber-utopian) and the cyber-realist Bush administration. The Obama administration is a hybrid between the two along two dichotomies: first, continuity vs. change in the general strategic framework of the GWOT and second, an election campaign and a foreign policy driven by cyber-utopian ideas facing the realities of institutionalized cyber-realism when entering office.

The first dichotomy describes the general continuity and path-dependency of the Obama national security policy in the war on terror, but refined in nuances (Renshon,

2009, p. 4). For example, Obama limited the scope the GWOT as a foreign policy matter of reduced importance (compared to Bush). It was reframed as an issue that did not require a mobilization of *all* instruments of national power, but only a selected few. Obama avoided the terms *global* and *long* war on terrorism (of uncertain duration) and spoke of a more limited "war against Al-Qaeda" (Starr-Deelen, 2014, p. 174). However, the focus on terrorist prevention and the overall idea of the global battle space (homeland and cyberspace) was maintained. A heavier emphasis was given to counter-insurgency in Afghanistan as the main battle space in the GWOT, and troops were withdrawn from Iraq (Onea, 2013, pp. 150-151). Only special- and training forces stayed behind, marking the shift from quantity to quality. The reason for the overall continuity is that big ships such as the US national security policy are slowly to maneuver. Many policies and reforms adopted by the Bush administration exhibited inertia and their effects became visible only during the first Obama term (like the establishment of US Cybercommand and offensive cyber-war programs that became ready under Obama). Path-dependency is a key explanatory factor for the continuity under Obama. Kaufman argues: "Obama inherited a United States that was economically troubled, militarily overstretched, politically polarized, and diplomatically estranged from world public opinion" (Kaufman, 2012, p. 12). Especially the economic crash of 2008 forced Obama to prioritize domestic policy (Obamacare) and to stabilize the US economy, which reduced his flexibility in national security politics and created a demand to effectively use the resources that were already in place: quality had to replace quantity. This explains the heavier use of special forces under JSOC like Navy Seals, UAV signature drone strikes and offensive cyber-attacks such as Stuxnet, which are all more punctuated tools compared to large armies.

The second dichotomy, cyber-utopianism as a candidate versus cyber-realism as President is more interesting. First, compared to Bush, Obama is described as technologically savvy or even a tech-enthusiast. Obama embraced the Internet and particularly the social media revolution of Facebook (est. 2004) and Twitter (est. 2006) quite early during his election campaign. The campaign heavily used new social media such as Twitter as well as big-data mining techniques. He was the first presidential candidate to tweet (Lee, 2015, p. 184). Interestingly, the campaign was also targeted by a cyber-attack through which perpetrators stole campaign files (Glendinning, 2008). More so, the election campaign on "change" embraced many cyber-utopian concepts, such as support for net-neutrality, digital privacy, transparency and more. These utopian ideas influenced early policy and stood in opposition to cyber-realist concepts. The personal

background of the President is one explanatory factor for the high priority given to cyber-security and cyber-war during his administration.

Another factor is the general timing of the campaign that coincides with major technological milestones in the history of the Internet (see Table 9. List of Internet Milestones and Security Incidents). Examples are the smartphone & social network (Web 2.0) revolution since 2007, which expanded the prevalence of the Internet into everyday life and the launch of the first Big Data, cloud-computing and Artificial Intelligence platforms that accelerated digitalization. New York Times columnist Thomas Friedman calls the year 2007 the "single greatest technological inflection point since Gutenberg invented the printing-press" (Takahashi, 2016). There is an equifinality of factors at work here. Mobile technologies expanded the use of the Internet globally. When Obama entered office in 2008, Internet penetration in the US has reached about 70% and 23% worldwide. When Obama left office in 2016, 40% of the world was online (see appendix Quantifying the Internet and the Digital Revolution). Particularly smartphones opened up the Internet for new user groups from the Middle East and developing countries, which was a facilitating condition of the 2011 Arab spring. The number of Internet devices skyrocketed and thus the potential vulnerability in these systems grew. During that time, a series of cyber-incidents happened that are often described as wake-up calls in the IC (see chap. 4.4.7.4 The Fusion of IW, Surveillance and Cyber-War (2003-2008)). These events raised awareness inside the cyber-security community. All that explains why the Obama administration jumped the cyber-hype bandwagon quite quickly.

Third, the Obama administration's perspective on the Internet is not as unitary and simple as the Bush administration’s, which was structurally dominated by cyber-realist thinking and framed cyberspace-issues in terms of the GWOT. Obama's Internet policy is more complex, nuanced, even contradictory because of different actor preferences. When entering office, the Obama administration revoked some of the controversial emergency measures such as the CIA Greystone torture and rendition program. President Obama also restored some of the IC oversight functions in the White House that were eliminated under Bush (Lepri, 2012, p. 77). However, the increased surveillance apparatus and its legal framework was left mostly intact controversial Patriot Act sunset provisions were extended in 2010 and even expanded by Congress in 2011, with strong presidential support. Obama affirmed the idea that connecting the dots could prevent terrorist attacks after the Christmas Day bombing attempt in 2009 (Lepri, 2012, pp. 70-73). Obama also extended the US cyber-war efforts, increasing its capabilities, budget, personnel and skills, and (allegedly) ordered the first large-scale cyber-attack against Iran. Additionally, the Obama

administration expanded the scope conditions of cyber-war, enabling retaliatory action and physical counterstrikes to CNA, which is seen as highly controversial. The Snowden disclosures in 2013 shed light on the state of the art of US Internet control practices. Obama's handling of the Snowden revelations revealed the gap between his rhetoric of cyber-utopianism and his practices of expanded, professionalized cyber-realism (with the creation of a unified military command, new cyber-weapons such as Stuxnet and the clandestine drone wars). Although he created a commission to evaluate NSA practices in 2013, he did not follow its recommendations and just made minor adjustments. This can be seen as proof that cyber-realism became indeed hegemony under Obama.

4.5.2 Ideas: Cyber-Utopianism under Obama and Clinton

The Internet-driven election campaign of Barack Obama embraced many cyber-utopian ideas such as the *free flow of information*, the *democratizing and economic potential of the Internet* and the demand for *net neutrality.* This chapter will analyze some noteworthy key election speeches and campaign documents that showed a heavy focus on Internet-related issues. I will proceed much in the same manner as the other chapters that focused on ideas, analyzing paradigmatic problem definitions and technological frames describing the Internet.

During the campaign in November 2007, Barack Obama and Joseph Biden launched their vision of technology called "Connecting and empowering all Americans through technology and innovation" (Obama, 2007). They want to "harness the power of the Internet to transform government and politics", making the government more transparent, accountable and allowing citizens to participate more in the democratic process. The core aims are: to "ensure the Full and Free Exchange of Information through an Open Internet and Diverse Media Outlets", including aims such as "Protect the Openness of the Internet", "Encourage Diversity in Media Ownership", "Protect Our Children While Preserving the First Amendment" and "Safeguard our Right to Privacy". Other goals are to "create a Transparent and Connected Democracy", to "Deploy a Modern Communications Infrastructure" and to "Employ Technology and Innovation to Solve Our Nation's Most Pressing Problems" (Obama, 2007).

The first goal argues that the free flow of information is *crucial in a democracy* and that the Internet is a critical facilitator for the democratic process. This touches upon the early Jeffersonian ideas of cyber-utopians such as Barlow and shows that this framing still exercises a degree of influence (see chap. 4.2.5 Framing Cyberspace as the Electronic Frontier (1990s)). The key argument is that the Internet must remain *accessible:*

> "A key reason the Internet has been such a success is because it is the most open network in history. It needs to stay that way. Barack Obama strongly supports the principle of network neutrality to preserve the benefits of open competition on the Internet. Users must be free to access content, to use applications, and to attach personal devices" (Obama, 2007).

This support for net-neutrality reflects the original visions of the Internet's designers, which is why Vint Cerf welcomed this proposal (Arthur, 2008). An Internet of two speeds, one slow lane for normal traffic and a faster, more pricier line for special services would "threaten innovation, the open tradition and architecture of the Internet, and competition among content and backbone providers. It would also threaten the equality of speech" (Obama, 2008). In another speech, Obama argues that "We can't have a situation in which the corporate duopoly dictates the future of the Internet" (Obama, 2008). This affirms central utopian ideas such as the hands-off norm, freedom of speech and the cyber-punk narrative of defending the open Internet from corporate or government encroachment. During his presidency, Obama kept word and maintained net-neutrality.

But in the campaign, the growing influence of cyber-realism becomes visible, especially within the goal to protect children from online crime. The openness of the Internet is generally seen as benign and it is argued that the *information age empowered individuals* by giving them new tools. At the same time "Barack Obama also recognizes that lurking out there are the darker corners of the media world: "from Internet predators to hateful messages to graphic violence and sex". Like in the 9/11 discourse, the frame of *dark figures lurking in the shadow* is used (see chap. 4.4.7 The Politicization of Cyber-Realism with the War on Terror (2000 - 2008)). But overall, Obama does not want to regulate technology, for example by censoring content. Instead he demands that the parents need to have the tools to shield their children from online threats. In line with the spirit of the end-to-end principle, he delegates the problem to the end-points of the network: the user. Interestingly, Obama does not just recognize the threats from child molesters or terrorists, but also: "The open information platforms of the 21st century can also tempt institutions to violate the privacy of citizens" (Obama, 2008). The availability of data creates a risk of (government) abuse. Therefore, the *privacy-enhancing power* of new technologies must be used in order to protect privacy.

Obama supports updating surveillance law to ensure that intelligence gathering adheres to legal principles and that data of American citizens is only used for the fight against terrorism and not "misused for other purposes" (Obama, 2007). This is in line with

the general rhetoric of his speeches, distancing himself from the Bush administration. In a famous 2007 campaign speech he made a powerful argument:

> "This administration [Bush/Cheney] also puts forward a false choice between the liberties we cherish and the security we provide. I will provide our intelligence and law enforcement agencies with the tools they need to track and take out the terrorists without undermining our Constitution and our freedom. That means no more illegal wiretapping of American citizens. No more national security letters to spy on citizens who are not suspected of a crime. No more tracking citizens who do nothing more than protest a misguided war. That is not who we are. And it is not what is necessary to defeat the terrorists. The FISA court works. The separation of powers works. Our Constitution works. We will again set an example for the world that the law is not subject to the whims of stubborn rulers, and that justice is not arbitrary" (Houck, 2013).

Barack Obama, with his constitutional law background built up some credibility in fighting against US mass surveillance in the past. He protested against Bush's Terrorist Surveillance Program, legitimized with the controversial unitary executive theory and against the expanding practice of national security letters including gag-orders that prevented a court of law. He also voted against the promotion of former NSA director Michael Hayden to become CIA director in 2006. However, in February 2008, when the Bush administration presented the FISA Amendment Act, a bill that post-hoc legalized and *expanded* the NSA mass surveillance program, Senator Obama voted in favor, although he threatened to filibuster the bill before (see chap. 4.4.7.4 The Fusion of IW, Surveillance and Cyber-War (2003-2008)). Observers argue that he needed to appear strong on matters of national security to bind a wider electoral base from the conservative spectrum (Bamford, 2009, p. 307).

The second major theme of the Obama campaign that reflects cyber-utopianism and even cypherpunk ideals is the focus on *transparency*: "The Bush Administration has been one of the most secretive, closed administrations in American history" therefore Obama wants to create "a new level of transparency, accountability and participation for America's citizens" (Obama, 2007). This includes the idea that the government should publish more data online, hold digital town-hall-meetings and holding ompanies and government agencies, who misuse private data, accountable. The Internet plays a special role in creating transparency because: "Full broadband penetration can *enrich democratic discourse,* enhance competition, provide economic growth, and bring significant consumer benefits" (Obama, 2007). The open access norm becomes apparent in the goal to provide full-broad band access for all Americans, thus bridging the digital gap.

It should have become clear by now that the Obama campaign relied heavily on cyber-utopian rhetoric, picking up key-frames from the 1990s such as the *empowerment*, the *democratization* and *economic growth* thesis, advocating for core cyber-utopian norms such as *open access, net-neutrality,*[158] *freedom of the Internet*. This rhetoric has been absent from governmental discourse during the Bush administration.

In 2009, after the election, President Obama made a visit to China and there he engaged in a Q&A with Chinese students. A student brought up the question of Internet control in terms of regulation. Obama's response to that question is enlightening. He says that:

> "But I am a big believer in technology and I'm a big believer in openness when it comes to the flow of information. I think that the more freely information flows, the stronger the society becomes, because then citizens of countries around the world can hold their own governments accountable. They can begin to think for themselves. That generates new ideas. It encourages creativity. And so I've always been a strong supporter of open Internet use. I'm a big supporter of non-censorship" (Obama, 2009a).

Assuming this is not a scripted response, the answer includes many cyber-utopian beliefs and generally adopts a positive undertone. He argues that the free flow of information strengthens societies and encourages creativity. This is similar to Marshal McLuhan in the 60s and cyber-utopians in the early 90s. He continues and argues the "Internet has become an even more powerful tool for that kind of citizen participation […] and it also helps to draw the world together" (Obama, 2009a). By reflecting on the Internet-usage practices of his daughters, he is fascinated by how they can speak to people at the other end of the world and the "enormous power that they have" because of the Internet, basically reaffirming the empowerment thesis. However, at the same time he is aware of negative Internet usage: "terrorists are able to organize on the Internet in ways that they might not have been able to do before. Extremists can mobilize. And so there's some price that you pay for openness, there's no denying that. But I think that the good outweighs the bad so much that it's better to maintain that openness" (Obama, 2009a). This is a remarkable statement against those who constantly demand more state control over cyberspace because of whatever threat they fear. Although there are certainly bad elements, like hate-speech against the President himself, he maintains that an open society must live with that and that the value of an open, uncontrolled Internet is the greater good.

[158] At the same time, the McCain campaign argued strongly against net neutrality, calling it unnecessary regulation (Holen, 2008). In fact, net neutrality is the default configuration of the Internet while prioritizing services like video would require regulation.

This remarkable attitude towards the Internet partly influences policy as well, particularly in the practices of the State Department. Secretary of State Hillary Clinton, referring to the policies of the Obama administration, adopts a similar tone in her 2010 "Remarks on Internet Freedom" speech. This speech stands in the context of the so-called "Green revolution" in Iran 2009 and the emerging Arab spring, where social media drove uprising against authoritarian rule in the Middle East (Penke, 2012). Clinton argued in her speech that the Western democracies must defend the openness and the freedom of the Internet from a grave threat:

> "Some countries have erected electronic barriers that prevent their people from accessing portions of the world's networks. They've expunged words, names, and phrases from search engine results. They have violated the privacy of citizens who engage in non-violent political speech. These actions contravene the Universal Declaration on Human Rights, which tells us that all people have the right "to seek, receive and impart information and ideas through any media and regardless of frontiers." With the spread of these restrictive practices, a new information curtain is descending across much of the world" (Clinton, 2010).

This strong statement against Internet control practices shows that the 1997 Supreme Court ruling, prohibiting Internet censorship in the US still has normative power (see chap. 4.3.5.3 Policy: Internet Censorship with the Communications Decency Act (1996)). Well-known utopian frames such as the *empowerment*, *power-distribution*, *free-information-flow*, *democratizing*, *digital-revolution, the dictator's dilemma, the global commons* all appear in her speech. Clinton also adopts the notion of the *electronic frontier* and *digital borders*: "Today, we find an urgent need to protect these freedoms on the digital frontiers of the 21st century." Electronic barriers or digital borders such as censorship systems prevent access to the free flow of information, thus creating insulated information spaces. These practices could result in a "fragmented planet in which access to information and opportunity is dependent on where you live and the whims of censors" (Clinton, 2010). This statement is interesting because one year later, President Mubarak shut down the Egyptian Internet on 25 January 2011 to block rebelling citizens from accessing Twitter and Facebook (Penke, 2012). Since then, the physical Internet shut-down of Internet backbones or services like Twitter, for example during elections or times of unrest, has become a common feature of Internet control in authoritarian societies (Deibert et al., 2010). Other examples are the Russian election of 2012 (Tselikov, 2014) or the protests against Turkish President Erdogan. Clinton warns in her speech that challenges for national security, such as the anonymity on the Internet, "must not become an excuse for

governments to systematically violate the rights and privacy of those who use the internet for peaceful political purposes" (Clinton, 2010).

Clinton also develops two relatively new utopian frames that do not seem to derive from counter-cultural and hacker discourses of the past. First, she argues: "the Internet can help bridge divides between people of different faiths" (Clinton, 2010). It can create a *dialogue between different religious communities*. This of course requires open access. The second novel idea is that *freedom of assembly* directly relates to the Internet as well: "the freedom to connect – the idea that governments should not prevent people from connecting to the Internet, to websites, or to each other. The freedom to connect is like the freedom of assembly, only in cyberspace" (Clinton, 2010). Clinton traces this argument back to her idol Eleanor Roosevelt.

But of course, Clinton is a pragmatist and well aware of threats of terrorism, hacking and criminal activity online. As such the speech tries to create a balance between realist and utopian frames. In the end, she states the position of the US:

> "States, terrorists, and those who would act as their proxies must know that the United States will protect our networks. Those who disrupt the free flow of information in our society or any other pose a threat to our economy, our government, and our civil society. Countries or individuals that engage in cyber attacks should face consequences and international condemnation. In an internet-connected world, an attack on one nation's networks can be an attack on all. And by reinforcing that message, we can create norms of behavior among states and encourage respect for the global networked commons" (Clinton, 2010).

The last sentence is remarkable, not just because it adopts the utopian frame of the *open commons*, but because it indicates a new security paradigm. It recognizes the interconnectedness and combines it with the idea of NATO's collective defense: an attack on a member equals an attack against all.[159] IT-experts such as Susan Landau argue that in the age of digital interconnectedness we must overcome our narrow, terrorist-focused understanding of *national* security and instead focus on *global or common security* of our networks (Landau, 2016). A vulnerability in one system affects everyone who uses it and thus potentially billions of people (for example everyone using Windows would be affected by a security vulnerability). In contrast, the practice of US Cybercommand during the Obama presidency represents the total opposite of this globalized understanding of cyber-security (see chap. 4.5.3 Practice: Professionalization of Offensive Cyber-War & Surveillance).

[159] Since around 2015 NATO argues, that a cyber-attack could trigger article 5 (McLeary, 2015). For more detail on NATO's offensive capabilities see (Lewis, 2015).

However, one practice of the US State Department to promote Internet freedom deserves some mentioning: the support of the "development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship" (Clinton, 2010). In 2013, the State Department supported anti-censorship and secure communication technologies with $25 million (U.S. Department of State, 2013). Technology such as TOR,[160] the secure, encrypted and anonymity-providing browser received an $1,8 million Dollar funding from the US government. TOR is used by journalists and activists worldwide to shield their anonymity from surveillance of authoritarian regimes (Hern, 2014). It is also used by criminals and terrorists. That is the reason why the IC lobbied heavily for the dismantling of anonymity on the Internet provided by the activist TOR network. The Snowden leaks that are introduced a bit later show how NSA wrestled with getting its head around TOR, breaking encryption and anonymity it provides (see chap. 4.5.5 Artifacts: The Snowden Leaks). Former NSA director Hayden described the paradox in 2013: "So on the one hand we're fighting anonymity, on the other hand we're chucking products out there to protect anonymity on the net" (Tucker, 2015). This highlights the utopianism-realism clash of the Obama administration and its hybrid nature.

Now that we have established utopian features in the rhetoric of the Obama administration, lets shed some light on the opposite: the realist practices.

4.5.3 Practice: Professionalization of Offensive Cyber-War & Surveillance

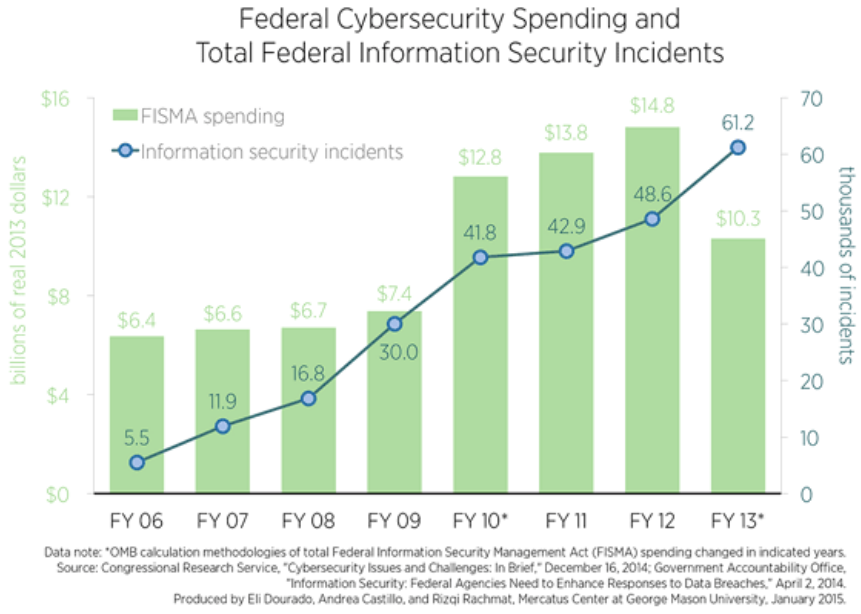
The Obama administration has four distinct cyber-themes I want to focus on: first, an increased focus on cyber-security. Second, the increased institutionalization of cyber-war. Third, the professionalization and the offensive-turn of cyber-war and fourth, the expansion of cyber-realist ideas. These are four distinct streams that all facilitate the normalization of cyber-realist thinking.

The first general gist of Obama's Internet policy is the *expansion and professionalization of cyber-security*. As one of the first issues after entering office, Obama ordered a Comprehensive Cyberspace Policy Review (Lee, 2015, p. 251), and confirmed Bush's Comprehensive National Cybersecurity Initiative (CNCI). This is a computer network defense effort to protect government/executive networks from foreign

[160] The Onion Routing (TOR) is a technology initially conceived by DARPA and the intelligence community to protect classified information. Since 2006, the TOR project is driven by researchers and internet activists to provide anonymity on the Web that even NSA cannot break (to the present date). Onion routing artificially reroutes data-packets through different servers, adding a layer of encryption at each hop. In the end, the origin of an internet activity cannot be traced and monitored. There is an overall consensus within the cyber-security community that TOR is the only affective guarantee for anonymity online to the present date.

intrusion. With this initiative, "President Obama has identified cybersecurity as one of the most serious economic and national security challenges" (Executive Office of the President of the United States, 2009, p. 1). The CNCI launches initiatives for better federal network management, intrusion prevention across governmental networks, a coordinated R&D effort, better security of classified networks and an education program. The initiative pursued the deployment of deep-packet-inspection equipment (called EINSTEIN) on internal governmental networks that monitors incoming traffic for malicious packets. Formally, DHS was the designated lead agency for protecting government networks but NSA also began to play a role.[161] Landau argues "giving the NSA a major role in securing unclassified networks represented a significant change" (Landau, 2010, p. chap 5.6). It can be argued that with the affirmation of this directive under Obama, cyber-security became its own policy field with increasing priority. The high priority given to the topic can be shown with the following graph**,** which summarizes the Federal Cybersecurity spending.

Figure 28. Federal Cyber-Security Spending and Incidents, Source: (Dourado & Castillo, 2015)[162]



[161] General Alexander lobbied for the expansion of NSA's role in protecting private networks: "I do not have the authority to stop an attack against Wall Street or industry, and that's a gap I need to fix." The financial executives resisted the plans to install surveillance equipment on their networks. "He wanted to create a wall around other sensitive institutions in America […] and to install equipment to monitor their networks," says a former administration official. (quoted inHarris, 2014, p. chap. 10).

[162] The graph combines data from the congressional research service, the GOA and the Federal Information Security Management Act of 2002. FISMA records the number of cyber-security incidents (thousands of incidents).

The increased spending is noteworthy, because other branches of government, including the overall military spending were downgraded due to the economic recession of 2008. Additionally, the graphic includes the cumulated rise of cyber-security incidents which increased with an ever-growing diffusion of Internet services and devices. This is a key explanation for the increased focus on cyber-security issues and Obama's cyber-policy and an equifinality of converging causal factors.

The second element of Obama's policy is the *institutionalization of cyber-war*, not just in the USA, but globally. The Bush administration, influenced by DNI Mike McConnell had set in motion the cyber-war machinery with plans for a cyber-command, the development of new CNA capabilities like Stuxnet and new surveillance-enabling legislation like FISAAA (see chap. 4.4.7.4 The Fusion of IW, Surveillance and Cyber-War (2003-2008)). However, it left a "cyber-security patchwork" (Singer & Friedman, 2014, p. 200).[163] The Obama administration tried to streamline the different capabilities that had been sprawled within the IC and the different military branches by creating a unified US Cybercommand (US CYBERCOM) in May 2010. The main purpose of US CYBERCOM was to answer the "who is in charge" question that resurfaced after the Buckshot Yankee incident in 2008 (Kaplan, 2016, p. chap. 10). CYBERCOM created a clear chain of command, overseeing and coordinating different cyber-warfare centers within the armed forces that had been established in the past (Lynn, 2010). CYBERCOM is coordinated by the director of NSA, and located in close proximity to Fort Meade, highlighting the nexus between cyber-war and surveillance. In total, it has around 60000 employees (Singer & Friedman, 2014, p. 134) and is coordinated by US STRATCOM, which plans and coordinates CNO and IO. Its mission statement is:

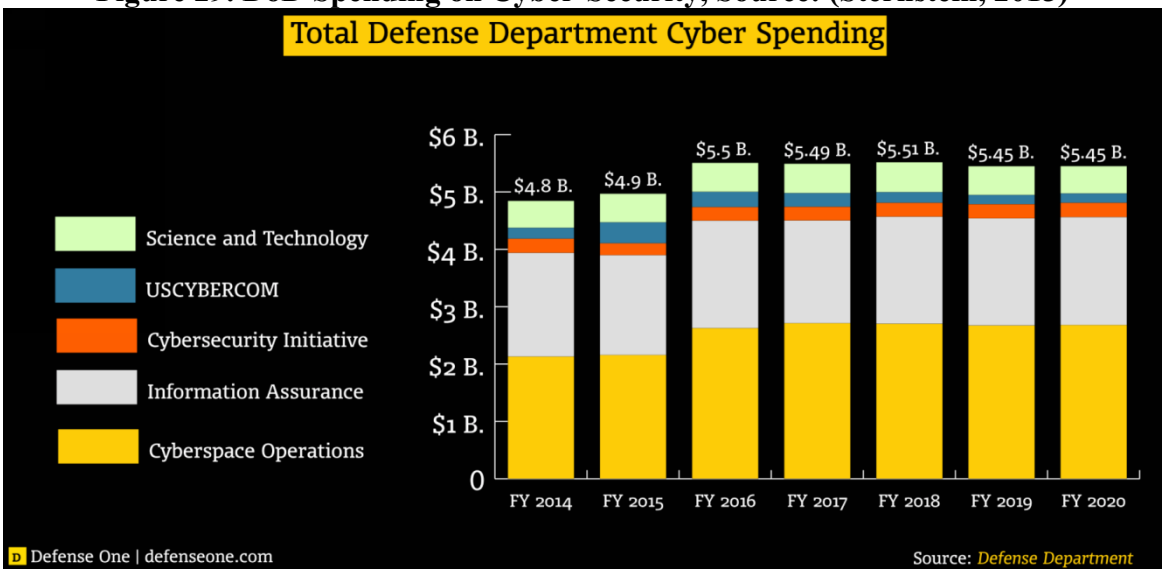
> "USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks; and prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries" (STRATCOM, 2010).

The new relevancy of CYBERCOM can be shown by looking at its budget (see following figure). In 2014, while the most of the military forces received less budget, that of CYBERCOM doubled (Singer & Friedman, 2014, p. 135) and "cyberspace operations" (CNA and CNE) received roughly $2 billion. CYBERCOM itself received around $509

[163] A 2013 Congressional Research Service report counted more than 50 statutes that form the legislative framework for cybersecurity (Fischer et al., 2013, p. 1).

million in FY 2015. Observe that it is estimated that in the future more money (around $2 billion) will be spent on Cyberspace Operations, i.e. offensive CNA compared to *information assurance*, a terminus-technicus for CND. The enormous budget can be explained because CYBERCOM operates "a 600,000-square-foot, $896.5 million supercomputer facility called the High Performance Computing Center-2" (Bamford, 2015).

Figure 29. DoD Spending on Cyber-Security, Source: (Sternstein, 2015)



In sum, CYBERCOM implements and institutionalizes many elements of the IW doctrine and cyber-realist paradigm in a joint military structure.

CYBERCOM also initiated the *professionalization of a cyber-war workforce* within the armed forces and IC (Department of Defense, 2015, p. 17). Since 2010 there are officer-career tracks, for example the US Air Force 17 deltas officer. US Navy is training 24000 recruits per year in its Information Dominance Center in Nevada (Saalbach, 2015, p. 31). Other agencies, like DHS, NSA or CIA also invested heavily in recruitment for digital war. Since 2012, CYBERCOM created its *Cyber Mission Force,* consisting of roughly 6200 civilian and military employees. These are subdivided for different tasks: *Cyber Protection Forces* for cyber-security (computer network defense),[164] *National Mission Forces* for offensive cyber-war like Stuxnet, which is coordinated by NSA's TAO and the

[164] The 2010 Quadrennial Defense Review explains: "DoD currently operates more than 15,000 different computer networks across 4,000 military installations around the world. On any given day, there are as many as seven million DoD computers and telecommunications tools in use in 88 countries using thousands of warfighting and support applications." (Department of Defense, 2010, p. 37). As a consequence, DoD reduced the number of access points to its internal network and implanted sophisticated network monitoring tools (DPI) at these gateways, analyzing incoming packets for malicious code. (Harris, 2014, p. chap. 3). NSA was tasked to compile lists and dossiers of known hackers, particularly in China but potentially on the entire globe.

even more elitist Remote Operations Center. Those groups are tasked with scouting out and breaking into networks to provide targeting information for CYBERCOM. Finally, there are *Combat Mission Forces*, with tactical CNA capabilities during combat operations (Saalbach, 2015, p. 60). An example are the Joint Special Operations Command (JSOC) that has its own cyber-warriors that can "conduct operations like embedding sensors in computer keyboards to follow what suspected terrorists type, or creating fake online identities in order to trap suspects and elicit information" (Priest & Arkin, 2012, p. 225). The use of cyber-war within limited combat theaters also marks a subtle shift in strategy. Publicly, advocates frame offensive CNA and cyber-war as a *strategic* element that shifts the nature of war by disrupting entire nations from the distance (see chap. 4.5.4 Discourse: Cyber-Doom and the Hegemony of Cyber-Realism). Internally, the military moved from the concept of strategic cyber-warfare to the concept of "*operational cyber-war*": CNA used by special forces in limited combat scenarios, resembling the concept of hybrid warfare (Geers, 2015).

The third theme of the Obama administration is the offensive-turn. From the job listings it becomes clear that US CYBERCOM prioritizes CNA and not CND, as its mission statement might suggest. "It's an attack agency...." according to Edward Snowden (Bamford, 2015). With a suitable cyber-war workforce comes the *increased sophistication and a general offensive turn in CNA capabilities*. Nothing represents this more than the technical artifact called Stuxnet. In June 2010, cyber-security experts discovered the so-called Stuxnet worm that specifically targeted Siemens SCADA systems[165] in the air-gapped Iranian nuclear enrichment facility in Natanz. The CNA utilized four previously unknown security vulnerabilities (zero day exploits) and was distributed via USB drives, indicating the involvement of secret agents. This weaponized software was one of the most sophisticated cyber-attacks known to date. It had around 650,000 lines of code, or 4000 times as much as typical malware (Kaplan, 2016, p. chap. 12). The enrichment centrifuges in Natanz were sabotaged remotely over a period of months (not in a single knockout blow). The goal of this artifact was to disrupt or delay the Iranian nuclear enrichment program. Stuxnet made great efforts to remain hidden during that time. "Only" 2000 of around 8700 centrifuges were damaged (Barzashka, 2013). While the tactical effect was limited, the strategic impact was profound. Michael Hayden and several other officials described this as a watershed moment: "This is the first attack of a major nature in which a cyber attack was used to effect physical destruction. Somebody crossed the Rubicon" (Lee,

[165] Supervisory Control and Data Acquisition are used for remote monitoring of industrial machinery over networks. They play a huge role in so-called "Industry 4.0", connecting industrial assets to the Internet.

2015, p. 60). The Rubicon is the so-called kinetic-threshold. Indeed, media reporting on Stuxnet was manifold and the case is often highlighted in cyber-security publications, indicating its high impact among security professionals. As a result of Stuxnet, many countries started to recognize cyber-security issues and began to develop national cyber-warfare programs and doctrines (Shafqat & Masood, 2016). In 2012, Iran allegedly retaliated with a counter-attack called Operation Shamoon, which erased data from 30000 computers, replacing it with an image of a burning American flag (Healey & Grindal, 2013).

The Washington Post reported in June 2012 that President Obama allegedly ordered the CNA, which was an outcome of operation Olympic Games (Lindsay, 2013), a program that began under the Bush administration around 2005 and became operational in 2008 (Nakashima, Miller, & Tate, 2012). According to malware analyst Ralph Langer, the development had cost several million dollars (Langner, 2013). The attribution problem of CNA/CNE makes the question of who was responsible hard to answer. Although the Obama administration never confirmed to be responsible for any type of CNA or CNE, indicators point to US and Israeli intelligence agencies. The high complexity of the malware and the detailed knowledge of the target systems indicate the involvement of intelligence agencies and years of preparation and simulation (Lindsay, 2013, p. 386). Operation Olympic Games also produced two of Stuxnet's technological siblings, Flame and Duqu. The Flame virus was revealed by Kaspersky in May 2012 and was a more refined version of Stuxnet's code. In contrast to Stuxnet, which was a CNA (with a big portion of information warfare in terms of deception), Flame was designed for CNE: it targeted high-ranking Iranian officials, stealing information (screenshots, audio, video, network traffic, key-logging) and sent it to remote servers in different parts of the world while masking its traces. In other words, it was a sophisticated targeted surveillance software directed at key leaders, just as the 1990s IW doctrine envisioned. According to US officials, Flame "prepared the battlefield for another type of covert action" (Nakashima, Miller, & Tate, 2012), which again highlights the logical connection between surveillance, intelligence-gathering and cyber-warfare. Stuxnet and Flame indicate the logical overlap between CNE, Internet surveillance and offensive CNA, which was also addressed in new military doctrines.

The fourth theme of Obama's cyber-policy was the *formulation of a new Cyberstrategy in 2011* (updated in 2015). It serves as the ideational background for the practice of cyber-war in the US and includes many of the ideas and concepts developed in the 1990s under the IW doctrine. This is no accident because some of the drafters of the

doctrine held IW positions in the intelligence community back in the day. In other words, it represents a continuity of ideas. For example, the cyber-strategy declares cyberspace officially as an operational domain, an idea that was invoked in the mid 1990s, finally cast into policy (Department of Defense, 2015, p. 4). Besides replicating well established cyber-realist ideas, it introduced a new approach to cyber-attacks: the *concept of equivalence* (Singer & Friedman, 2014, p. 136). The US "will respond to a cyberattack on US interests through its defense capabilities" and "conduct cyber operations to counter an imminent or on-going attack against the US homeland or US interests in cyberspace" (Department of Defense, 2015, p. 5). In other words, the US would respond to cyber-attacks either in kind ("to hack back") or with conventional weapons, and even preemptively (a legacy from the Bush administration). For the first time, digital attacks were equated with conventional attacks. This is a highly controversial position because of the attribution problem. The DoD strategy recognizes the problem of attribution which makes retaliation difficult. It argues that anonymity [of the Internet] "enables malicious cyber activity by state and non-state groups". However, it highlights that the IC "invested significantly in all source collection, analysis, and dissemination capabilities, all of which reduce the anonymity of state and non-state actor activity in cyberspace" (Department of Defense, 2015, p. 15). In other words it is, at least implicitly, confirmed that intelligence programs are designed and able to remove anonymity from the original TCP/IP infrastructure. Therefore, the cyber-strategy maintains the old IW doctrine's strategic goal to gather "actionable intelligence about global networks and systems, adversary capabilities, and malware brokers and markets" (Department of Defense, 2015, p. 16). This position yet again highlights the entanglement of the IC (and CNE) with cyber-war (and CNA) (Lewis, 2015).

A second noteworthy new concept adopted in the US cyber-strategy is General Alexander's idea of *"active defense"* that he developed after taking over the helm at NSA. This is a euphemism for preemptively hacking enemy command and control structures in order to anticipate cyber-attacks. This is a controversial notion because it intentionally blurs the line between offense, defense and peace and war. This is controversial because the difference between CNE, which needs no authorization from the President, and CNA, which does, is often only the flick of a switch. A CNE operation can be easily turned into a CNA by enabling the destructive payload of a malware. More so, if CNA can trigger a kinetic response, the risk of escalation is not trivial. What further complicates matters is

that all of this is done in great secrecy.[166] Thus, in the worst-case scenario, "active defense" could trigger a military escalation and no-one would know about it.

Generally, the cyber-strategy indicates the *normalization of cyber-war*. Cyber-realist ideas that emerged in the 1990s now are perceived as normal tools of statecraft (Valeriano & Maness, 2014, p. 347). Considering that many other states started their own cyber-war programs as a reaction to Stuxnet, the idea to exercise control over another nations' IT infrastructure with the instrument of state-hacking can be seen as a consolidated norm that started to diffuse around 2010 with the technical artifact called Stuxnet. Although not analyzed as deeply as the other technical artifacts, the case can be made that Stuxnet is another instance of norm-diffusion via technology-diffusion. General Michael Hayden acknowledges this norm-diffusion: "The rest of the world is looking at this and saying, "Clearly someone has legitimated this kind of activity as acceptable international conduct. The whole world is watching" (Kroft, 2012). This could be called norm-diffusion by emulation (Florini, 1996). The norm diffusion got accelerated by technical diffusion. For example, soon after Duqu's code was discovered and publicly dissected, derivative malware popped up on the Internet. In other words, unknown hackers were mimicking their US counterparts by replicating and repurposing their technology.

Accompanying this normalization is the classified, TOPSECRET/NOFORN Presidential Policy Directive PPD 20 of October 2012, issued only a few months after the press discoveries of Stuxnet. It defined under what circumstances the US President would authorize CNA. In general, this doctrine materializes cyber-realist ideas: the primacy of US military and IC in defending US networks and controlling international cyberspace and the elevation of CNA to the status of traditional combat (Harris, 2014, p. chap. 3). It ordered relevant agencies and departments to identify adversarial critical infrastructures against which US cyber-attacks "can offer a favorable balance of effectiveness and risk, as compared to other instruments of national power" (Kaplan, 2016, p. chap. 12). To scope out enemy command and control structures (targeting) during peace time was first conceived with the IW doctrine in the early 1990s and then, 20 years later put into operational policy. According to Kaplan, the PPD-20 closely resembled an article from NSA's in-house journal called Cryptolog in 1997, which clearly shows the continuity of cyber-realist thought over time (Kaplan, 2016, p. chap. 12).

[166] Former NSA director Hayden argues: "Beyond complexity, developing policy for cyber ops is hampered by excessive secrecy (so says this intelligence veteran!). Look at the bloodline. I can think of no other family of weapons so anchored in the espionage services for their development (except perhaps armed drones). And the habitual secrecy of the intelligence services has bled over into cyber ops in a way that has retarded the development—or at least the policy integration—of digital combat power. It is difficult to develop consensus views on things that are largely unknown or compartmented or only rarely discussed by a select few" (Hayden, 2016b, p. chap. 8).

In sum, these factors indicate the transition from defensive cyber-security, concerned with hardening networks and critical infrastructure protection (that goes back to the Clinton administration) to offensive and even preemptive cyber-war. This represents the creation of new policy goals and as such incremental paradigm-change within cyber-realism, according to the theory (see chap. 2.2.3 Degrees of Change). The creation of a cyber-workforce, the institutionalization of defensive and offensive competencies under USCYBERCOM and the doctrinal guidance that allows in-kind or even physical responses establish offensive cyber-war as a new norm within US policy. "The core infrastructure for fighting a cyber war has been created. Now the United States is raising an army" (Harris, 2014, p. chap. 3). More so, because of its role-model character, many other states and organizations (particularly NATO) followed this US position and started to develop offensive cyber-war capabilities as well. As a result, offensive cyber-war and the norm of control become established globally, creating an arms race in cyberspace. This can be shown by pointing to the 2011 cyberspace strategy that argues for the right to self-defense in case of CNA: "We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law" (The White House, 2011, p. 14), as a response to cyber-attacks. It is seen as appropriate that states strike back digitally and physically.

That cyber-realist norms became dominant under Obama can be shown by referring to their discursive trail. Although we saw cyber-realist topics spilling over from governmental circles to the public discourse before, since 2011 this happened at an unprecedented scale. The next chapter will introduce the discourse around cyber-warfare in the US.

4.5.4 Discourse: Cyber-Doom and the Hegemony of Cyber-Realism

Whereas the cyber-realist paradigm was predominantly held by military and intelligence officials during the Clinton administration and brought into the political sphere by neo-conservative hawks in secrecy by Bush, under Obama, it became normalized and in fact hegemonic. Cyber-realist concepts, originally invented within the military discourse on information war, became standard or unquestioned terms in political discourse during the Obama presidency. Since then, even democratic policy-makers adopted the cyber-war narrative in public speeches or op'ed newspaper articles. Cyber-doomsday scenarios (Lawson, 2011), became standard headlines in media coverage. Between 2007 and 2011, cyber-realists openly securitized the Internet. They used incidents like Estonia 2007 as a legitimization for new security measures and offensive cyber-war capabilities in front of a

wider media audience. The discourse peaked in late 2010 or early 2011 with the revelation of Stuxnet. Whereas the debate about cyber-war had been limited to military papers and academic literature before, suddenly TV documentaries (Stuxnet: Cyberwar 2011) and movies (Cybergeddon) illustrated the threat of cyber-attacks for a wider audience. This securitization of cyber-security through discourse is well studied by academia (Lawson, 2011; Lawson, 2012; Hansen & Nissenbaum, 2009; Dunn Cavelty, 2007; Dunn Cavelty, 2013b; Dunn Cavelty, 2013a; Eriksson, 2001; Gartzke, 2013). Because these threat frames and security mechanisms are well studied, there is no need for replication and I only present a short overview over the discourse that unfolded after Stuxnet. The purpose of this chapter is to gauge its general societal impact. This chapter does not conduct a full-fledged discourse analysis but describes the overall story-line of the discourse in a narrative fashion, much like the previous chapter on cyber-utopian ideas appearing in public discourses (see chap. 4.2.8 Norms and Key Ideas of Cyber-Utopianism).

There are generally two discursive positions: cyber-realist hawks and more skeptical, often academic or professional voices. Cyber-realist advocates include military and intelligence actors including DNI Mike McConnell (McConnell, 2009; McConnell, 2010), CIA-director Leon Panetta (Mulrine, 2011), (Panetta, 2012), NSA General Keith Alexander (Gertz, 2011) or politicians like Deputy Secretary of Defense William J. Lynn III (Lynn, 2010). Even President Barack Obama (Obama, 2012) adopts cyber-realist positions. There are also cyber-security firms (like McAfee) and arms & surveillance technology manufacturers that frame cyber-war and hacking in terms of doomsday scenarios. Cyber-realist advocates act as bricoleurs, sense-makers, in this particular context. Doomsday scenarios are narratives that focus on strategic cyber-war and operate with the crippling-blow thesis (Lawson, 2011). They assume that a single sophisticated CNA (like Stuxnet) could bring down a modern, information-based society (the referent object). CNA like Stuxnet or Shamoon are framed as an extraordinary threat to which must be responded by adopting new policies and a military strategy. For example, Barack Obama argued in 2009: "the cyber threat to our nation is one of the most serious economic and national security challenges we face" (Obama, 2009b) and "the number one strategic threat to the United States, placing it ahead of terrorism for the first time since the attacks of September 11, 2001" (Department of Defense, 2015, p. 8). A CBS article quotes the script of a documentary called Stuxnet that aired in March 2012, summarizing some of the famous quotes by the central cyber-realist advocates from within the IC:

> "FBI Director Robert Mueller: I do believe that the cyberthreat will equal or surpass the threat from terrorism in the foreseeable future. Defense Secretary Leon Panetta: There's a strong likelihood that the next Pearl Harbor that we confront could very well be a cyberattack. House Intelligence Committee Chairman Mike Rogers: We will suffer a catastrophic cyberattack. The clock is ticking" (Kroft, 2012).

Terrorists could use cyber-attacks to poison the water supply, derail trains or damage air control traffic systems. Since Stuxnet passed the physical threshold (Hayden), the metaphoric genie is out the bottle and it is only a matter of time until a "digital 9/11" or "digital Pearl Harbor" takes place.[167] The overall similarity to the Y2K discourse is striking (see chap. 4.4.5 Discourse: Y2K and Critical Infrastructure Failure) with the difference that now there are clear adversaries. Adversaries are generally China, Russia, terrorists or other sophisticated states. This line of thought is basically the continuation of early IW and RMA thinking that includes many of the same metaphors ("digital Pearl Harbor" from 1991). An example is the "cyber-revolution thesis" (Lindsay, 2013). The argument here is that new technologies are a game-changer that alter the fundamental nature of war (technical determinism). The technological structure of TCP/IP produces asymmetric effects: modern, information societies depend on the Internet to operate (finance, electricity, transportation, military command & control) and are therefore more vulnerable than non-state actors or industrial societies (say North Korea). The weaker get empowered while the stronger become more vulnerable. Additionally, the offense is said to be easier (only one security vulnerability must be found), while the defense gets harder (CND must protect the entire network of interconnected devices) and because the Internet grants attackers anonymity, which creates the problem of attribution. This, in a nutshell, are the predictions made by the IW doctrine in the 1990s (see chap. 4.4.2.3 Core Ideas: Information Weapons & Digital Battlespace). In theoretical terms, the cyber-doom discourse represents a counter-signification that frames the Internet and related phenomena in predominantly national security terms and threats. The Internet is presented predominantly as an existential threat to the US and not as a harbinger for democracy that it used to be in the 1990s (see chap. 4.3.3 Ideas: Cyber-Utopia on the Information Superhighway (1993)). An outcome of this process is that instead of a prefix, the former greek adjective "cyber" is now often signified and treated as a standalone noun. When policy-makers speak of "the cyber", they generally mean something negative, something

[167] The "not if but when" frame is particularly interesting because it operates like a prophecy. In this frame there is no alternative future and as such it represents a hegemonic articulation. Interestingly, the "not-if-but-when" frame was seldom uttered during the Cold War, where the possibility of a nuclear first strike was always taken for granted.

that is a problem for national security. "Cyber" as a noun signifies the cyber-security domain and thus, the meaning is no longer equivalent with the adjective "digital".

The general function of this cyber-securitization is to legitimize extraordinary measures that would not be legitimate without an existential threat. Extraordinary measures that are demanded include a heavier focus on offensive and preemptive cyber-attacks (reframed as "active defense") and cyber-deterrence by retaliation (a legalization of digital and physical retaliation), new funding for offensive programs (like Olympic Games) and more network surveillance infrastructure (like deep-packet inspection software) to monitor the Internet. Former head of NSA and DNI Mike McConnell even demands to "reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment – who did it, from where, why and what was the result – more manageable" (McConnell, 2010). Nothing makes the norm of Internet control, once derived from the core problem of attribution, more visible in public discourse than this quote. McConnell actively argues to change the code, the underlying architecture of the Internet to enable better surveillance. As we have seen, CND, CNE and CNA are structurally similar which brings it down to this formula: more offensive capabilities (CNA) equals an empowerment of surveillance (CNE). Many of these measures feature elements of Internet control and therefore are a manifestation of the norm of control. The goal becomes to control the Internet, not just within the homeland but also beyond one's own border.

The second line of argument is critical of these often unproven assumptions and fear-mongering strategies in the cyber-war narrative. Because cyber-security is a highly technical and specialized discourse, it is mostly academics (Deibert, 2003; Deibert, 2015; Rid, 2012; Lindsay, 2013; Gartzke, 2013; Dunn Cavelty, 2013b; Libicki, 2014; Valeriano & Maness, 2015; Lawson, 2012; Healey & Grindal, 2013) who criticize these threat figures by relying on classical theories of peace and conflict research and empirical data (Valeriano & Maness, 2015). For example, to the present day, not a single person has died because of a strategic cyber-attack. Comparing CNA with the destructive capabilities of physical weapons is way out of scale. Additionally, every year storms, falling trees or squirrels produce more power-outages and black-outs than cyber-attacks in the US alone (Peterson, 2016). The general line of argument is that strategic cyber-war and crippling blows will very likely not take place (Rid, 2012), because only a few actors have strategic incentives and relevant capabilities. Even if a digital Pearl-Harbor took place, its effects will be limited and most likely not produce chaos, due to the temporary nature of digital disruptions (Lawson, 2011).

Additionally, some argue that the threat of cyber-terrorism is overblown because destructive cyber-attacks like Stuxnet are too sophisticated and cost intensive that they do not favor well in the cost/benefit calculation of extremists. Terrorists can produce greater effects with cheaper means like AK rifles and pipe-bombs, as for example the Paris attacks have shown (Sin et al., 2016). They argue that much of the cyber-war discourse is overblown, which blurs the real issue: cyber-crime and economic espionage (as well as foreign intelligence), which produces factual economical damage. Scholars like Thomas Rid argue that most instances (like Estonia or Stuxnet) resemble acts of military deception or sabotage, but do not qualify as acts of war (Rid, 2012). Indeed, statistically, most cyber-incidents are either cyber-crime (data & intellectual property theft) for monetary gain (82,7% of cases), hacktivism for political reasons (9,3%) and cyber-espionage (4,0%), done by intelligence agencies. Inter-state cyber-attacks account only for 2,7% of the cases, according to analysts (Passeri, 2016).[168] In terms of actual damage, cyber-crime is the more pressing issue.

Especially computer scientists that analyze the technicalities of CNA argue that the cyber-attacks that already did happen are not as severe as cyber-realist advocates frame them (Farwell & Rohozinski, 2011; Barzashka, 2013; O'Connell, 2012).

However, because of the high technical sophistication of the cyber-security discourse (Hansen & Nissenbaum, 2009), the playing field is not equal. Because most cyber-attacks remain either hidden or are dealt with in secrecy, there is no transparency and room for critical and independent evaluation. Data used for attribution of intruders is seldom published. The actors who are tasked with CND are also those who are tasked with CNA and CNE, which often results in the classification of events that happen. These actors have a strategic interest in boosting the cyber-threat because it results in more competencies (like digital-retaliation or more CNE/CNA capabilities) and funding. In contrast to other policy areas, a civil-society discourse not taking place. It is mostly academics (social & computer sciences), a few critical NGOs (ACLU, EFF) and cyber-security experts who warn of a militarization of cyberspace and provide critical arguments. They do so mostly within inner-academic circles (scientific journals) and with a temporal delay. Observe that critical evaluation of Stuxnet happened roughly three years after the fact, when more data became public. At this point, the institutionalization of new CNA capabilities was already at full steam. Critics argue that war-games in cyberspace make the Internet more vulnerable and are contradictory to efforts to increase cyber-security. As a result, there is a

[168] Additionally, there is a wide range of "cyber-attacks" from simple, but often occurring automated network probing to sophisticated malware ala Stuxnet, that rarely is discovered. When statistics speak of millions of cyber-attacks a year, most of them are actually harmless.

huge imbalance within the media discourse: the cyber-realists from the IC have an information advantage which they use to dominate the news, which allows them to establish their cyber-revolution narrative as dominant. In terms of discourse theory, the cyber-war discourse resembles what philosopher Jürgen Habermas calls a "dominated discourse" that structurally favors one discursive position over another (Habermas, 1970). Thus, the institutionalization of cyber-realism and its upgraded standing in a post 9/11 world, allow it to dominate the discourse.

The issue became even more apparent when former NSA-contractor Edward Snowden leaked roughly 3 million internal documents describing NSA's mass surveillance and cyber-war machinery to the public. This further increased public salience of the issue and led to much controversy regarding these practices.

4.5.5 Artifacts: The Snowden Leaks

This chapter introduces some of the Snowden leaks that are of relevance for this thesis. There are reasons for this.

First, as indicated before, the Snowden leaks can be theorized as a potential shock for the cyber-realist paradigm which led to a potential juncture in the causal process. The controversial nature of these leaks increased the chances for policy change. Snowden himself argued that he hoped his actions would lead to a rethinking of the US global mass surveillance and hacking practice (Gellman & Markon, 2013). The leaks tested the durability of the cyber-realist paradigm much like the dot-com burst tested the explanatory power of cyber-utopianism (see chap. 4.2.7 Junctures: Dot-com Bubble (2000-2001)).

The second reason why these leaks are important is because they showed the public what "full-take" and the norm of Internet control actually meant. They are smoking-gun evidence for the existence of cyber-realist inspired technical artifacts and norms (see chap. 3. Methodology & Research Design). In the press, intelligence officials described this norm guiding NSA mass data-collection established by NSA director Keith Alexander:

> "Rather than look for a single needle in the haystack, his approach was, 'Let's collect the whole haystack,'" said one former senior U.S. intelligence official who tracked the plan's implementation. "Collect it all, tag it, store it. . . . And whatever it is you want, you go searching for it" (Nakashima & Warrick, 2013).

Furthermore, the leaks show how information- and cyber-war together with surveillance form a tightly-knit assemblage of interrelated practices (Haggerty, Kevin, 2000). Before the leaks, these practices were shrouded in secrecy, only known to highest-ranking

intelligence officials. The leaks also show the globalization of cyber-realism in terms of the IW-goals and how the norm of Internet control became adopted by international partners (like the Five Eyes) and corporations that manage information.

Third, these documents describe the goal-oriented construction and use of artifacts inspired by a cyber-realist mindset. Thus, these documents are prime source material to trace the diffusion of both technology and the norms it carries. Although repeatedly justified with the GWOT, the leaks included programs that had little to do with terrorism, like the surveillance of the EU and UN embassies (DROPMIRE), the spying on the UN security council members and allies during UN or G20 meetings, the surveillance of video games (Angry Birds, World of Warcraft), the surf-behavior of love-interests (Gorman, 2013) or spying on allied heads of states (Angela Merkel's phone). These programs make more sense if one understands them in the context of the *goal of total information awareness* (see chap. 4.4.2.3 Core Ideas: Information Weapons & Digital Battlespace). I argued earlier that cyber-war and surveillance should be understood within the framework of information-warfare.

Because of the massive scope of leaks and programs, I will concentrate only on a few programs that focus on the circumvention of norms of the original Internet and the fusion of IW, cyber-war and surveillance. A disclaimer is in order upfront. Due to the contested and classified nature of the Snowden documents, the author cannot (and will not) assure the accuracy of the claims depicted in the documents. However, NSA did not deny the authenticity of many of these documents.

What is noteworthy with these programs is that most of them operate within the expanded legal framework that was introduced under Bush (see chap. 4.4.7.2 Policy: The Patriot Act and Intelligence Reform (2001 - 2004)). They often rely on special interpretations of law to circumvent the warrant process, heavily use gag orders and secret contracts that prohibit commercial partners from disclosure (for example to affected customers, as the rule of law normally dictates). In contrast, NSA officials argue that these programs are subject to strict oversight from Congress and the FISA court, but to assess the legality of the programs is not the task of this thesis (Nakashima & Warrick, 2013). What is more important for this work is the fact that they aim to realize the goal of total information awareness – by collecting every piece of data transmitted, stored and generated and make data accessible to partners and other agencies (sharing norm). Additionally, data obtained by programs is used an analyzed by multiple other programs (and probably third parties), creating an assemblage of interconnected systems.

The PRISM program, leaked on 7 June 2013, documented the extraction of user data (E-mail conversations and data stored in online services) from servers of private companies (and the largest providers of Internet services and devices) such as Google, Apple, Facebook and Microsoft. PRISM collects mails, browsing histories, social media activity, voice chats and multimedia from servers, is legalized under controversial section 215 of the Patriot Act and protected by gag-orders (see chap. 4.4.7.2 Policy: The Patriot Act and Intelligence Reform (2001 - 2004)). The data seemed to be obtained by NSA either directly by request without the need for wiretapping, or by intelligence sharing, obtained by the FBI in the first place (The Washington Post, 2013a). According to Hayden, it was only data about foreign targets that was stored domestically on US servers, like terrorists using a Gmail account (Hayden, 2016b, p. chap. 20). The participating companies denied the cooperation – which could be the result of the gag orders – and are legally protected from law-suits with the FISA Amendment Act of 2008. However, leaked documents describe another NSA program called MUSCULAR that aims at "copying entire data flows across fiber-optic cables that carry information among the data centers of the Silicon Valley giants" probably using the aforementioned splitter technique (see chap. 4.4.7.3 Artifacts: NSA and the Full-take Norm of Internet Control (2001 -)). MUSCULAR is said not to require a FISA warrant but collects "twice as many data points ("selectors" in NSA jargon) compared to the better known PRISM" (Gellman & Soltani, 2013). According to NSA power-points, the PRISM program is closely tied to the aforementioned UPSTREAM data collection at IXP that was already established under Bush.

Another noteworthy program called MAINWAY seems to resemble the legacy of TIA (see chap. 4.4.7.3 Artifacts: NSA and the Full-take Norm of Internet Control (2001 -)). It does social network analysis of the various SIGINT data collected with other programs to create networks of associations. "N.S.A. correlates 164 "relationship types" to build social networks and what the agency calls "community of interest" profiles, using queries like "travelsWith, hasFather, sentForumMessage, employs." It is "large-scale graph analysis on very large sets of communications metadata without having to check foreignness" (Risen & Poitras, 2013).[169] This program possibly can reveal the innermost secrets of a person because pattern of life analysis can determine sexual preferences or

[169] Fred Kaplan did the math: "Imagine someone who had dialed the number of a known al Qaeda member, and assume that this person had phoned 100 other people over the previous five years. That would mean the NSA could start tracking not only the suspect's calls but also the calls of those 100 other people. If each of those people also called 100 people, the NSA—in the second hop—could track their calls, too, and that would put (100 times 100) 10,000 people on the agency's screen. In the third hop, the analysts could trace the calls of those 10,000 people and the calls that they had made—or (10,000 times 100) 1 million people. In other words, the active surveillance of a single terrorist suspect could put a million people, possibly a million Americans, under the agency's watch" (Kaplan, 2016, p. chap 13).

political orientation based on association data (Jernigan & Mistree, 2009). Closely connected to MAINWAY is MARINA, a metadata program that "tracks a user's browser experience, gathers contact information/content and develops summaries of target" conducting pattern of life analysis. MARINA can look back on 365 day's "worth of DNI metadata", regardless of "whether a person is a NSA target". James Ball argues that there are millions of users in this database (Ball, 2013). Another TIA legacy can be found in an unnamed program that is "harvesting huge numbers of images of people from communications that it intercepts through its global surveillance operations for use in sophisticated facial recognition programs" (Ball, 2013). This program seems to be in operation since 2011 and aims to create a database of biometric information that can be used for precision targeting and can track people when they cross borders. This system is connected to other databases such as PINWALE, TIDE (Terrorist Database) and PISCES, a system that is collecting "biometric data on border crossings from a wide range of countries" (Risen & Poitras, 2014).

The need-to-share norm found its manifestation in a program called XKEYSCORE, a mass storage and information management system or database that combines many NSA programs into one searchable database. To make sense of the vast amounts of data NSA and its partners obtain via tapping into fiber optic cables with programs such as TEMPORA, FASCIA, MUSCULAR, Squeaky Dolphin, SOMALGET and PRISM, an interface is needed that can organize these data points, to make them usable and searchable. Edward Snowden described the functions as following:

> "You could read anyone's email in the world, anybody you've got an email address for. Any website: You can watch traffic to and from it. Any computer that an individual sits at: You can watch it. Any laptop that you're tracking: you can follow it as it moves from place to place throughout the world. It's a one-stop-shop for access to the NSA's information. […] You can tag individuals […] Let's say you work at a major German corporation and I want access to that network, I can track your username on a website on a form somewhere, I can track your real name, I can track associations with your friends and I can build what's called a fingerprint, which is network activity unique to you, which means anywhere you go in the world, anywhere you try to sort of hide your online presence, your identity" (NDR, 2014).

XKEYSCORE also marks the global diffusion of this surveillance system and its underlying logic and norms since it is used by various Western intelligence agencies around the globe. The German investigation into BND-NSA cooperation revealed this (Biselli, 2016). It is an actant in that regard (Latour, 2005b), a non-human norm-entrepreneur that transports the goals and functions embedded in the system and makes

them available for a wider audience, thereby establishing a norm of practice. There are reports that third-party intelligence agencies *and* law-enforcement agencies have access to parts of XKEYSCORE.[170]

To indicate the fusion of information-war, cyber-war and mass surveillance, let me introduce another of programs. The first is a CNE program called TURBINE that was allegedly conceived by General Alexander in 2004 (see chap. 4.4.7.4 The Fusion of IW, Surveillance and Cyber-War (2003-2008)) and materializes the idea of active defense. It is said to be a semi-automatic hacking system that uses security vulnerabilities in networks and a whole set of hacking-techniques like Trojans, packet-spoofing, DNS-injections to break into networks. Theoretically it would allow "industrial scale" infection of "millions of computers". It is said to have the "capability to deploy and manage hundreds of Computer Network Exploitation (CNE) and Computer Network Attack (CNA) implants to potentially millions of implants" (Gallagher & Greenwald, 2014). Implant is an euphemism for malware, which can be used for data-exfiltration but also computer network attacks on a very large scale. The aim of this $67 million program is nothing less than "owning the net", according to its Powerpoint slide. This is a prime indicator for the norm of Internet control. "Owning" the net is a hacker term to describe skill and domination – utilizing NSA's access to worldwide Internet switches. There, a Turbine Module called SECONDDATE can become active, which enables "mass exploitation potential for clients passing through network choke points" (Gallagher & Greenwald, 2014). The communication of an entire network flowing through a hacked switch could be potentially altered and exploited. On NSA's Powerpoint slides it is called "a more aggressive approach to SIGINT", yet again manifesting General Alexander's idea of "active defense". It is said to be in use in the US, UK and Japan (Gallagher & Greenwald, 2014).

Closely connected to TURBINE is QUANTUM, a set of different CNE, CNA and CND capabilities. This system could be used for surveillance, CNA and economic espionage, for example against European partners like Belgium. According to der Spiegel, "Belgacom's network engineers were targeted by GCHQ in a QUANTUM mission named "Operation Socialist" – with the British agency hacking into the company's systems in an effort to monitor smartphones" (Gallagher & Maass, 2014). This operation is said to be part of a wider initiative to target administrators of computer networks with spear-fishing attacks in order to gain access to the networks they administer. Similar techniques are said

[170] Among them the German BND and Verfassungschutz, Swedish FRA, Australia's Signals Directorate, New Zealand's Government Communications Security Bureau, British GCHQ and allegedly third party intelligence agencies in Belgium, Denmark, France, Italy, Japan, the Netherlands and Norway (Rensfeldt, 2013).

to have been used to target German companies Stellar, Cetel and IABG (Poitras, Rosenbach, & Stark, 2014). These companies provide satellite Internet communications to remote places like Oil-drilling platforms or armed forces in the field and are connected to major EU Internet backbones. They also offer service to German companies as well as government communications (defense ministry and Bundeswehr), which makes them a lucrative target for economic espionage as well as for the aforementioned preparation of information war in peace time (see chap. 4.4.2.3 Core Ideas: Information Weapons & Digital Battlespace). According to the leaks, British GCHQ got access to the networks they administer, "spying on the Internet traffic passing through these nodes". This and other data have been used to create profiles of the leadership of 122 states and filing them in a "Target Knowledge Database". This database is said to allow the creation of profiles of state leaders, among them Angela Merkel, Bashar Al Assad and Yulia Tymoshenko. For Merkel, the database included 300 citations, "derived from intelligence agencies, transcripts of intercepted fax, voice and computer-to-computer communication", in other words a multitude of different surveillance programs. Similar authorization is said to exist for "China, Mexico, Japan, Venezuela, Yemen, Brazil, Sudan, Guatemala, Bosnia and Russia" (Poitras, Rosenbach, & Stark, 2014). This is very much in line with what has been envisioned with the information warfare doctrine of the 1990s: using CNE to create leadership profiles of the enemy and allied heads of states, to "penetrate their thinking" and to gain advantages, for example in state negotiations (see chap. 4.4.2.3 Core Ideas: Information Weapons & Digital Battlespace).

In a similar vein, 2010 "Operation Shotgiant" allegedly targeted the network infrastructure of Chinese IT-giant Huawei. During this CNE, NSA obtained information about the workings of Huawei routers and switches, which connect a third of the world's population with the Internet, in China but also in Western countries. "The N.S.A. could roam through their computer and telephone networks to conduct surveillance and, if ordered by the president, offensive cyber-operations" (Sanger & Perlroth, 2014). Unknown security vulnerabilities in Huawei switching hardware would be highly valuable for launching offensive cyber-attacks, underscoring once more the close connection between CNE and CNA.

Closely connected is another program called BULLRUN, which is described by journalist Greenwald as, the "biggest threat" to "the use of ubiquitous encryption across the Internet" (Ball, Borger, & Greenwald, 2013). Good encryption is a cornerstone of effective cyber-security and is used in services such as online-banking and shopping (HTTPS and SSL protocols), in Virtual Private Networks (VPN) that companies and universities use to

connect to their networks from afar, or even by government and military organizations to maintain sensitive information. NSA spends $250 million annually to influence the design of encryption products to implement so-called Backdoors (secret access) and calls this the "price of admission for the US to maintain unrestricted access to and use of cyberspace" (Ball, Borger, & Greenwald, 2013). The list of private collaborators is protected by the highest classification possible. By introducing artificial vulnerabilities into software that promises uses secure communication, NSA undermines the "fabric of the Internet" such as "security and privacy", according to IT specialist Schreier, quoted in the article (Ball, Borger, & Greenwald, 2013). Bullrun also shows that the NSA did not stop its war on cryptography after its Clipper failure (see chap. 4.3.5.1 Policy: The Clipper Chip (1993)).

A final example underscoring the synergy between surveillance, information and cyber-war is "Operation Rolling Thunder" of GCHQ, a little known information- and cyber-war campaign against Anonymous in 2011. The aim of GHCQ hackers was very much in line with the US information war doctrine: to "destroy, deny, degrade [and] disrupt enemies by discrediting" them and "planting misinformation and shutting down their communications" (Cole et al., 2014). This was done by using Anonymous very own CNA of choice, DDoS attacks, but also included information-war and "propaganda campaigns use deception, mass messaging and pushing stories via Twitter, Flickr, Facebook and YouTube" and "false flag operations, in which British agents carry out online actions that are designed to look like they were performed by one of Britain's adversaries" (Cole et al., 2014). In sum, Snowden claims that NSA conducted over 61000 cyber-attacks until 2013 (Kaplan, 2016, p. chap. 13)

All of these leaks produced a crisis questioning the legitimacy of surveillance in general (Schulze, 2015). Although there have been intelligence scandals before (2005 with the warrantless wiretapping program, and 2000 with the leak of the Echelon spying network), this was undoubtedly the one with the most international resonance, resembling a shock for cyber-realism. The public's acceptance of mass surveillance began to shift from majority support to opposition (Rainie & Maniam, 2016). This trend was facilitated because IC officials denied the existence of the mass surveillance programs back in March 2013 during a congress-hearing. There, Senator Ron Ryden asked DNI Clapper whether NSA does "collect any type of data at all on millions or hundreds of millions of Americans?" Clapper replied, "No, sir . . . not wittingly" (Kaplan, 2016, p. chap. 13). After the Snowden leaks, Republican Senator Rand Paul complained that DNI "Clapper lied in Congress, in defiance of the law, in the name of security. Mr. Snowden told the truth in the name of privacy" (Landau, 2013, p. 55). Former Vice President Al Gore attacked the

government practice as unconstitutional because it clearly violates the Fourth Amendment (Landau, 2013, p. 54).

Initially, the White House defended the bulk-telephony metadata-retention program based on a controversial interpretation of Section 215 of the Patriot Act (The White House, 2013). Because of the public and international diplomatic outcry from allies, President Obama was driven to set up a review board, evaluating two of the most controversial programs (but not all of them, which is an important caveat). Thus, the juncture continued over the course of 2013. For better readability, the report of the evaluation panel and the ideas and critique it includes, is presented in the next chapter.

4.5.6 Juncture: The President's Panel on NSA Practices

On 9th August 2013, Obama gave a press-conference on the Snowden leaks. Highlighting his "healthy skepticism" (The Washington Post, 2013b), he announced a balanced review of these programs. A committee would make suggestions for intelligence reforms on August 27th 2013, with a final report due to the end of the year 2013. This panel included several high-ranking US intelligence officials such as former Bush cyber-czar Richard Clarke, former CIA director J. Morell, but also two constitutional lawyers and one first amendment scholar. It can be said that the panel was rather balanced since it included insights from both the IC and from a more privacy-focused legal perspective.

The general gist of the report is a critique of radical cyber-realist provisions that were legalized within the framework of the unitary executive theory. Cyber-realism is seen as an unbalanced approach to national security, realizing primarily the *particular* interests of state actors (military and IC) but not the *universal* interest of the general public (both within the US but also internationally). In the very beginning the report states that there are two sides to security: national security but also "the right of the people to be *secure* in their persons, houses, papers, and effects, against unreasonable searches and seizures" (Clarke et al., 2014, p. 15), as reflected in the 4th amendment. Privacy is another variant of security and particularly relevant on the Internet. While on the one hand acknowledging the new threat of terrorism, the report argues that the government overreacted after 9/11 (Clarke et al., 2014, p. 53), focusing exclusively on risks to national security while ignoring the risks that come with an expanded national security apparatus: risks to privacy, to freedom and liberties, to commerce but also the risks to the relationship to other nations (a clear reference to the spying on Angela Merkel’s phone). Because the "natural tendency of government is toward abuse of power" and the "tendency of intelligence activities to expand beyond their initial scope", to "generate ever-increasing demands for new data",

which all thrives in secrecy (Clarke et al., 2014, p. 58), the FISA system was put in place. However, this system was severely changed with post-9/11 legislation. The report criticizes many of the legal provisions of the Patriot Act that changed or circumvented the FISA system (see chap. 4.4.7.2 Policy: The Patriot Act and Intelligence Reform (2001 - 2004)), for example the general suspicion (vs. prior individualized suspicion), the issuance of National Security Letters with gag orders,[171] the increased classification to prevent public disclosure, the repeated bypassing of legal checks and balances and the bulk-collection of telephony metadata under section 215. Although new digital technologies allow for more information to be gathered, it does not logically follow that the government *should* collect everything. The government should resist the temptation of the full-take approach – collecting everything just because it might be useful in the future (Clarke et al., 2014, p. 48). The report argues for a norm of democratic restraint that should make democratic surveillance and intelligence regimes structurally different from their counterparts in authoritarian regimes.

They criticize that in many instances empirical evidence is lacking whether more intelligence is helpful and that "the abstract possibility does not, by itself, provide a sufficient justification for acquiring more information" (Clarke et al., 2014, p. 51). This argument seems to stem from interviews that the panel held with NSA and FBI members where they learned that not a single terrorist had been caught with the help of the meta-data surveillance system.[172] According to Clarke, who was very skeptical, this begged the question why this controversial system was kept in place if it had not produced any results (Kaplan, 2016, p. chap. 14).

Besides questions of efficiency, there are also fundamental *legal issues*. The panel also learned that domestic communication indeed inevitably was caught with this dragnet technique because of packet-switching, which made it impossible to distinguish between foreign and domestic data-packets (see chap. 4.4.8 The Norm of Internet Control). This was no accident but *intentional design*. To find the needle in the haystack, the whole haystack had to be scanned. NSA operated according to the logic *collect first and check for relevancy later* (inductively so to speak) whereas since the 1970s, the rule of law was based on a deductive approach: have a suspicion first, get a warrant and then conduct surveillance. An important question the reviewers asked is, what happened with the

[171] According to the report, in 2012 FBI issued 21000 NSL and 97% included a gag-order, highlighting how normalized this practice has become (Clarke et al., 2014, pp. 90-92). Gag orders effectively prevent third parties to take legal measures against the disclosure demand.

[172] "Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders" (Clarke et al., 2014, p. 104).

haystack after the search. According to the FISA Amendment Act of 2008, the data had to be deleted but the panel quickly realized that there is an enormous potential for abuse and a potential threat for democracy. The same was true for the questionable practice of National Security Letters with gag-orders issued by the FBI. Neither had there been any evaluation regarding the effectiveness, nor was there anyone monitoring that practice. The FBI had a relatively free-hand and there was no chance for judicial control because gag-orders prevented the court of law (Kaplan, 2016, p. chap. 14).

In sum, the panel indicated that the IC overstepped by putting in place a mechanism resembling a totalitarian logic. In contrast to totalitarian states, the democratic rule of law sets limits to intelligence gathering, for example that surveillance should not be collected to punish political enemies or suppress dissent (as happened in the 1970s). Some of the new surveillance provisions violated this democratic core principle. The panel argued that when people realize they are being monitored, associational and expressive are freedoms hindered. This might create chilling effects for the democratic process and increase public mistrust in government conduct (Clarke et al., 2014, p. 117).

To remedy these problems, the 300-pages report makes 46 recommendations (henceforth called "Rec") which are full of normative statements, of which I only can discuss a few. One general theme is better *legal, congressional oversight and transparency,* reinstating lost checks and balances. Section 215 should be altered to reinstate the principle that third parties have to inform their customers of government searches (Rec 1). National Security Letters should follow normal warrant standards (Rec 2). As a general rule: "without senior policy review, the government should not be permitted to collect and store all mass, undigested, non-public personal information about individuals to enable future queries and data-mining for foreign intelligence purpose" (Rec. 4). Data collection for terror-prevention is seen as necessary, but should be permitted only upon senior executive and legal review (creating accountability). Rec. 7 demands that Congress should be informed annually about the issuance of NSL and the number of warrants obtaining of business records (under section 215) and the installation of pen registers and trap-and-trace devices (under section 702 FISA Amendment Act of 2008). Disclosure of such information to Congress and citizens should be the norm in a democratic society and not covered in classification. Big, far-reaching programs such as NSA metadata retention should not be kept secret from the public, and can only remain classified by providing strict legal justification (Rec 11). For such programs, the President should create a high-level approval process, creating better official accountability (Rec 16).

Another theme is the *limitation of the increased quantity and quality of post 9/11 surveillance technology*. Bulk meta-data collection by NSA should be prohibited. Instead, a third party should maintain the data and NSA still should be able to access it with a FISA warrant (similar to EU data retention policies). Rec. 6 asks for a rethinking of the 1970s idea that meta-data does not contain private information (which with digital communication, it increasingly does). The surveillance of foreign leaders and allies as well as economic espionage should be stopped (Rec. 31), unless there is substantial reason not to (Rec 19). NSA surveillance should return to the pre-9/11 targeted approach, instead of following the full-take principle (Rec 20). The NSA should return to its original mandate being a foreign-oriented agency, effectively scaling back the expansion and power-grab of NSA (Rec 23). As was shown before, after 9/11 NSA's ears were turned to domestic soil, which was originally the domain of the FBI (see chap. 4.4.7.3 Artifacts: NSA and the Full-take Norm of Internet Control (2001 -)). In a similar vein, the government should conduct a technological assessment of Big Data and data-mining programs, determining the effects on civil liberties and evaluating cost-effectiveness (Rec 35). The impact of future surveillance programs should also be assessed by an independent expert group (Rec 36). The general theme of this is a critique of the haystack approach or full-take principle to sweep up and analyze as much data as possible. The data-sharing practice (need-to-share) created security vulnerabilities and privacy issues, because more agencies (and third parties) than necessary can access critical data and there is no accountability who has access. The need-to-know principle should be reinstated and updated with a work-related access model which ensures that only analysts that really need the data can obtain it (Rec 41). The loose sharing-culture, which also includes private corporations should be reduced. The report maintains that the need-to-share norm also creates security problems: much of the gathered data is unencrypted and theoretically can be accessed by third parties.

A third theme is *reestablishing the balance between military and IC interest vis-à-vis the public interest*, in other words, reducing cyber-realist hegemony by questioning the supremacy of the military and IC in cyberspace issues. The DNI should be a senate-confirmed position (Rec 22). In general, the blurring of domestic law-enforcement and foreign intelligence is criticized. Another theme is reducing structural dominance of the military and IC within the intelligence process by creating a counterweight in form of civil actors which represent the general public's interest (the other side of security so to speak). Rec 27 proposes the creation of a Civil Liberties and Protection Board that oversees IC activities and should be open to whistle-blower complaints. Within the FISC, there should be a Public Interest Advocate, so that the judges would hear both sides of a story, and not

just the IC perspective before issuing a warrant. Rec 28 also argues that the transparency of FISC decisions should be increased by declassifying them, increasing public accountability. Congress should also reconsider the appointment of judges and the review-procedures for warrants. Also, FISC should build better technical expertise (because the old judges often cannot comprehend the scope and technicalities of surveillance programs they approve).

Finally, the report also addresses cyber-war and argues for a *demilitarized perspective on cyberspace*: "even where a military rationale exists for information collection and use, there increasingly will be countervailing reasons not to see the issue in purely military terms" (Clarke et al., 2014, p. 187). It argues for a clear separation of the functions, cyber-security/network defense (information assurance), surveillance (SIGINT) and cyber-offense (CNA). These functions should not be fused together under one agency (NSA). The report confirms positions put forward repeatedly by the computer science community that argue that computer network defense (information assurance) and offense have conflicting interests, which weakens global cyber-security. Offense benefits from insecure systems, while defense aims to make them more secure: "when the offensive personnel find some way into a communications device, software system, or network, they may be reluctant to have a patch that blocks their own access" (Clarke et al., 2014, p. 192). This addresses NSA's practice to hoard zero day vulnerabilities instead of patching them, which is in contrast to industry security best-practices. NSA does this because these weaknesses are necessary for offensive cyber-attacks, which is the reason why these functions should be separated. The director of Cybercommand and NSA should not be a single (NSA-) official (Rec 24). Protection of domestic networks should be the responsibility of DHS (which operates under a different legal regime compared to NSA) and not that of NSA. While it legally is, DHS lacks NSA's resources and technical sophistication. For that reason, NSA's Information Assurance Directorate, responsible for network protection should be a separate agency, reporting to the DoD (Rec 25). This could ensure that DHS gets state of the art network-defense technology and tools to execute its legal mandate.

In theoretical terms, the report criticizes the hegemony of cyber-realist principles and norms that guide US cyberspace policy. The Internet should not be seen primarily as a military or intelligence issue, subsuming everything under this guiding frame, thus increasing the further militarization of cyberspace. It questions the legitimacy of the norm of Internet control driven by the idea of total information awareness.

The interesting question now is whether this report was effective and how many of these measures were implemented. In January 2014, President Obama announced the changes (McCarthy, 2014). In his speech, the hybrid presidency became visible again. On the one hand Obama argued: "As the nation that developed the Internet, the world expects us to ensure that the digital revolution works as a tool for individual empowerment, not government control" (Obama, 2014). However, on the other hand he did not end any of the leaked surveillance programs. Critics argue the changes were rather cosmetic. Obama made clear that although there is enormous potential for abuse, and that the IC has the inherent bias "to collect more information about the world, not less" he will not end the programs because they make America and its allies more secure. They secure not just against terrorism but against foreign intelligence agencies and cyber-threats, highlighting yet again the fusion of surveillance and cyberwar. However, he acknowledges that trust has been lost and that the American citizens should not blindly trust the good intentions of the Government, so as a results he put forward several initiatives that aim at greater transparency and trust-building (Obama, 2014).

As a reaction, the government declassified a lot of material describing the legal rationale behind some, but not all, of their surveillance programs based on Section 215 of the Patriot Act and Section 702 of FISAAA. The storage of US citizen's phone records would be moved away from NSA, because of potential abuses. However, it still has access to it via FISA or inter-agency intelligence sharing (Harris, 2014, p. chap. 14). Contact-chaining and social-network analysis of meta-data is now limited to two hops. According to Michael Hayden, President Obama cancelled the spying on international organizations such as the UN, the World Bank, the IMF and some state leaders like Angela Merkel (Hayden, 2016b, p. chap.20), but a future President could reinstate this. The IC must apply to the FISA court, which was the law anyway. The FISA court will now include a public interest advocate to balance the dominance of the IC in the hearings and will be equipped with better technical expertise because the review panel found out that the old FISA judges often lacked the technical know-how for understanding what they were legitimizing. However, large portions of the programs remained untouched. It must be kept in mind that the Obama initiative and the review panel only focused on a fraction of the surveillance practices, i.e. domestic telephony meta-data retention under section 215 of the Patriot Act and section 702 of the FISA Amendment Act. The other leaked programs or even the question of the legality of the NSL-system were never part of the evaluation and remained largely unchanged. The government still scoops up large portions of Internet traffic and analysts can search their databases without the need for warrants, as the President’s panel

suggested. Most changes affected NSA, but the FBI, which does a substantial part of domestic surveillance, remained untouched. It still can issue NSL and secret gag orders, against which the President's panel argued, although the NSL now can expire, unless the FBI writes a letter that it should not. According to the EFF, the move "doesn't fix the constitutional problem," […] "that there's a gag order when [a letter] is issued, without any judicial involvement or showing that there needs to be a gag" (Childress, 2015). The bulk-collection of telephony metadata is still in place as well. NSA contractor Snowden was charged with espionage, based on a broad interpretation of the Espionage Act of 1917, although "leaks of classified information to the press have relatively infrequently been punished as crimes," according to a Report from Congressional Research Service (Landau, 2013, p. 54). This, again is evidence for the war-paradigm that drives cyber-realism and replaced the law-paradigm of the 1990s. Before leaving office in 2016, Obama announced that the head of US CYBERCOM would be separated from the NSA (Nakashima, 2016).

In sum, cyber-realism survived this shock situation with a mix of pragmatism, endurance and power-politics, prioritizing national security interests over norms and values such as the protection of privacy, which represents a classical realist line of thought. Cyber-realism ultimately reached hegemony and it would require a strong political will to break with these established norms of total control or even implement a few of these proposed changes (Diersch, 2014). In the wake of more terrorist attacks, the public's support for these surveillance measures increased again (Rainie & Maniam, 2016). During the presidential election of 2016, both candidates supported more surveillance powers with only a minority of politicians opposing the expansion of the surveillance apparatus. The dominance of cyber-realism will be quantified in the next chapter.

4.5.7 Outcome: The Dominance of Cyber-Realism

The purpose of this chapter is to assess the dominance of cyber-realism and its ideas within the United States. If cyber-realism is indeed the dominant paradigm, we should see some spill-over into public and elite opinion. To check for that, I will use several opinion polls to assess whether the cyber-doom discourses and the elite's attitudes toward the topic had a wider societal impact. Due to time and financial constraints I could not conduct my own survey of US public opinion in order to test whether cyber-realist or utopian frames are dominant within the general public. To make such a judgement, one would require a longitudinal survey of the publics' attitude towards the Internet, starting in the mid 1990s, which then should be repeated during certain intervals. Ideally, it would include items or frames distilled from each paradigm (like "How much do you agree with the statement

"information should be free"?), which would allow us to compare the attitudes before and after say, 2010, when the cyber-doom discourse was highly relevant or before and after Snowden. Such a study does not exist. Therefore, I rely on my own findings and that of other studies, which of course use different questions and items and thus are not always comparable. These polls provide some very limited evidence on the dominance of cyber-realism.

In previous chapters I have shown that during the early 1990s, the general public was skeptical towards government attempts towards Internet control. A majority of citizens opposed the Clipper initiative (see chap. 4.3.5.1 Policy: The Clipper Chip (1993)) and argued that privacy on the Internet is more important than national security (see chap. 4.3.5.2 Policy: Wiretapping the Internet with CALEA (1994)). Both Democrats and Republicans were skeptical of government control of information technologies, indicated by the dictator's dilemma that was widely acknowledged by policy-makers and independent institutions like the Supreme Court. This changed with the dominance of cyber-realism.

In 2011, the Internet Society conducted its first global Internet survey (Internet Society, 2011) asking over 6000 Internet users (from different countries) about their opinion on different topics (see appendix Polls on the Dominance of Cyber-Realism). The survey is interesting because it includes some utopian items such as privacy, net-neutrality, censorship and open access, as well as cyber-realist topics such as the question of Internet control and surveillance. Unfortunately, this provides only a snapshot view and allows no before/after comparison. The following table summarizes the findings for the US Population (N=1001).

Table 7. Internet Society Survey 2011, Source: (Internet Society, 2011)

	Agree (including agree somewhat) in %	**Disagree (including disagree somewhat) in %**
20. There should be no restrictions on accessing lawful content via the Internet.	73	27
21. There should be no restrictions on lawful software or services on the Internet.	66	34
23. The ability to share and access information privately using the Internet is important to me.	94	6
24. The Internet needs to be controlled to protect end-users.	64	36
25. The Internet needs to	58	42

remain as uncontrolled as possible to promote innovation.		
Source: http://www.internetsociety.org/survey (2011)		

The first two items that ask about restricting content on the Internet show the tendency that the majority of Internet users in the US still adheres to the "hands-off" norm, specifically that there should not be any type of censorship on the net. For them, the Internet is, as the original designers intended, about sharing and the free flow of information. The picture is not as clear when it comes to the items of whether the Internet should be controlled, which leaves open the question: by whom? Users generally favor control of the Internet when it is about security and protection. However, the question is quite open (Protection from what? Who should protect etc.?). Other items (see appendix Polls on the Dominance of Cyber-Realism) ask about what the *greatest concern facing the Internet is*. 30% of users say privacy, followed by the security of the infrastructure (26%), spam (21%), government control (12%), net-neutrality (5%) and a few minor items. This is not a clear tendency. Interestingly, 12% strictly still oppose government control of the Internet, the core cyber-utopian norm of the early 1990s. This indicates the relative decline of cyber-utopianism. On the other hand, privacy is a major concern. Interestingly, a final item asks about "*How concerned are you that the Government is monitoring your use of the Internet?"* and 46% are very, 32% somewhat, 17% not very and 5% not concerned. Interestingly, the US numbers are higher than the global average (Internet Society, 2011). Unfortunately, this is only a snapshot and allows no comparison with the post-Snowden timeframe.

The dominance of these cyber-realist threat narratives or ideas have been measured by other researchers (see appendix Polls on the Dominance of Cyber-Realism). For example, Pew research conducts an annual telephone survey, giving Americans a list of national security threats, asking them to rate them according to the most severe ones. In the 2013 poll, *fear of cyber-attacks from other countries*, for the first time, entered the list of major threats. 70% of the survey participants see cyber-attacks as a major concern, second place only to international terrorism (75%). Unfortunately, the cyber-attack item does not appear before 2013 but it nevertheless shows the increased significance since otherwise the item would not be included after all.

A Gallup poll with a similar methodology asks about critical threats for the US and replicates this finding. Cyber-terrorism, i.e. *the use of computers to induce fear* (73%) appears on the top-list of critical threats for the first time in 2016, third after nuclear weapons in Iran (75%), and international terrorism (79%). This is noteworthy because in

the history of cyber-security, there has not been a single successful act of cyber-terrorism causing physical harm. Nevertheless, the threat-frame of cyber-terrorism and digital 9/11 make this issue to appear more real and more dangerous than it is. This could be a consequence of the cyber-doom discourse. Of course, the question of causation cannot be answered because there exists no data before 2013. The case can be made that the elite talk about the issue and spectacular media coverage increased salience of these issues within the general public, which in return facilitates more elite discourse.

That the Snowden shock did only temporarily contest cyber-realism can be shown with the following Pew Study that found out that directly after the Snowden leaks, a majority was indeed critical of Internet surveillance practices, but the pendulum swung back after successive terrorist attacks, for example the San Bernardino shooting or because of the visible threat of the so-called "Islamic state" in the Middle East (Rainie & Maniam, 2016).

The dominance of cyber-realism can also be shown by elite support for its ideas, norms and policies. The continuity of programs under Obama and Bush also has shown that there is a bipartisan consensus on these issues: cyber-war and surveillance are here to stay. Within the US political system, there are only a few, often strongly democratic (Sen. Ron Wyden) or strongly libertarian (Sen. Rand Paul) politicians who oppose more surveillance capacities. In the 2016 presidential campaign, both Hillary Clinton and Donald Trump supported the extension of the intelligence apparatus in the war against terror, including controversial policies such as demanding government-enabled backdoors into otherwise secure cryptography (Elmer-Dewitt, 2016). The website ISideWith.com condensed the most important positions of the candidates with regard to the Internet and compared it to public opinion (ISideWith.com, 2016).[173] Regarding surveillance, Donald Trump argued that *basic data-collection of US citizens is necessary to track terrorists* and even supported a database for Muslims within the US (racial profiling based on surveillance data). Hillary Clinton opposed, and so did the general public (only 31% agree, 69% opposed). When asked whether the US should monitor allied heads of states via NSA surveillance (that was stopped by President Obama after the monitoring of Angela Merkel's cellphone was discovered), Donald Trump argued in favor, while Clinton opposed. Regarding this item, the general public was also in favor (52% yes, 48% no). Both candidates supported the Patriot Act and both argued that Edward Snowden should

[173] ISideWith.com is a useful resource to track the original statements of the candidates regarding the question items. However, the public opinion is measured via an online poll with approx. 3-4 million votes per item. However, since users have to participate voluntarily, it might not be the most representative survey (ISideWith.com, 2016).

not be granted immunity from prosecution under the Espionage Act. The underdog candidates Jill Stein (Green) and Gary Johnson mostly argued against these practices but only received a small fraction of the votes in the 2016 election (ISideWith.com, 2016).

President Trump's picks for key positions such as FBI- or CIA-director or Attorney General included only strong cyber-realists who in the past opposed restraints put on NSA. General attorney Jeff Sessions for example is a strong advocate of Internet surveillance without the need for warrants (Strohm, 2016). Thus, it is very likely that both Internet surveillance and offensive computer network attacks will likely grow under a President Trump and a Republican controlled Congress.

One effect of the Snowden leaks was an increase in encrypted Internet traffic that could not be read by the NSA spying infrastructure and thus NSA and the FBI began lobbying efforts to gain "exceptional access" to wiretap secure, encrypted communication. When asked about this, Donald Trump supported this. Thus, a new war on cryptography, like Clipper in 1993 is likely going to happen within the next few years. In Europe, a similar initiative is pushed by France and Germany and most states have started to build technical capacities for CNO, breaking into encrypted messenger systems such as WhatsApp or Telegram (Schulze, 2016b).

The irony of the Snowden leaks is that they made the world aware of these practices. The leaked tools created a demand-pull where intelligence agencies worldwide began to lobby their governments for similar capacities. Especially foreign intelligence agencies like Russian and Chinese agencies closely monitored the leaks and soon began to draft wish-lists. Since Snowden, most Western democratic *and* authoritarian regimes adopted very similar legislation and gave their intelligence agencies similar surveillance and cyber-war capacities. In the wake of the Paris attacks, France gave its services broad Internet surveillance powers (Pick, 2015). The United Kingdom initiated its "Investigatory Powers Bill", characterized by critics as the most extreme surveillance law in any democratic state (MacAskill, 2016). The German government initiated the process of legalizing many Internet control practices of its BND (Mützel, 2016). Since early 2017, the German domestic intelligence agencies demand similar competencies as their NSA counterparts, for example the capacity for "active defense" or hacking back (DPA, 2017). A recent, quite alarmist report from Amnesty International found similar initiatives in Austria, Belgium, Hungary, the Netherlands and Poland, (Amnesty International, 2016). Thus, the case can be made that the example of NSA's internet surveillance and cyber-war artifacts, leaked by Edward Snowden, accelerated the diffusion of Internet control as a global norm, even among democracies.

4.5.8 Critical Analysis

Cyber-realism itself has some blind spots that deserve a critical discussion. Within the cyber-realist paradigm, espionage is presented to be normal or appropriate behavior: "competitive espionage are [is] the expected manner of conducting business" (Schwartau, 1997, p. 50). Controlling cyberspace and information therein is framed as a necessary practice, although modifying information stored on another nation's servers breaches the Westphalian sovereignty rights of other nations (the principle of non-intervention). CNA and CNE violate this principle, if their targets are located in another state (Betz & Stevens, 2012, p. 61). If CNO are indeed to be classified as weapons, then the attack on another country's digital infrastructure might be equitable with an act of war. Cyber-realists seldom explain why exploiting other nation's information networks is a legitimate or rightful thing, it is just demanded that this must be a capability. Another issue is the constant nature of the doctrine that does not differentiate clearly between war and peace. During an armed conflict, a CNA against military or civilian networks might be lawful according to the laws of armed conflict, but in peace time it is not.[174] This is particularly important because the primary target of IO are critical infrastructures which are mostly civilian in nature (like banking, electricity, transport). This might violate the principle of necessity in armed conflict.

Second, the cyber-war crippling strike narrative is probably overblown. There are lots of hypotheticals, which remain untested. The worst-case scenario of shutting down an entire nation by a cyber-attack simply did not happen (yet). Until today, no-one has died because of a cyber-attack. Even in spectacular cases like Stuxnet, the effect was rather limited. Advocates argue: "but it could happen!". Indeed, but even if adversaries have the possibility, it does not follow that an attack is probable. There needs to be further incentive and most likely physical force to maintain the often short term effects of cyber-attacks. More so, even if something happens, catastrophe does not logically follow. There is no determination between successful CNA, a societal blackout and mass casualties, as Lewis (Lewis, 2002) and Lawson (Lawson, 2011) show in their studies. A Hurricane or Tornado can be more devastating than a cyber-attack, but panic rarely occurs. Rid (Rid, 2012) argues that because of tech-determinism, cyber-war advocates *overestimate the*

[174] An Assessment of the legal status of information operations by the DoD reaches the same conclusion (Department of Defense, 1999, p. 8).

decisiveness of strategic cyber-war[175] against critical infrastructure much in the same way as theorists of air power overestimated the decisiveness of air power.[176] RMA is driven by the idea to end wars quickly, from far away, if possible without own casualties. The belief is that a critical precisions strike on the enemy leadership could end war is theoretically true, but practically problematic. Even if attacks shut down critical infrastructure of an information economy, the decisiveness of this attack might be limited.[177]

Third, these fallacies might have security implications that are overlooked by cyber-realism. Cyber-realism is based on a technological bias: the idea that technology can mediate human imperfection in data-processing. But computers are human-made machines that do not have full artificial intelligence and are not perfect. They, too, make errors and crash. Additionally, one of the reasons why it took so long to kill Bin Laden was that he avoided using digital technologies. His communications system relied on carriers of trust that could not be intercepted. Terrorists of the future most likely will write physical letters or use oral telegrams, because digital surveillance does not work here. We already see the increased use of steganography, hiding messages in images and paintings. The technological response to terrorism prevents effective social mechanisms like community policing, deradicalization programs, integration and education policies that aim to tackle the root causes of terrorism: personal grievances, hopelessness, personal isolation, ideology and arms training, often perfectly combined in civil wars in failed states.

Another problem that is ignored by cyber-realism is *data storage and data security*. Recent history is full of data-breaches where criminals stole private and public data. The data breach of the US Office of Personnel Management in 2014, where security clearances and private information of government employees were stolen by a foreign power serve as a warning example (Office of Personnel Management, 2015). The more intelligence data is stored and shared between multiple parties, the more susceptible it becomes for exploitation and manipulation (i.e. cyber-war) by external third parties. The trend to privatization of surveillance and outsourcing of intelligence to private companies produces a whole set of difficult issues that cannot be addressed here. It is important to remember that the IW doctrine assumed that intelligence data stored in databases can be used to

[175] Observe that this is not an argument against the overall utility of cyber-attacks. Cyber-attacks might be used effectively in war, but in concert with other weapons ("joint operations"). The argument is against the assumed "independent war-winning effects" attributed to strategic cyberwar.

[176] Lindsay compared the discourses on "air power of the 1930s" with the cyber-war discourse and finds that these operate with very similar frames and assumptions (death of distance because of speedy airplanes, no pre-warning mechanism, advantage of the offense, crippling blow thesis). He also presents evidence that the crippling blow thesis might be overstate because even during the heavy-allied bombardment during 1943, Germany was able to increase economic output by placing factories under-ground (Lindsay, 2013).

[177] This can be proven by looking at events where infrastructures fail, for example during hurricane Katrina, or in almost every American Winter when the power-outages cut off cities, sometimes for days (Rid, 2012).

influence decision-making and can be altered without the owner knowing. The manipulation of the ever-increasing list of data-bases by foreign hackers can produce a whole new dimension of intelligence failures, for example when innocent dissidents are placed on kill-lists or terrorist suspects are removed from no-fly lists by third party hackers.

The more general problem is that the international advancement of cyber-war and the development of CNE/CNA skills (a cyber-arms race so to speak) increases the risk of intrusion and escalation and reduces the overall security of the internetworked infrastructure. With more states hoarding zero-day exploits and writing malware to penetrate target systems, the overall global cyber-security is reduced because most states rely on similar technologies (i.e. Windows computers). This classical security-dilemma or rather prisoner's dilemma, conceived by realist scholars, is actually produced by cyber-realists, resembling a self-fulfilling prophecy.

4.4.9 Summary

With the Obama administration, cyber-realism became the dominant paradigm, after some initial hegemonic struggle between the utopian ideas, particularly put forward during the election campaign and more realist ideas becoming more salient during the actual presidency. This chapter outlines the causal mechanism for this process.

It can be argued that Obama started as a cyber-utopian. His *election campaign framed the Internet and Obama's policy in terms of utopian ideas* and norms, such as the freedom of information, net-neutrality, an anti-censorship attitude and a general positive perception of the Internet for the democratic process and the economy (part 1). He was also very critical of the extensive cyber-realist agenda of the Bush administration. However, Obama was not a wholehearted libertarian and blind follower of utopianism, so that his campaign incorporated more critical undertones as well. This has to do with timing. Obama witnessed the disenchantment of utopianism and thus represented a more educated or rational version of it, not blindly believing in all the rosy predictions. This can be seen as a learning effect of cyber-utopianism adjusting to new realities, of which the war on terror is one. Obama was aware of potential malign uses of the Internet for cyber-crime, hacking and terrorist activity. However, the positive undertones still dominated the campaign and thus a reintroduction of cyber-utopian ideas into politics was a possibility.

This changed when he entered office. Here, *Obama mostly followed the path* developed by the Bush administration, making some minor adjustments in terms of transparency. In theoretical terms, this represents incremental paradigm change in terms of

instrument settings and the formulation of some new cyber-realist goals, such as "active defense" and the "concept of equivalence" (see chap. 2.2.4 Explaining Change). How can we explain this? One argument is the staying power of the status quo and already institutionalized operating procedures in terms of IW. As was shown before, over the course of time, the cyber-realist paradigm had become institutionalized in terms of national strategy and military institutions, which recruited and educated new generations of realists, positioning those throughout leadership positions. This pre-structured the relatively new policy field of (governmental) cyber-security with cyber-realism being the dominant voice and realist institutions as the perceived appropriate actors.

Another explanation is the *structural constraint* Obama witnessed after the financial crisis as well as the gridlock in Congress. Additionally, the GWOT was still the dominant narrative of the time so that many of the ideas, norms and policies that were adopted as a response to this problem remained still valid or useful. There was not much room for completely new accents in policy compared to, for example, the Clinton/Gore administration. To utilize already available tools such as the global NSA SIGINT collection may also have been pragmatism that is required of the presidency. The perceived utility of these technical artifacts seemed greater than constitutional or ethical concerns. Thus, the general explanation for Obama's cyber-security policy is *path-dependency and the staying power of the status quo* (part 2). This can for example be shown with path-trajectories that were initiated under Bush, such as the creation of US CYBERCOM or Operation Olympic Games that were completed when Obama entered office. It was simply unfeasible to ignore these developments or alter them.

Although Obama was technologically literate, the IT-agenda was not his most pressing concern (in contrast to Gore). He rather chose to focus on domestic issues such as health care. Within the cyber-security policy field, he chose to focus on quality instead of quantity, which led to a further *professionalization and specialization of the cyber-security policy field*. Cyber-security and Internet politics became a more pressing issue around the year 2010/11 with notable events such as the Stuxnet revelation, the Wikileaks affair, the Arab Spring and the Sony Hack, all cases in which the Internet played a huge role (context). The number and quality of cyber-security incidents continued to rise as well, making this issue highly salient, even among the public (see Table 9. List of Internet Milestones and Security Incidents).

This can be shown with regard to the *public discourse,* where cyber-realists, most notably intelligence officials, used threat frames to convince the public that immediate presidential action is necessary to solve this issue. They pushed for policy changes and the

formulation of a coherent strategy. The cyber-doom discourse happened out in the open and not in secret circles as in the 1990s. Movies, newspapers and documentaries picked up the issue and *the narrative of the crippling-blow taking out the US economy became prevalent in the public* (part 3). The cyber-doom discourse had characteristics of hegemonic and naturalizing speech acts that presents the possibility of devastating cyber-attacks as some kind of natural force, the question being not if but when they will happen. This security framing shows some of the features of the early cyber-utopian discourse arguing that the digital revolution is an irresistible force leading to a determined future. The narrative had a high fidelity and is highly commensurable because of the steady news of hacking events (like the Sony Hacks or the hack of the Office of Personnel Management in 2014) representing what the cyber-realists are warning about. Furthermore, these cyber-realist advocates are seen as experts on the issue, while secrecy prevents critical evaluation of their claims. The structural composition of the cyber-security discourse increases the authority of cyber-realist advocates (Nissenbaum, 2005).

The outcome was *a new national cyber-security strategy* that gave cyber-realists new competences (like hoarding zero-day vulnerabilities and sophisticated new malware technologies) and allowed them to realize some of their strategic goals (to gather "actionable intelligence about global networks and systems, adversary capabilities, and malware brokers and markets" (Department of Defense, 2015, p. 16)). It also included offensive-driven concepts such as equating digital and physical force and the euphemism of active defense for preemptive cyber-attacks. More so, military actors and the intelligence community officially became the primary institutions defending and safeguarding cyberspace. Civil actors or private cyber-security firms were thus marginalized in this process.

While the cyber-doom discourse happened out in the open, the Stuxnet revelation was more of an expert issue (part 4). It can also be argued that the *Stuxnet revelation triggered a global norm-diffusion process* where more and more states began to formulate cyber-security policies and strategies (Shafqat & Masood, 2016) and began to mimic concepts and ideas developed in the US. In 2013, DNI Clapper argued that cyber-security replaced terrorism as the most-pressing national security issue (Boyd, 2016). This securitization was successful and thus, the cyber-security budget grew. The increased salience of the topic also increased the standing of those agencies in charge of this issue because they were able to use this window of opportunity to their advantage. All these interrelated processes (equifinality), the new cyber-doctrine, Stuxnet and hacking events and this new institutional framework further *materialized the norm of control* within the

institutions of the intelligence community and the executive in general, making them in fact hegemonic.

A crucial test for the hegemony of cyber-realism were the *Snowden leaks that presented a critical juncture or shock,* where the dominance of cyber-realism and its policies, legitimized with the war on terror, came under public scrutiny (part 5). Former cyber-utopians such as Al Gore heavily criticized government overreach and the full-take principle collecting the whole haystack. Gore called it "outrageous", "completely unacceptable" and "crimes against the Constitution" (Gabbatt, 2013). President Obama, campaigning with claims to cut-back the mass surveillance apparatus of the Bush-administration, came under fire domestically and internationally and was forced to set up a critical review panel. The panel did a balanced job and argued for a more qualitative approach: SIGINT and targeted surveillance to fight terrorism were seen as legitimate tools, but the full-take principle, the lack of suspicion, the evasion of checks and balances through secrecy and the dominance of military and intelligence-actors in this whole surveillance-cyber-security nexus were criticized. They argued for a more civil approach, contesting the ongoing militarization of cyberspace. Although Obama adopted some smaller changes and acknowledged the potential dangers of a militarized cyberspace, *the dominance of cyber-realism remained unbroken.*

Table 8. Causal Mechanism of the Hybrid Presidency

Context	Economic recession & mobile Internet revolution with high Internet penetration in the US and worldwide.
Part 1	Obama *supported* cyber-utopian and criticized extreme cyber-realists ideas in the election campaign.
Part 2	In office, structural constraints and pragmatism of the presidency lead to a *continuation*/path-dependency of most cyber-realist policies. Institutionalization of offensive cyber-war capabilities leads to a *professionalization* of personnel and attack capabilities (Stuxnet).
Context	Increase of noteworthy hacking and computer security incidents during the Obama administration around 2010/11.
Part 3	Cyber-realists engage in discursive *framing* (cyberdoom) to increase the salience of cyber-security and cyber-war in public discourse. Cyber-security becomes top-priority. Extension of offensive cyber-war capabilities and influences the creation of a new cyber-security strategy. Cyber-security becomes a mature policy subsystem.

Part 4	Stuxnet and the diffusion of technical artifacts such as Xkeyscore accelerate a global norm-diffusion of cyber-realism, picked up by local norm-entrepreneurs in other states.
Part 5	Snowden leaks question the legitimacy of offensive cyber-realism, but path-dependency prevents bigger changes.
Outcome	Stabilization of Internet control practices and dominance of norm of Internet control inside the US but also more and more globally.

5. Conclusion

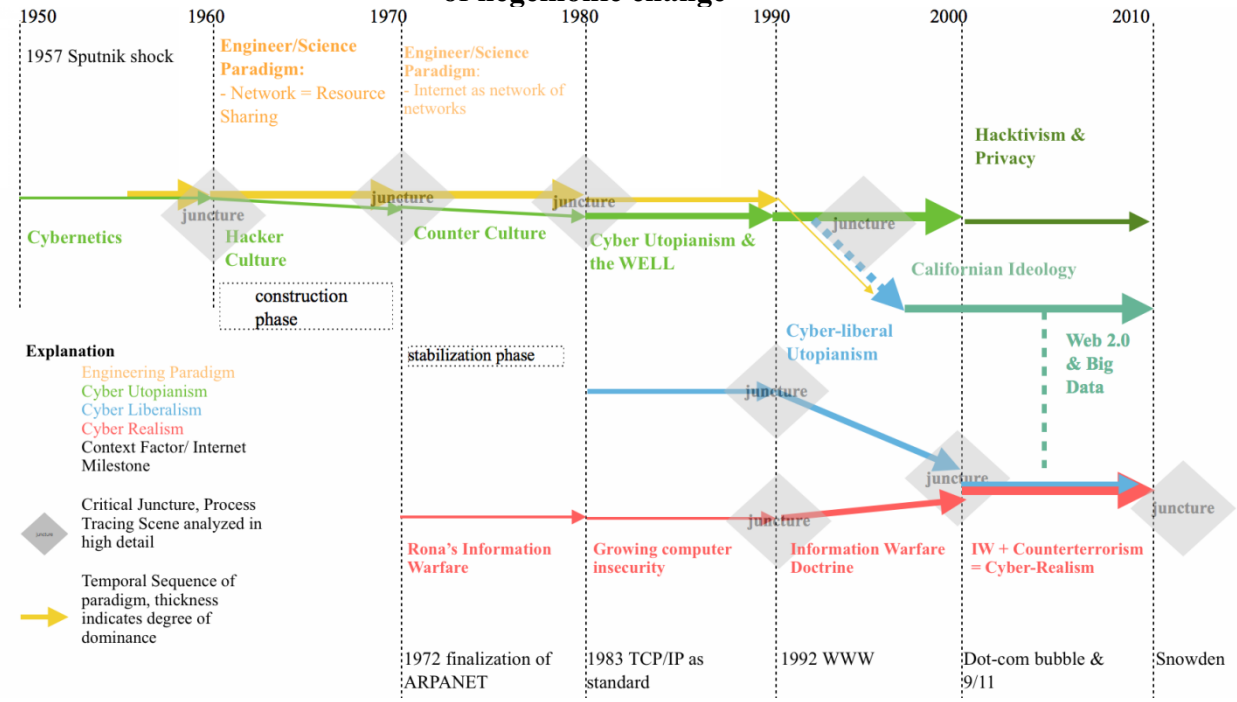
"We're losing a lot of people because of the Internet […]. We have to go see Bill Gates and a lot of different people that really understand what's happening. We have to talk to them about, maybe in certain areas, closing that Internet up in some way. Somebody will say, 'Oh freedom of speech, freedom of speech.' These are foolish people. We have a lot of foolish people."

President Donald J. Trump (2016)

Let me now answer the research question by shortly summarizing the process that led to the establishment of the norm of Internet control. This chapter summarizes the empirical findings while the next chapter focuses on theoretical explanations for the norm of Internet control.

The following graphic presents the timeline of crucial events this thesis discussed. It shows the development paths of each paradigm and the relative dominance of each, indicated by the thickness of the arrows.

Figure 30. Dominant Paradigms shaping the Internet technology & critical junctures of hegemonic change

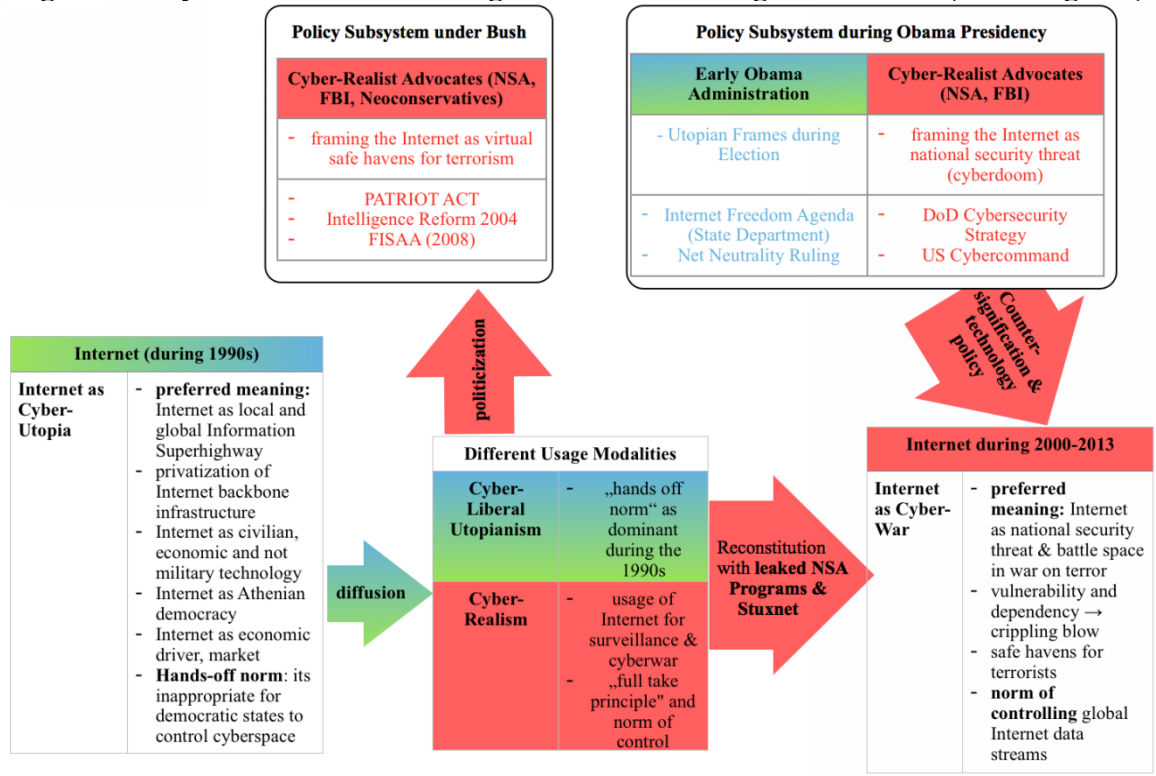


The graphic combines key technological milestones of the Internet with important junctures of each paradigm. It shows the early dominance of the engineering perspective (orange) towards the Internet, which of course was only valid with the early developer and ARPA community until it became gradually replaced by a more utopian perspective. Of course, utopians even existed among the ARPA developers like J.C.R. Licklider. The junctures on this arrow indicate the different development steps of the ARPANET/Internet.

Utopianism (green) became the dominant perspective among early Internet users in the 1980s, while politics at the same time began to recognize computer security incidents. During the 1990s, the three paradigms existed in parallel. Utopianism got politicized by the Clinton/Gore administration while the information war doctrine (red) began to form within military and intelligence circles. During the mid 1990s, utopianism created a spin-off, a more liberal version described as the Californian ideology that is still present today in Big Data and Web 2.0 business models. However, this thesis could not analyze this vast field. 9/11 was the critical juncture that led to the creation of a cyber-realist paradigm out of the IW doctrine, combined with counter-terrorist policies. This led to a decline of utopianism.

Of course, a timeline is just descriptive and not analytical. The sum of the individual causal mechanisms presented for the individual chapters combined looks like the following graphic that is based on the theoretical model presented thus far.

Figure 31. Cyber-Realism becoming dominant meaning for Internet (own diagram)



The Internet during the early 1990s was predominantly understood in liberal utopian terms (green/blue on the left) as it diffused globally. The thesis has shown that the "hands-off norm" diffused together with the Internet and was actively promoted by policy-entrepreneurs. One effect of this norm was the privatization of the Internet infrastructure and the strong anti-censorship consensus that was reinforced by the Supreme Court. The

Internet was thus understood as a global commons and as a facilitator of global democracy. For many it represented a cyber-utopia.

The diffusion of the Internet had a particular effect on impact constituencies concerned with national security (red, middle). For them, the promised anonymity of the Internet and the attribution problem introduced by TCP/IP was a major problem. In theoretical terms, these early cyber-realists engaged in deviant usage modalities, utilizing the Internet for the conduct of war, a usage neither intended by the original designers nor by utopians. Repurposing the Internet first for Information, later for cyber-war resulted in new problem-solving practices and ideas which formed a coherent paradigm with its focus on controlling or exerting control over this new technology that was perceived as chaotic and fundamentally insecure. This assessment was not necessarily wrong, since the Internet was not designed to be secure or to guarantee authenticity of data.

During the course of the 1990s, cyber-realism became institutionalized in the military and intelligence bureaucracy of the US, which is a primary reason for why it could become dominant. Over time, it gained institutional support of the biggest political bureaucracy in the world. Cyber-realist advocates also began to lobby for policies like the Clipper chip or CALEA, but could not break the dominance of cyber-utopianism during the 1990s. Only with the cumulative disenchantment of cyber-utopianism with the Y2K-panic, the dot-com crash and the war on terror, could realism replace utopianism. This paradigm change is very much in line with the theory: the old paradigm witnessed an anomaly it could not explain (the dot-com crash dismantled the rosy future predictions and Y2K showed that technology is not just positive) while at the same time an alternative paradigm was ready that could explain these events better. The Y2K event and 9/11 fit nicely to the expectations of realism and the paradigm advocates were highly capable of framing these events in their terms ("cyber-safehavens" for terrorists for example). Cyber-realists became the new dominant meaning managers explaining the Internet with the GWOT-framework. However, we also saw change on lower orders of magnitude, for example when new administrations entered office or when new policy goals were formulated (several security directives, Clipper, CALEA, Information Superhighway, Patriot Act, IRPTA). Thus, paradigm change is not just a sudden change from one paradigm to another in a short amount of time, but also unfolds slowly.

But there is another factor that is crucial: cyber-realism got politicized (red arrow to the top) because it was supported by key political advocates within in the Bush administration. This confirms the insight of the advocacy coalition framework that access to power is crucial. The role of the Vice President as a norm-entrepreneur is also an

interesting finding of this thesis. Cheney argued that in times of constant war it is appropriate to mass monitor the Internet.

The context of the war on terror is a crucial explanation for the dominance of cyber-realism because it created a new enemy that was both a domestic and a global, networked threat. The focus on terror prevention by accumulating more data was highly compatible with the idea of information superiority or dominance that was developed by military actors during the 1990s. Thus, we saw the merger of two idea sets into one paradigm.

More so, the post 9/11 and realism-inspired national security reforms upgraded the standing of intelligence agencies and the military became the primary means of combatting terrorism, which at the same time gave rise to the idea that the military should be the dominant actor in digital battle-spaces as well. This made these actors more important, giving them more resources and thus political influence, which in turn they used for increased advocacy. New policies like the Patriot Act were adopted, which gave NSA and others new surveillance and cyber-attack capabilities. In other words, the norms of cyber-realism became embedded in Internet surveillance artifacts such as Stellarwind. Surveillance and cyber-war technologies were designed as counter-artifacts, trying to reconstitute the original Internet (red arrow to the right) by trying to disable anonymity online and reintroducing intelligence and control in a network that was designed to have none.

These artifacts and policies were maintained by Obama, although a different pathway could have been chosen. Instead, Obama increased the sophistication of cyber-attacks (Stuxnet), accelerated the professionalization (USCYBERCOM) and developed new doctrines. Artifacts like Stuxnet and Duqu also showed that surveillance and cyber-war are logically connected, forming a nexus. We saw that cyber-doom discourses under President Obama framed the Internet in predominantly negative terms, thus altering the meaning and perception of this technology for a wider audience. This public and political advocacy of cyber-realist actors is one key explanation for why President Obama chose to maintain the Internet-surveillance infrastructure he opposed during the election. But there are of course others. First, cyber-security incidents became highly salient under Obama, both in quality and quantity, which gave cyber-realist arguments greater urgency and credibility. Second, because of the technical complexity and the secrecy of computer network operations and mass surveillance, it is hard to assess the overall costs and benefits of such systems. Advocates of course claim that these tools are appropriate and effective. At the same time, independent oversight and evaluation is lacking. This structural composition of the policy-

field puts cyber-realist arguments in a stronger position, thus increasing the staying power of the status quo, as theory predicted.

There is another factor that only becomes visible over time. Internet surveillance technology and cyber-war capabilities become normalized and institutionalized over time (USCYBERCOM), which further increased their staying power. In contrast, cyber-utopianism never was fully institutionalized and thus more fragile. Cyber-realism on the other hand became deeply embedded within the national security structure of the US and thus is likely to stay. Another reason why the cyber-realist agenda is likely going to stay are external adversaries like Russia and China.

However, there is a particular irony here. Cyber-realism created a self-fulfilling prophecy or a classical security dilemma: based on the fear that other states might disrupt the high-tech US Information society over the Internet, the US rushed into the development of offensive computer network attack capabilities, which in turn inspired other countries to develop the same capabilities, which ultimately produced the very insecurity one was afraid of in the first place. Thus, the more states engage in disruptive or destructive Internet control activities, the less secure the global Internet infrastructure gets. This is where IR constructivism and realism meet. The diffusion of the Internet control norm together with Internet surveillance artifacts that enable this norm led other states to emulate such practices. The more states repeat this behavior, the more the norm of Internet control gets normalized, and the more insecure the global digital infrastructure gets. This creates a cyber-security dilemma. It can be argued that the norm of Internet control currently diffuses globally, with many countries adopting cyber-realist ideas and norms in their national security strategies. It is unclear however, if a tipping point of some sort is reached. To determine this would be the job of future research. The next chapter will summarize the findings that are relevant for the theories.

5.1 Theoretical Findings

The purpose of this chapter is to summarize and hypothesize the theoretical findings that might be useful for further studies and to show how this thesis contributes to the research landscape. I indicate the hypotheses that might be useful for further investigation in *italics.* I will shortly summarize my initial critique and ambitions of this thesis and then introduce the gathered insights.

The thesis contributes to research because it provides one of the first longitudinal studies of the militarization of cyberspace thesis, outlined in the beginning (see chap. 1.2 Literature Review). It does so by focusing not only on one history, for example of the

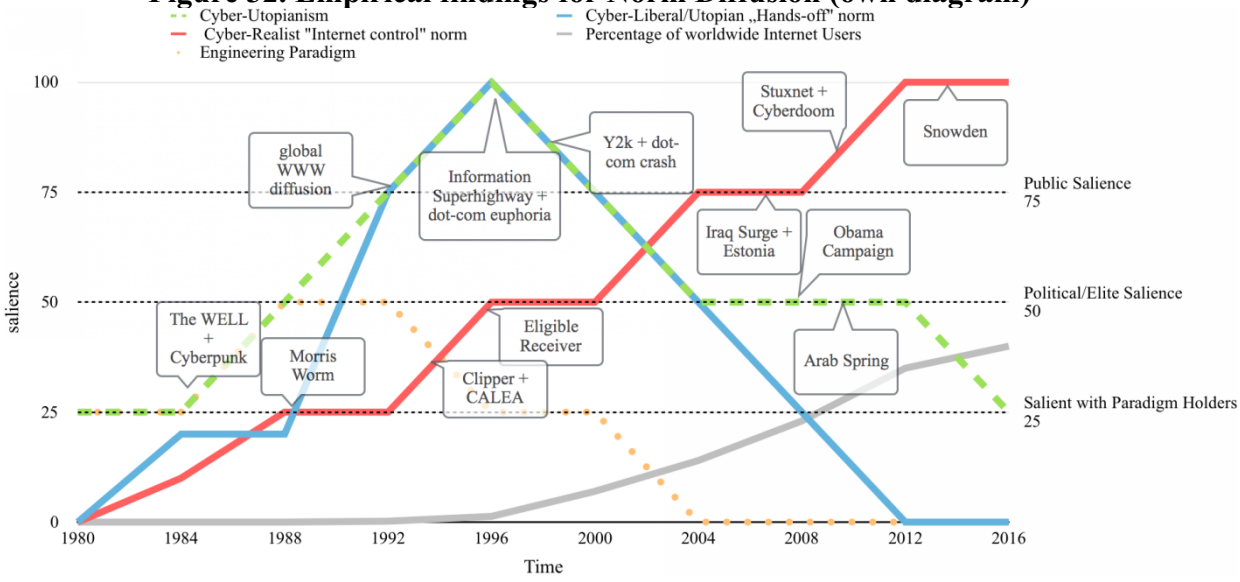
technical development of the Internet, but adopts multiple perspectives, from designers, users, policy-makers and military and intelligence actors. It shows how their perspectives partly overlap, but more so how these actors perceive the same technology in vastly different ways. More so, this thesis shows that each of these perspective have concrete discursive effects, such as the change of meaning of the Internet, the inspiration of new policy, but also material impacts on technology. I showed how paradigm ideas influenced both the design and technical reconstitution of key artifacts such as the Internet or counter-artifacts, such as surveillance technology. Thus, this thesis expands on discursive or narrative approaches in studying the securitization of the Internet. It offers an alternative framework to study technology from the perspective of norm research. Let me now summarize the key findings that might be relevant for future norm-research studies. There is no particular order to these findings.

First, the thesis has shown that it makes sense to expand the view on norm-networks, including supportive ideas, goals and problem definitions. The paradigmatic perspective was useful for explaining the early emergence of norms within paradigms. I showed that *norms developed out of problem-solving activities of key actors that, over time, became normalized*. These processes take decades until initial ideas form coherent paradigms and norms. Utopian norms had their origins in the centralized practice of using computers, which led to the normative demand that technology or information should be free and unregulated. Realist norms had their origin in solving the problem of perceived computer insecurity and SIGINT, which then became expanded with political goals such as information superiority and the politics of terrorist prevention. These accelerated the norm-diffusion and gave Internet control norms a new direction. Had I conceptualized norms as static things with an essential content, I might have overlooked this gradual shift (see chap. 2.1.3 Critique of Diffusion Models).

Second, the interplay of utopianism and realism also shows that it is useful to perceive norms in plural. *The rise and diffusion of norms often coincides with the decline of others* and this becomes only apparent if one broadens the scope. The following graphic depicts the norm change with key events described in this thesis. Observe that there is no concrete measurement of salience, but that this represents a heuristic based on the empirical insights. I argue that *norms first require salience within an advocacy group (counter-culture, hackers or military actors) and if they get politicized, they gain salience among policymakers as well*. It must be stated that the order of causation is not entirely clear, because politicians often react to public demands and so it could be argued that public salience comes before political salience. This was certainly the case with cyber-

utopianism, but cyber-realism showed that it first was dominant among national security actors within the political administration. In both instances, the politicization of paradigms and norms is key.

Figure 32. Empirical findings for Norm Diffusion (own diagram)



I have added the percentage of worldwide Internet users (grey) to show an interesting effect: Cyber-utopianism was dominant during the 1990s, but mostly among early adopters which, technically, were a minority. However, since these early adopters acted as explainers and sense-makers for the rest of the population, their normative impact was higher. Thus, we can hypothesize that *early-mover advantages seem to matter with the diffusion of norms*. Claiming the early meaning-space and establishing the first narrative is also one of the key arguments of narrative research. Cyber-realism on the other hand became dominant at a time when more Internet users were exposed to its ideas, which means that it reached potentially more people. What is true in both cases is that *norms and paradigms must be compatible to other ideas of a time-period* (which I sometimes called the "zeitgeist"). Utopianism resonated well with the end of the Cold War while cyber-realism resonated well with the war on terror narrative. If there is an overlap between a paradigm's idea, or semantic network and the dominant ideas in society, this potentially increases the follower base of a paradigm. Thus, *the more norms resonate with idea sets or discursive formations of a time, the higher the chances for diffusion*. A fruitful question for future research would be how resonance can be theorized and how it works. What can be *hypothesized is that commensurability and narrative fidelity is important*, which is in line with framing theory. Both cyber-utopianism and realism invented interesting narrative devices and concepts such as "cyberspace", "electronic frontier", "cyber-9/11", "cyber-

war" or metaphors such as the "death of distance" or "the Information Superhighway". This includes expectations of the future or prognostic frames, one utopian and one dystopian. Cyber-realism also engaged in frame-bridging, connecting its ideas with utopian concepts. The idea of a cyber-*space* as a realm is one of those bridges. The lack of control, that was seen as positive by utopians was reframed by cyber-realists as uncontrollable chaos or anarchy, which gives it a more negative connotation. This means that *paradigms can lose control over their frames* if they reach a wider audience.

The previous graphic also shows something else, which I have barely touched upon. *Paradigms do not vanish after they lose their dominance*. They still are part of the political idea space or primeval policy soup (see chap. 2.2.4 Explaining Change). Cyber-utopian ideas (green) did not die out after 9/11. In contrast, a sense-making period kicked in and most utopian advocates turned to privacy issues.[178] Utopian ideas began to resurface during the Obama administration and the Snowden leaks but could not gain dominance again. On the other hand, the whole idea-norm-network of the Information Superhighway (blue) lost most of its salience. The metaphor still exists, but it is not as widespread anymore. The same is true for the original engineering perspective (orange). This is evidence for theories of norm-regression which argue that norms can die out and that norm-diffusion is no deterministic or teleological process. Drawing on the paradigm perspective, the thesis offers a useful mechanism that can explain the regression of norms: *if an anomaly produces an unexplainable crisis for a paradigm that negates its predictions and expectations, while at the same time a viable alternative exists, then norm and paradigm change is likely.* This is a variation of Legro's argument (Legro, 2000). It could also serve as a scope condition necessary for paradigm change.

Third, the interplay of multiple norms is interesting if we add the notion of dark norms that contest traditional liberal-democratic norms. Cyber-realism promotes several dark norms, like suspicion-less mass surveillance of Internet data or the intrusion into other nation's networks regardless of their sovereignty rights. This implies that the contestation of liberal norms is successful and that this could be part of the explanation why cyber-realist norms became dominant. Especially realist advocates are evidence for the argument that norm-diffusion is not about morality and deontological norms (the analysis did not uncover any morality argument legitimizing the norm of Internet control), but might be driven by power interests of particular groups. This was confirmed by some sources who called Internet-surveillance and cyber-capabilities as a "power-grab" or described it as a "means of power". This *affirms the notion that dark norms include a power-component.*

[178] What happened to utopianism in the mid 2000s would be an interesting future-research project.

Power includes the marginalization of alternatives. In my case, the dominance of cyber-realism positions military and intelligence actors as the dominant instrument of states in dealing with the Internet, while marginalizing civil- or non-military approaches to cyber-security. Cyber-utopians argued for a decentralized governance structure of the Internet which became marginalized or overwritten by the realist state-centric approach. The power dimension is also visible with the information in-balance in the cyber-security field, produced by classification and the clandestine nature of cyber-operations that prevents external oversight and evaluation. Even intelligence actors such as Michael Hayden argue that the secrecy partly goes too far and even obstructs efficient cyber-security (Hayden, 2016b, p. chap. 8). This knowledge gap, or a dominated discourse as philosopher Jürgen Habermas would call it, is problematic. There is a huge knowledge-divide because of classification. Observers and parliamentary control have a structural disadvantage here because the advocates of cyber-realism maintain the relevant knowledge to critically evaluate their demands. Whether post 9/11 Internet surveillance indeed is effective, or even meets the goal of preventing terrorism, was never evaluated. Whereas efficiency and rationality criteria are guiding almost all policy subfields, they are absent in national security issues. There is no evaluation of whether the trillion dollar programs are indeed effective which implies that the GWOT and Internet control are taken for granted. However, I could only touch upon this issue and future research should untangle this power dynamic.

Fourth, the paradigm perspective was useful for studying norm emergence and politicization on the domestic level. I have shown that a *huge variety of actors advocate norms*, from military or national security actors such as the director of NSA or National Intelligence, Vice Presidents such as Cheney or Gore and even Internet users. We should not underestimate the norm-advocacy of intelligence actors worldwide. A hypothesis could be that the *similar interest formation of intelligence actors explains the dominance of cyber-realism in both democratic and authoritarian states.* However, I could not systematically test this because I focused on the US alone. This would be interesting to test in future research.

I could confirm the assumption *that the closer a norm-advocate is to the political power structure, the higher the chances for diffusion among political circles are.* This was the case with Gore and Cheney. The advocacy coalition perspective also confirmed another insight from norm-research, namely that institutionalization matters. If a paradigm and its *norm get embedded in powerful institutions such as the military or intelligence agencies, its staying power increases,* especially if these actors become upgraded and more

important over time. Cyber-utopianism lacked this institutionalization, which guaranteed the socialization and education of new paradigm followers and advocates. The paradigm perspective showed how important education, textbooks and paradigm socialization were. Cyber-realist military career tracks and textbooks exemplify this.

This also creates *persistency of arguments and ideas*, which is another explanation why cyber-realism could become dominant. One peculiar element of cyber-realism is the persistency and continuity of certain ideas and frames. Winn Schwartau's frame of the "digital Pearl Harbor" was first uttered in 1991 and still appears in current discourses, although no such event ever happened (Schwartau, 1997). Initiatives like Clipper, CALEA, the Patriot Act and FISAAA show similar elements: they all aimed at giving the IC more capabilities while downscaling legal restrictions. This might have to do with the structural composition of the national security policy field: the same actors rotate to different functions (former NSA heads become DNI, or heads of CIA/FBI), which allows them to present the same arguments over a longer period of time. The history of cyber-war and surveillance is a history of a few reappearing names (Alexander, Cheney, Hayden, McConnell). Additionally, from an IC perspective, their proposed policies are stable: less oversight, more competencies, more information gathering, less encryption. This makes it somewhat possible to predict future policies demands from these actors. In contrast, policymakers change every four or eight years, but they often are dependent on insights from the IC, which reduces their ability to critically evaluate their demands. Technical complexity and IT-literacy further complicate this matter. We see that technologically educated politicians show higher interest in IT-matters and thus are theoretically better suited for critical evaluation. Thus, the advocacy for ideas stays stable whereas the targets of this advocacy change with each election. Thus, *continuity and consistency of advocacy increases changes for dominance*. Cyber-utopianism lacked both continuity and consistent advocacy.

Another related insight from policy-research is that *the structure of the policy-field matters*. Cyber-utopians could advocate their norms because the 1990s technology policy-field was large enough to make regulation necessary, while at the same time it was not pre-structured. Cyber-realism became dominant within the national security field which is highly secretive and closed to outsiders. Closed or mature *policy-systems imply that norm change is harder because outside voices are less heard*. That utopianism played no role in the Bush administration might have to do with the fact that there were no utopian advocates present within this administration. Instead, there might have been cyber-realist

group-think (Badie, 2010). The psychological dynamics within paradigms would be also interesting for future research.

The fifth insight is that *institutionalization does not just mean institutions and organizations, but also technology*. Norm and technology diffusion are clearly intertwined processes. The combination of social construction of technology and norm-research is useful. The two theoretical camps are compatible and offer complementary explanations. Most notable are the aforementioned early-mover advantage in framing a technology and path-dependency of technology. The technology perspective also removes the strong actor-centrism of original norm-research. Neither cyber-utopianism nor realism would exist without the Internet. At the same time, these paradigms shape our perception of the technology (because of their framing) and also influence our usage modalities. The norm of control developed out of a particular perspective on the Internet which was also shaped by the technical modalities of the Internet, namely the security blind spots. The causation goes in both ways: *paradigms influence usage of a technology* while *the technical affordances influence usage and thus the formation of paradigms*. The analysis has shown that both realism and utopianism competed with each other regarding the technical affordance of decentralization or the end-to-end principle. This design choice had a different impact for both paradigms. What kind of impact it has depends on the distinct usage modalities. Utopians saw the end-to-end principle as positive because it supported their goal of flat hierarchies. Realists saw it as problematic because it complicated SIGINT.

Thus, *how actors use a technology influences their normative preferences.* Cyber-realists engaged in the deviant usage of the Internet for war, while utopians used it for idea-exchange and community-building. Both groups adopted a somewhat technological determinist perspective and argued that there is an essence inherent to the Internet. Both paradigms also assumed that their individual usage modality of the technology would implicate the very same global usage modality. Utopians thought everyone would use the Internet for empowerment, academics thought everyone would use the Interent for knowledge diffusion while miltiary actors naturally thought that everyone would use the Internet for war. This had the character of a self-fullfilling prophecy (dot-com crash & cyber-security dilemma), which will I discuss further in a bit.

Additionally, technical knowledge matters. It seems reasonable that *tech-savvy users see a technology less as a threat and potentially more in positive terms*, while technology illiterate decision-makers are more likely to adapt a negative perspective. This should be tested in future research.

I also showed that norm-research should consider technical affordances of artifacts, especially in cases where norms are directed at artifacts (like the prohibition of land-mines, drones, nuclear or chemical weapons). Thus, political technologies like weapon systems, cyber-attack capabilities or surveillance-infrastructure should be further analyzed by norm-research since these technologies clearly include a political dimension. These devices are not neutral or instrumental technologies but serve and reinforce political agendas and distinct ideas. The framework I have provided in this thesis thus might apply to other technologies and their normative components.

Once a *technology is developed or bought, it is unlikely to go away and thus will increase the staying power of norms and ideas* that are related to it. Mass surveillance continues because the technical infrastructure is in place and became normalized over time. More so, *powerful technical artifacts such as Internet surveillance systems create a demand-pull in other countries*, which too want to buy or develop these capacities. The Snowden leaks facilitated this trend. Thus, *with the diffusion of these artifacts, the norms embedded in these systems (like "mass surveillance is appropriate") are likely to diffuse as well*. This creates a powerful argument and precedent, especially in authoritarian regimes: "if the liberal US are doing this, so can we". I only have hinted at the fact that other countries are actively emulating (Florini, 1996) the mass surveillance capacities by the US, thereby spreading the norm of Internet control globally. Future research should confirm this. The same mechanism also worked with utopianism and the early Internet, since many Western democracies also replicated the "hands-off" norm and the privatized US Internet governance model.

5.2 Methodological Issues and Alternative Explanations

This chapter discusses some methodological issues that appeared in this study. The purpose is critical reflection.

This thesis did not study the global diffusion of Internet norms, as originally intended. I only gave limited evidence for the global reach of the "hands-off" norm promoted by Gore and how it resonated with other democratic states. More so, I only hinted at the global norm diffusion of Internet control practices with intelligence agencies. I strongly invite future research to address this gap and to provide comparable data on the dominance of paradigms in other countries. An interesting question would be the degree of overlap between control practices of democracies and authoritarian regimes by creating some sort of index.

Another shortcoming is that I did not provide any mathematical measurement on the dominance of the Internet control norm. Analytically it is hard to determine whether norm A is stronger or more dominant than norm B. I have assessed the dominance of norms heuristically by observing the frequency of cyber-realist ideas appearing in public and political discourses and by pointing to some opinion polls. Discourse theory and STS argue that closure can be witnessed when the meaning-fluctuation stops. However, this is hard, if not impossible to study in the empirical reality. Maybe an even longer timeframe is needed for that. It is possible that utopian frames and ideas will be forgotten in 20 years or so. Alternatively, one could have analyzed the current cyber-war discourse in higher detail, as I originally intended. However, due to space and time constraints this step was skipped. I am optimistic that future studies will fill this gap.

Methodologically, some issues with process tracing have to be discussed. The first issue concerns the correct identification of junctures. Internet governance scholars might argue that crucial pathways of the Internet were enabled elsewhere, for example during the 1990s at international consortiums. Economists or copyright researchers might point to crucial legislation such as the Digital Millennium Copyright Act of 1996 that represents an economic vector of Internet content control in terms of copyright. Cyber-security scholars might point to crucial developments on the international level, such as the EU Budapest Convention on Cyber-crime (2004) or the Tallinn Process to codify the laws of war for cyber-space (Schmitt, 2013). This critique probably is well founded. Since I excluded the economic and international perspective from this research, I invite other scholars to theorize the causal impact of this path-trajectory on Internet control, which probably will represent an additive causal effect.

In the same vein, there could be a hidden, alternative pathway that enabled cyber-realism to become dominant. Although I carefully screened the existing literature and did not find evidence for this, the possibility cannot be excluded. One possible alternative explanation could lie in utilizing a different set of theories to explain the events in the causal mechanism. A critical reader might have observed that my thesis includes a constructivist reading of IR-realism. Instead of using norm-research as a starting point, IR-realist theories might provide useful additional arguments to explain the dominance of cyber-realism. I already have hinted at the power-maximizing tendencies of both states and their intelligence agencies, creating a classical security dilemma globally: States desiring to increase their security develop offensive hacking tools that diminish the security of others. The early Internet of the digital natives was an instance of an anarchic global system. With the emergence of the state in cyber-space we began to see classical realist

phenomena like power-struggles and arms races. What we currently witness is the struggle to create a new global order in this chaotic system and actors like Russia, the US or China struggle to reach global dominance in cyberspace. The question is whether we will see some kind of Westphalian order in cyberspace.

Alternatively, a rational choice or cost/benefit perspective might be useful to explain the dominance of cyber-realism, especially with regard to the staying power of the status quo (Bennett & Checkel, 2014, p. 31). I have indicated in the Obama chapter that once an intelligence reform is in place, money and resources have been spent and stakeholders occupy new positions, which means there is little structural incentive for change (Hayes, 2012). A strong intelligence apparatus is beneficial for presidential decision-making, which is why extensions of intelligence capacities are seldom cut-back. Thus, from a rational choice perspective it is rational to maintain a surveillance infrastructure that had cost billions of dollars instead of dismantling it.

Studies on political bureaucracies or organizational studies also might be helpful here, especially if it comes to the turf-battle dynamics between intelligence organizations. Critics might point to the fact that the Intelligence Community is not as homogenous and like-minded as I assume in this thesis. History is full of examples where NSA withheld information from CIA or where the IC mistrusted military intelligence agencies and organizations. All of these branches of government adhere to different organizational cultures (Barnett & Finnemore, 2009), to different norms and maybe even paradigms. For example, I described a general euphoria of military thinkers regarding the revolution in military affairs (see chap. 4.4.2.1 Optimistic Cyber-Realism: Revolution in Military Affairs (1992-2000)), whereas intelligence actors from NSA were relatively sceptical early on (see chap. 4.4.8 The Norm of Internet Control). This diverging perspective within cyber-realism could either represent a learning-curve or indicate different organizational cultures.[179] A follow-up study should investigate the norms and ideas of these agencies, maybe with in-depth interviews and oral histories to check whether how much they correspond with cyber-realism as I have outlined. We are also lacking sources that document the early cooperation and idea exchange between military and intelligence actors during the information warfare period. The same is true for the private-public partnerships in this sector.

Economic theories of actor interests might be helpful. Others have observed that the intelligence apparatus in the US is in large parts driven by private industry (Shorrock, 2009), creating a dynamic sometimes called "surveillance-industrial-complex" (Harris,

[179] Learning theories might also be worthwhile in studying the ideas of political elites regarding the Internet.

2014). Understanding surveillance and cyber-war from a market perspective with different stakeholders trying to maintain their business models further helps to understand the staying power of cyber-realism. There is so much money involved that the stakeholders must have a strong material interest in maintaining external threats to which they sell solutions. Thus, a future study could adopt a congruence testing approach, checking whether rationalist or constructivist theories might be better in explaining the dominance of cyber-realism (Blatter & Haverland, 2012).

Similar evidence comes from intelligence studies. Secrecy and classification practices create an interesting dynamic that should be analyzed more deeply. Knightley indicates that there is a mysterious historical trend that intelligence agencies are always up-scaled. They are given more personnel, money and capacities over time and that the reverse movement (like the Watergate scandal) only rarely occurs. Most intelligence agencies like MI5, KGB, CIA or NSA were intended as small bureaucracies with quite narrow functions that over time significantly expanded or even became dominant players in the political system, as with the KGB in the Soviet Union (Knightley, 2003, p. chap. 14). In other words, once broad surveillance capacities, technologies and organizational structures are in place, they exercise a strong staying power producing strong rational incentives but also normalizing tendencies to keep them intact.

Another open question is whether there exists a historical tendency of state control over communication technologies. I have hinted at the fact that other technologies, such as the telegraph, radio, the cable TV and others initially also have been perceived in utopian terms (see chap. 4.2.2 Ideas: Stewart Brand and the Counter-culture (1960-1970)). The question is whether the norm change from utopia to realism is a general historical pattern with technology. Is there a historic trend towards state control of technology? Comparative case studies, comparing the Internet with the telegraph or the cable-TV would be interesting.

Let me now offer a word on generalization. Of course, the general mechanism of this thesis cannot be generalized. However, the theoretical elements identified in the previous chapters can. The very same framework of norms and technology could be used for studying other artifacts like drones (UAV), border-surveillance systems or other kinds of weaponry. More so, I would speculate that we can see a similar norm-change from utopianism to realism in other Western democracies, like the United Kingdom. Cyber-realism probably will have a similar shape, whereas cyber-utopianism probably will look different, absent of the counter-cultural and libertarian elements present in the US.

5.3 Discussion and Outlook

It is worth repeating what Al Gore, Barack Obama, Tim Berners-Lee, Vint Cerf and others have said about the Internet over the course of this thesis. The core reason it exists is its openness. The lack of control emerging from the free-wheeling ARPA spirit and the openness of the design process and the protocol design are central for the success of the Internet. The idea not to restrict anything on the net, to create total freedom so to speak is central. This was only possible because the Internet developed in a context that explicitly endorsed and supported this lack of control. The decentralized nature and its creative chaos were once seen as positive, inherently liberal-democratic features of the Internet which should be protected from state-encroachment and totalitarian tendencies of imposing control. Cyber-utopians were right in the sense that the Internet is an empowering tool that allows everyone, even marginalized citizens to be heard and to participate in a global conversation. What utopianism not expected was what kind of voices it would also empower: fascists, trolls, propagandists, populists, terrorists and other criminals that are also part of liberal societies. In that sense, the idea that the Internet reflects *all,* even the undesirable, aspects of a liberal society is not that far-fetched. But the Science and Technology Studies perspective has shown that features like "empowerment", "freedom of speech" or the Internet's "openness" are not its essence: these features exists because the technology is embedded in a society that cherishes these features. In other words, the Internet is not inherently democratic but it is democratic for us because we used to perceive and frame it in these terms. The Internet allows global, uncensored communication because democratic states explicitly endorsed this. The idea of a democratic global cyberspace is a socially constructed, but fragile reality of the Internet that currently is under siege (Deibert, 2015). If democratic states no longer uphold these values and authoritarian or nationalistic states begin to shape the global Internet and advocate for more control and surveillance, it might lead to a technical and social reconstruction, or reconstitution of the Internet.

The militarization of cyberspace is such a reconstitution that might produce undesirable consequences. The analysis has shown that the US is a country "whose stated goal is to dominate cyberspace as a battlefield and that has the means to do it" (Harris, 2014, p. Prologue). Currently, the dominant approach of US vis-à-vis cyberspace is through military and intelligence means, guided by a national security doctrine. The US has created a widespread set of instruments, ranging from state-hacking with NSAs special units, computer espionage on a large scale as well as collecting every piece of information traversing global cyberspace and utilize it as a means of offensive cyber-war and

surveillance. The analysis has shown that surveillance, espionage and cyber-war cannot be separated: they are part of the same mind-set, forming a nexus. Thus, if cyber-realist advocates demand more cyber-war capabilities, this often also includes new surveillance capabilities. The discourses on cyber-war and surveillance should not be separated, but conceived as one.

The global war on terror was the metaphorical "fall of man", not just in terms of human rights becoming contested by extraordinary rendition or water-boarding practices, but also in terms of the digital domain. The war on terror also brought war and an exceptionalist logic to cyberspace. This exceptionalist logic both contests core norms of liberal democracies and the openness of the Internet itself. 9/11 established cyber-realist norms and ideas in the shared consciousness: first the unquestioned *belief that it is possible, given enough intelligence, to prevent surprise attacks by terrorists* and second that the *battle-space expands globally, domestically*, and *digitally* because terrorists hide against the backdrop of society. Third, this diagnosis *normalizes the use of extraordinary foreign military and surveillance technology to be used against US* and other nations' citizens. It represents a militarization of cyberspace that was *legitimized as a temporary state of emergency after 9/11.*

The civil law-enforcement paradigm of managing issues in cyberspace and the liberal interpretation of the Internet was abandoned and replaced with a war logic: The Internet no longer is a global-village but a battle-space and a target. Legal regimes of liberal democratic states restrict invasive surveillance by demanding a targeted approach based on suspicion became dismantled with the war on terror. Whereas surveillance in the past worked in a deductive fashion – from initial suspicion to target surveillance to test the suspicion – the new norm has a reversed logic. It operates without suspicion and collects data inductively, to generate a suspicion once after the data is collected. This is highly problematic and can undermine citizens' trust in their governments, as the writers of the NSA report indicated (Clarke et al., 2014). It is also problematic because it contests the core notion of democracies. Collecting vast data-streams or *"full-take"*, which became the default or the norm even for democratic states, includes totalitarian ideas. In the introduction, I referred shortly to surveillance practices of the former Stasi. The Stasi, too, aimed for a "full-take" approach in terms of intercepting and opening letters sent from the GDR to the West, or in terms of the "full-take" interception of all phone-calls within the GDR (Foschepoth, 2013). But the Stasi never had the technological infrastructure to reach this goal. Nowadays, democratic states have built this very infrastructure.

But Western states also have externalized this logic. Since the war on terror is global, this practice is repeated on a global scale. Offensive cyber-war blurs the line between intelligence operations, surveillance and military conduct (Harris, 2014, p. chap. 4). *Offensive computer network attacks expand control towards foreign objects and servers*: information should not just be controlled domestically, but also inside other countries. Historically, this is an utterly new development. Cyber-war serves as the logical expansion of the norm of control internationally. It is not just passive surveillance anymore, but active manipulation of data and target systems.

The militarization of cyberspace is problematic, because it contests the notion of the Internet as a civilian or democratic space, run by private companies and inhabited by millions of international citizens. A "neighborhood, a library, a marketplace, school yard, a workshop – and a new, exciting age in human experience, exploration and development" (Harris, 2014, p. chap. 10). The unilateral, state-centric claim to control cyberspace is in opposition to the decentral structure of the Internet as a commons that should be maintained by everybody. With what right can the US claim dominance over the Internet and with what right can it deny non-democratic states such as China and Russia the same claim? Of course, the US is a role model of the future and other states want to mimic the cyber-competencies that were established in the post 9/11 world. Whereas the use of cyber-war competencies for domestic and international spying is at least somewhat regulated in democratic states, it is not in countries like China and Russia. There, sophisticated CNA and CNE tools are turned against their own societies. Russia and China are using the cyber-war arsenal to wage internal information wars to maintain the authority of the elite (Blank, 2013).

In sum, this exceptionalist norm of control became *normalized in the sense that control of cyberspace became a goal that is shared and adapted by more and more states.* In other words: democracies and dictatorships both claim the right to control the Internet and all the information stored and transmitted therein. A provocative thesis thus would be that in cyberspace, there is no longer much difference between authoritarian regimes and democracies. If someone would break into your computer network to steal data you would not know whether its NSA or the Russian FSB. The question is, whether this new authoritarian logic in cyberspace is part of, or even precedes, the current crisis of liberal norms and democracies. If democracies become more authoritarian, represented by right-wing or even neo-fascist regimes, it should not come as a surprise that the online behavior of these states also shows authoritarian or totalitarian tendencies.

If that thesis is true, then we can expect that democracies will adopt new means of Internet control that currently are pioneered by authoritarian regimes: the ban of encryption technology to circumvent state surveillance, more Internet censorship under the disguise of "fake news" or "moral decency", as can be seen in Poland, the treatment of Internet companies as media institutions for which censorship and content control laws apply (as in Russia), the construction of Internet kill-switches (as in Turkey) and, in the worst-case, the physical reengineering of the Internet to enable more surveillance, probably legitimized under the pretense of terrorism (as in China). Cyber-realist advocates and authoritarian leaders alike already formulate demands to reengineer the Internet to allow better surveillance. DNI McConnell argued in 2010 that "we need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment – who did it, from where, why and what was the result – more manageable" (McConnell, 2010) and likewise, current US President Trump argued in the entry quote for this chapter "We have to talk to them [Internet engineers] about, maybe in certain areas, closing that Internet up in some way". The risk of neo-nazi or neo-fascist parties taking over the vast Internet surveillance machinery in many states is highly problematic. Internet surveillance data can be easily used to draft kill or deportation lists of immigrants, homosexuals, Muslims or political opponents. But there is not just a human risk, but also a technical one.

I said in the beginning that the Internet allows a global democratic conversation because it was technologically and socially constructed in that way. If more countries follow an authoritarian logic, the idea of a global, liberal-democratic interconnected network of networks is history and with it the possibility of easy and instant human interaction on a global scale. Instead, we will see what Tim Berners Lee warned about: a balkanized or nationalized splinter-net as developed by China. In this vision, each country will have its own nationalized network. Global access to information would be limited. Global idea exchange would hampered and national governments would position themselves as curators or censors, deciding what information can be accessed or not. Authoritarianism and nationalism contest the logic of a shared, global commons. The only regimes in the world to prevent this from happening are liberal democracies. If they do not advocate their liberal norms of freedom of speech, rule of law, human rights and privacy on the Internet, no one else will.

Bibliography

9/11 Commission. (2004). *The 9/11 Commission Report.* The National Commission on Terrorist Attacks Upon the United States. https://9-11commission.gov/report/.

Abbate, J. (2000). Inventing the Internet. The MIT Press.

Acharya, A. (2004). How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism. *International Organization*, *58*(2), 239-275.

Ackerman, G. A., Bale, J. M., & Moran, K. S. (2006). Assessing the threat to critical infrastructure. In J. J. F. Forest (Ed.), *Homeland Security: Critical infrastructure* (Vol. 3). Greenwood Publishing Group.

Adler, E. (2013). Constructivism in International Relations: Sources, Contributions and Debates. In W. E. Carlsnaes, T. Risse, & B. A. Simmons (Eds.), *Handbook of International Relations* (Second Edition ed.). SAGE Publications Ltd.

Adler, E., & Pouliot, V. (2011). International practices. *International Theory*, *3*(01), 1-36.

Aitel, D. (2013). Cybersecurity Essentials for Electric Operators. *The Electricity Journal*, *26*(1), 52-58.

Akamai. (2015). State of the Internet Report. https://www.akamai.com/us/en/our-thinking/state-of-the-internet-report/index.jsp.

Alberts, G. (Ed.). (2014). Hacking Europe: From Computer Cultures to Demoscenes. Springer London Ltd.

Allen-Ebrahimian, B. (2016). The Man Who Nailed Jello to the Wall. *Foreign Policy* http://foreignpolicy.com/2016/06/29/the-man-who-nailed-jello-to-the-wall-lu-wei-china-internet-czar-learns-how-to-tame-the-web/.

Amnesty International. (2016). *Dangerously Disproportionate. The Ever-Expanding National Security State in Europe.* Amnesty International. https://www.amnesty.de/files/Amnesty-Bericht-EU-Antiterrorgesetze-Januar2017.pdf.

Amoore, L., & de Goede, M. (2008). *Risk and the War on Terror*. Routledge.

Anderson, R., & Murdoch, S. J. (2008). Tools and Technology of Internet Filtering. In R. Deibert, J. Palfrey, R. Rohozinski et al. (Eds.), *Access Denied. The Practice and Policy of Global Internet Filtering*. London: MIT Press.

Aradau, C. (2010). Security That Matters: Critical Infrastructure and Objects of Protection. *Security Dialogue*, *41*(5), 491-514.

Arquilla, J., & Ronfeldt, D. (Eds.). (2001). Networks and Netwars: The Future of Terror, Crime, and Militancy. (1 ed.). Rand Corporation.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is Coming! *Comparative Strategy*, *12*(2), 141-165.

Arthur, C. (2008). Vint Cerf, "father" of Internet says Obama best for net. *The Guardian*. https://www.theguardian.com/technology/blog/2008/oct/15/obama-net-neutrality-cerf-google.

Assange, J., Appelbaum, J., Muller-Maguhn, A. et al. (2013). *Cypherpunks: Freedom and the Future of the Internet*. The Times Group Books.

Auletta, K. (1994). Under the Wire. Will the telecommunications revolution end in monopoly or Big Brotherhood? Neither, if Al Gore gets his way. *The New Yorker*. http://www.kenauletta.com/underthewire.html.

Bacevich, A. J. (2002). American Empire: The Realities and Consequences of U.S. Diplomacy. Harvard University Press.

Bacevich, A. J. (2013). The New American Militarism: How Americans Are Seduced by War (Updated Edition ed.). Oxford University Press.

Badie, D. (2010). Groupthink, Iraq, and the War on Terror: Explaining US Policy Shift toward Iraq: Groupthink, Iraq, and the War on Terror. *Foreign Policy Analysis*, *6*(4), 277-296.

Baldwin, D. A. (2012). Power and International Relations. In W. Carlsnaes, T. Risse, & B. A. Simmons (Eds.), *Handbook of International Relations* (2 ed.). SAGE Publications.

Ball, J. (2013). NSA stores metadata of millions of web users for up to a year, secret files show. *The Guardian*. http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents.

Ball, J., Borger, J., & Greenwald, G. (2013). Revealed: how US and UK spy agencies defeat internet privacy and security. *The Guardian* http://www.ihatefeds.com/Revealed_ How US and UK spy agencies defeat internet privacy and security _ World news _ The Guardian.pdf.

Bamford, J. (2009). The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America. Anchor.

Bamford, J. (2012). The NSA is building the country's biggest spy center (watch what you say). *Wired*. http://hotredchiles.com/NSAcenter.pdf.

Bamford, J. (2015). What @Snowden Told Me About the NSA's Cyberweapons. *Foreign Policy*. http://foreignpolicy.com/2015/09/29/what-snowden-told-me-about-the-nsa-offensive-capabilities/.

Bar-Joseph, U. (2010). The Professional Ethics of Intelligence Analysis. *International Journal of Intelligence and CounterIntelligence*, *24*(1), 22-43.

Baran, P. (1964). On distributed communications. I. Introduction to Distributed Communication Networks. Proceedings from Unites States Air Force Project RAND, Santa Monica.

Baran, P., & Farber, D. (1977). The Convergence of Computing and Telecommunications Systems. *Science*, *Vol.195*, 1166-1170.

Barbrook, R., & Cameron, A. (1996). The Californian Ideology. *Science as Culture* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.460.8355&rep=rep1&type=pdf.

Bari Kolata, G. (1980). Cryptography: A New Clash Between Academic Freedom and National Security. *Science*, *209/4460)*, 995-996.

Barkin, J. S. (1998). The Evolution of the Constitution of Sovereignty and the Emergence of Human Rights Norms. *Millennium - Journal of International Studies*, *27*(2), 229-252.

Barlow, J. P. (1990). Crime & Puzzlement. https://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/crime_and_puzzlement_1.html .

Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. *wac.colostate.edu* http://wac.colostate.edu/rhetnet/barlow/barlow_declaration.html.

Barnard-Wills, D., & Ashenden, D. (2012). Securing Virtual Space: Cyber War, Cyber Terror, and Risk. *Space and Culture*, *15*(2), 110-123.

Barnett, M., & Finnemore, M. (1999). The Politics, Power, and Pathologies of International Organizations. *International Organization*, *53*(4), 669-732.

Barnett, M., & Duvall, R. (2005). Power in International Politics. *International Organization*, *59*(01).

Barnett, M. N., & Finnemore, M. (2009). The Politics, Power and Pathologies of International Organizations. In F. V. Kratochwil & E. D. Mansfield (Eds.), *International Organization And Global Governance: A Reader* (2 ed., pp. 177-193). Longman.

Barzashka, I. (2013). Are Cyber-Weapons Effective? *The RUSI Journal*, *158*(2), 48-56.

Baumgartner, F. R. (2013). Ideas and Policy Change. *Governance*, *26*(2), 239-258.

Beach, D., & Pedersen, R. B. (2012). Process-Tracing Methods: Foundations and Guidelines. The University of Michigan Press.

Beattie, A. Market Crashes: The Dotcom Crash. *Investopedia* http://www.investopedia.com/features/crashes/crashes8.asp.

Beebe, B. (2010). Intellectual property law and the sumptuary code. *Harvard Law Review*, *123*(4).

Bell, D. (2000). The End of Ideology: On the Exhaustion of Political Ideas in the Fifties, with "The Resumption of History in the New Century" (2nd ed.). Harvard University Press.

Bendiek, A. (2016). Sorgfaltsverantwortung im Cyberraum. Leitlinien für eine deutsche Cyber-Außen und Sicherheitspolitik. *SWP-Studie*, *S 3*.

Bendrath, R. (1999). Der Kosovo-Krieg im Cyberspace. userpage.fu-berlin.de/~bendrath/cyberkosovo.rtf.

Bendrath, R. (2001). The Cyberwar Debate. Perception and Politics in U.S. Critical Infrastructure Protection. *Information & Security*, *7*, 80-103.

Bendrath, R. (2003). The American Cyber-Angst and the Real World - Any Link? In R. Latham (Ed.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security* (First Edition ed., pp. 49-73). New Press, The.

Benford, R. D., & Snow, D. A. (1988). Ideology, Frame Resonance and Participant Mobilization. In B. Klandermans, H. Kriesi, & S. G. Tarrow (Eds.), *From structure to action: comparing social movement research across cultures*. Greenwich, Conn: JAI Press.

Benford, R. D., & Snow, D. A. (2000). Framing processes and social movements: An overview and assessment. *Annual review of sociology*, *26*(1), 611-639.

Benkler, Y. (2006). The Wealth of Networks: How Social Production Transforms Markets and Freedom (9/23/07 ed.). Yale University Press.

Benkler, Y. (2011). Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate, A. *Harv. CR-CLL Rev.*, *311*.

Bennett, A., & Checkel, J. T. (2014). Process Tracing: From Metaphor to Analytic Tool (Strategies for Social Inquiry). Cambridge University Press.

Bennett, A. J. (2013). The Race for the White House from Reagan to Clinton. Palgrave Macmillan.

Bennett, C. J., & Parsons, C. (2013). Privacy and Surveillance: The Multidisciplinary Literature on the Capture, Use and Disclosure of Personal Information in Cyberspace. In W. H. Dutton (Ed.), *The Oxford Handbook of Internet Studies*. Oxford: Oxford University Press.

Berger, A. A. (2008). Manufacturing Desire: Media, Popular Culture, and Everyday Life. Transaction Publishers.

Berger, T. (1996). Norms, Identity and National Security in Germany and Japan. In P. J. Katzenstein (Ed.), *The Culture of National Security: Norms and Identity in World Politics*.

Berners-Lee, T. (2016). Four Days to Save the Open Internet in Europe: An Open Letter. http://webfoundation.org/2016/07/four-days-to-save-the-open-internet-in-europe-an-open-letter/.

Berners-Lee, T. (1989). Information Management: A Proposal.

Berners-Lee, T. (2000). Weaving the Web. The Original Design and Ultimate Destiny of the World Wide Web. New York: Harper Business.

Berners-Lee, T., & Cailliau, R. (1990). WorldWideWeb: Proposal for a HyperText Project.

Besser, H. (1995). The information superhighway: Social and cultural impact. In J. Boal & I. Boal. San Francisco: City Lights Press.

Best, K. (2003). Revisiting the Y2K Bug Language Wars Over Networking the Global Order. *Television & New Media*, *4*(3), 297-319.

Betz, D. (2012). Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. *Journal of Strategic Studies*, *35*(5), 689-711.

Betz, D. J., & Stevens, T. C. (2012). Cyberspace and the State: Towards a Strategy for Cyberpower (Adelphi series) (1 ed.). New York: Routledge.

Betz, J., & Kübler, H.-D. (2013). Internet Governance: Wer regiert wie das Internet? (2013 ed.). Springer VS.

BeVier, L. R. (1999). The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break Up of AT&T. *Stanford Law Review*, *51*(5), 1049-1125.

Bijker, W. E. (1995). Of bicycles, bakelites, and bulbs: Toward a theory of sociotechnical change. MIT press.

Bijker, W. E., Hughes, T. P., & Trevor, J. (1987). The social construction of technological systems: New directions in the sociology and history of technology. Cambridge, MA: MIT Press.

Bijker, W. E. (2008). Why and How Technology Matters. In R. E. Goodin & C. Tilly (Eds.), *The Oxford Handbook of Contextual Political Analysis*. Oxford University Press, USA.

Biselli, A. (2016). Endlich öffentlich: Aussage des BND-Mitarbeiters A. Sch., der XKeyscore beim Verfassungsschutz installierte. https://netzpolitik.org/2016/endlich-oeffentlich-aussage-des-bnd-mitarbeiters-a-sch-der-xkeyscore-beim-verfassungsschutz-installierte/.

Bitton, R. (2014). The Legitimacy of Spying Among Nations. *American University International Law Review*, *29*(5), 1010-1065.

Blank, S. (2013). Russian Information Warfare as Domestic Counterinsurgency. American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy, 35, 31-44.

Blatter, J., & Haverland, M. (2012). Designing Case Studies: Explanatory Approaches in Small-N Research (Research Methods). Palgrave Macmillan.

Blatter, J., Janning, F., & Wagemann, C. (2007). Qualitative Politikanalyse: Eine Einführung in Forschungsansätze und Methoden (Grundwissen Politik) (2007 ed.). VS Verlag für Sozialwissenschaften.

Blom, J. D. (2010). Unmanned Aerial Systems: A Historical Perspective. *Occasional Paper 37*.

Bloss, W. (2007). Escalating U.S. Police Surveillance after 9/11: an Examination of Cause and Effects. *Surveillance & Society*, *4*(3), 208.228.

Börzel, T. A. (1998). Organizing Babylon - On The Different Conceptions of Policy Networks. *Public Administration*, *76*, 253-273.

Botnet, C. (2012). Internet Census 2012. Port Scanning /0 using insecure embedded devices. http://internetcensus2012.bitbucket.org/paper.html.

Boyd, A. (2016). DNI Clapper: Cyber bigger threat than terrorism. *Federal Times*. http://www.federaltimes.com/story/government/cybersecurity/2016/02/04/cyber-bigger-threat-terrorism/79816482/.

Brand, S. (1968). Whole Earth Catalog Fall 1968. http://www.wholeearth.com/issue-electronic-edition.php?iss=1010.

Brand, S. (1972). Spacewar. *Rolling Stone* http://scholar.googleusercontent.com/scholar.enw?q=info:Oo2Wn47HFAYJ:scholar.google.com/&output=citation&scisig=AAGBfm0AAAAAV6nV8sT-Li_fg8t5COFHp6YHJDwXIH3M&scisf=3&ct=citation&cd=0&hl=de.

Brand, S. (1995c). We owe it all to the Hippies. *Time Magazine*.

Brickel, E. F., Denning, D. E., Kent, S. T. et al. (1993). Skipjack Review. Interim Report. The SKIPJACK Algoritm. https://epic.org/crypto/clipper/skipjack_interim_review.html.

Broad, W. J. (1992). Clinton to Promote High Technology, With Gore in Charge. *The New York Times*. http://www.nytimes.com/1992/11/10/science/clinton-to-promote-high-technology-with-gore-in-charge.html?pagewanted=all.

Brown, G., & Poellet, K. (2012). The Customary International Law of Cyberspace. *Strategic Studies Quarterly*, *6*(3), 126-145.

Bucher, B. (2014). Von Normerosion und Normkontestation zu Normenkonkurrenz und Normenpolitik. Proceedings from 4th DVPW conference on International Politics.

Buckley, M., & Singh, R. (2006). The Bush Doctrine and the War on Terrorism: Global Responses, Global Consequences (New Ed ed.). Routledge.

Burman, E. (2003). Shift!: The Unfolding Internet-Hype, Hope and History. John Wiley & Sons.

Bush, G. W. (2002). President Bush Delivers Graduation Speech at West Point. https://georgewbush-whitehouse.archives.gov/news/releases/2002/06/images/20020601-3_westpointgradp18166-515h.html.

Bush, G. W. (2005). Text of President Bush's radio address on Saturday, as released by the White House. *The Washington Post* http://www.washingtonpost.com/wp-dyn/content/article/2005/12/17/AR2005121700498.html.

Bush, V. (1945). As we may think. *The Atlantic Monthly*, *176*(1), 101-108.

Buzan, B., Waever, O., & Wilde, J. D. (1997). *Security: A New Framework for Analysis* (Unabridged. ed.). London: Lynne Rienner Publishers Inc.

Collective, C. A. S. E. (2006). Critical Approaches to Security in Europe: A Networked Manifesto. *Security Dialogue*, *37*(4), 443-487.

Cairncross, F. (1997). Death of Distance: How the Communications Revolution Will Change Our Lives (First Printing ed.). Harvard Business School Press.

Castells, M. (1999). The Information Age, Volumes 1-3: Economy, Society and Culture (Information Age Series) (v. 1-3). Wiley-Blackwell.

Cate, F. H. (1994). The National Information Infrastructure: Policymaking and Policymakers. *Stan. L. & Pol'y Rev.*, *6*, 43.

Cauley, L. (2006). NSA has massive database of American's phone calls. *USA Today*.

Cerf, V. G. (1990). An Interview with VINTON CERF OH 191. *Reston, VA* https://conservancy.umn.edu/handle/11299/107214.

Cerf, V. G. (1993). Dr. Cerf's Letter to Congress. http://cpsr.org/prevsite/program/clipper/cerf-letter-to-congress.html/.

Cerf, V. G. (2014). Startup Grind Hosts Vint Verf (Internet Pioneer, Google). https://www.startupgrind.com/events/details/startup-grind-washington-dc-hosted-vint-cerf-internet-pioneer-google.

Cerf, V. G. (2015). Mail correspondence.

Cerf, V. G. (2000). Internet Society Panel on Business Method Patents.

Cerf, V. G., & Kahn, R. E. (1974). A protocol for packet network intercommunication. *IEEE*, *22*(5).

Cerf, V. G., & Kahn, R. E. (2000). Al Gore and the Internet. http://web.eecs.umich.edu/~fessler/misc/funny/gore,net.txt.

Chaikin, D. (2007). Network investigations of cyber attacks: the limits of digital evidence. *Crime, Law and Social Change*, *46*(4-5), 239-256.

Chatzis, N., Smaragdakis, G., Feldmann, A. et al. (2013). There is more to IXPs than meets the eye. *ACM SIGCOMM Computer Communication Review*, *43*(5), 19-28.
Checkel, J. (1997). Ideas and International Political Change. Soviet/Russian Behavior and the End of the Cold War. Yale University Press.
Checkel, J. (1998). The Constructive Turn in International Relations Theory. *World Politics*, *50*(2), 324-348.
Checkel, J. (1999). Norms, Institutions, and National Identity in Contemporary Europe. *International Studies Quarterly*, *43*(1), 83-114.
Chiang, O. J. (2009). The Decade in Data. http://www.forbes.com/2009/12/27/broadband-text-messages-technology-cio-network-data.html.
Childress, S. (2015). How the NSA Spying Programs Have Changed Since Snowden. *Frontline* http://www.pbs.org/wgbh/frontline/article/how-the-nsa-spying-programs-have-changed-since-snowden/.
Cisco Systems. (2016). *The Zettabyte Era — Trends and Analysis – Cisco.* CISCO. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html.
Clark, D. D., & Landau, S. (2011). Untangling attribution. *Harvard National Security Journal*, *2*, 323.
Clark, D. D. (1992). *A Cloudy Crystal Ball – Visions of the Future*. Proceedings from 24th Internet Engineering Task Force.
Clarke, R. A. (2004). Against All Enemies: Inside America's War on Terror (Reprint ed.). Free Press.
Clarke, R. A., & Knake, R. (2010). Cyber War: The Next Threat to National Security and What to Do About It (Reprint ed.). Ecco.
Clarke, R. A., Morell, M. J., Stone, G. R. et al. (2014). The NSA Report: Liberty and Security in a Changing World. The President's Review Group on Intelligence and Communications Technologies.
Clegg, S. R. (1989). *Frameworks of Power*. SAGE Publications Ltd.
Clinton-Gore Campaign Headquarters. (1992). Technology: The Engine for Economic Growth. A National Technology Policy for America September 18, 1992. Clinton-Gore Campaign Headquarters.
Clinton, H. R. (2010). Remarks on Internet Freedom. http://iipdigital.usembassy.gov/st/english/texttrans/2011/12/20111209083136su0.3596874.html.
Clinton, W. J. (1994). Electronic Mail Message to Prime Minister Carl Bildt of Sweden.
Clinton, W. J., & Gore, A. (1993). Technology for America's Economic Growth, A New Direction to Build Economic Strength.
CNBC. (2006). Bush on Google. https://www.youtube.com/watch?v=AQ45fO1uiOQ.
CNN. (2006). Looking at the Y2K Bug. https://web.archive.org/web/20060207191845/http://www.cnn.com/TECH/specials/y2k/.
Cohen, D. (1978). *On Interconnection of Computer Networks*. Proceedings from Interlinkining of Computer Networks., Bonas.
Cohen, H. (1997). The Communications Decency Act of 1996. *CRS Report for Congress*.
Cohen, M. S. (2016). Aristotle's Metaphysics. https://plato.stanford.edu/entries/aristotle-metaphysics/.
Cohen, N. (1994). Wiretapping and the Digital Telephony Bill: Past and Present. http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall94-papers/cohen-digital-telephony.html.
Cole, M., Esposito, R., Schone, M. et al. (2014). Exclusive: Snowden Docs Show British Spies Used Sex and 'Dirty Tricks'. http://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-british-spies-used-sex-dirty-tricks-n23091.
Coleman, G. (2013). Coding Freedom: The Ethics and Aesthetics of Hacking. Princeton University Press.
Coleman, G. (2014). Hacker, Hoaxer, Whistleblower, Spy: the Story of Anonymous. Verso Books.
Collins, S. (2004). Summary of Intelligence Reform and Terrorism Prevention Act of 2004. United States Senate Committee on Governmental Affairs.

Comey, J. (2014). Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

Computer Professionals for Social Responsibility. (1994). *Electronic Petition to Oppose Clipper.* https://epic.org/crypto/clipper/cpsr_electronic_petition.html.

Computerworld (2000). Some Key Facts and Events in Y2K History.

Congressional Budget Office. (2007). *Federal Support for Research and Development.* Congressional Budget Office. https://www.cbo.gov/sites/default/files/110th-congress-2007-2008/reports/06-18-research.pdf.

Congressional Digest. (2016). *Warrantless Police Entries.* http://congressionaldigest.com/issue/warrantless-police-entries/probable-cause-and-reasonable-suspicion/#gsc.tab=0.

Conrad, C. (2004). The Illusion of Reform: Corporate Discourse and Agenda Denial in the 2002 Corporate Meltdown. *Rhetoric & Public Affairs*, *7*(3), 311-338.

Cortell, A. P., & Davis, J. W. J. (1996). How Do international Institutions Matter? The Domestic Impact of International Rules and Norms. *International Studies Quarterly*, *40*(4), 451-478.

Creswell, J. W. (2012). Qualitative Inquiry & Research Design: Choosing Among Five Approaches. Sage Publications (CA).

Crocker, S. D. (2009). Op-Ed Contributor. How the Internet Got its Rules. *The New York Times*. http://www.nytimes.com/2009/04/07/opinion/07crocker.html?_r=0.

Crocker, S. D. (2012). Meet the man who invented the instructions for the Internet. *Wired*. http://www.wired.com/2012/05/steve-crocker/.

Crocker, S. D. (2015). Mail to Steve Crocker.

Dahlgren, P. (2015). Civic Cosmopolitanism and Political Communication. Media, Activism, and Agency. In R. Figueiras & P. D. Santo Espirito (Eds.), *Beyond the Internet: Unplugging the Protest Movement Wave* (pp. 7-30).

Dam, K. W., & Lin, H. S. (1996). Cryptography's Role in Securing the Information Society. National Research Council.

Daniel, J. (1996c). Cyberspace. *Texas Monthly*. http://www.texasmonthly.com/articles/cyberspace-•-mike-godwin/.

David, M. (2010). Peer to Peer and the Music Industry: The Criminalization of Sharing (Published in association with Theory, Culture & Society) (1 ed.). SAGE Publications Ltd.

David, P. A. (2001). The Beginnings and Prospective Ending of "End-to-End": An Evolutionary Perspective On the Internet's Architecture. *SIEPR Discussion Paper*, *No. 01-04*.

Davies, D. (1986). An Interview with Donald W. Davies. *National Physical Laboratory* https://conservancy.umn.edu/handle/11299/107241.

Davies, D. (1965). Proposal for the Development of a National Communications Service for On-Line Data Processing.

de Lint, W., & Kassa, W. (2015). Evaluating U.S. Counterterrorism Policy: Failure, Fraud, or Fruitful Spectacle. *Critical Criminology*, *23*(3), 349-369.

De Saussure, F. (1981). Course in general linguistics. Suffolk: Fontana.

Debnam, B. (1994). Answers from Vice President Al Gore: The Information Superhighway. *Observer-Reporter*.

Deibert, R. (2003). Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. *Millennium - Journal of International Studies*, *32*(3), 501-530.

Deibert, R. (2015). Cyberspace Under Siege. *Journal of Democracy*, *26*(3), 64-78.

Deibert, R., & Crete-Nishihata, M. (2012). Global Governance and the Spread of Cyberspace Controls. *Global Governance*, *18*, 339-361.

Deibert, R., Palfrey, J., Rohozinski, R. et al. (Eds.). (2008). Access Denied. The Practice and Policy of Global Internet Filtering. London: MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R. et al. (Eds.). (2010). Access Controlled. The Shaping of Power, Rights and Rule in Cyberspace. Cambridge, London: MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R. et al. (Eds.). (2012). Access Contested: Security, Identity, and Resistance in Asian Cyberspace. Cambridge, London: MIT Press.

Deitelhoff, N., & Zimmermann, L. (2013). Aus dem Herzen der Finsternis: Kritisches Lesen und wirkliches Zuhören der konstruktivistischen Normenforschung. Eine Replik auf Stephan Engelkamp, Katharina Glaab und Judith Renner. *ZIB*, 61-74.

DeNardis, L. (2009). Protocol Politics: The Globalization of Internet Governance (Information Revolution and Global Politics). Cambridge, London: The MIT Press.
Denardis, L. (2013). The Emerging Field of Internet Governance. In W. H. Dutton (Ed.), *The Oxford Handbook of Internet Studies*. Oxford: Oxford University Press.
DeNardis, L. (2015). The Global War for Internet Governance. Yale University Press.
Denning, P. J., Hearn, A., & Kern, W. C. (1983). *History and Overview of CSNET*. Proceedings from CSNET Project at the ACM SIGCOMM symposium on data communications, March 8-9, 1983.
Department of Defense. (1999). An assessment of international legal issues in information operations. Office of General Counsel.
Department of Defense. (2003). Information Operations Roadmap. Department of Defense.
Department of Defense. (2006). Directive Number TS-3600.01. Information Operations (1996).
Department of Defense. (2007). Department of Defense Global Information Grid Architectural Vision. Vision for a Net-Centric, Service-Oriented DoD Enterprise.
Department of Defense. (2010). Quadrennial Defense Review Report.
Department of Defense. (2015). *The DOD Cyber Strategy.*
Department of the Air Force. (2006). 609 IWS: A Brief History. Oct 1995 - Jun 1999.
Der Derian, J. (1992). Antidiplomacy: spies, terror, speed, and war. Blackwell.
Diersch, V. (2014). The President's Review Group on Intelligence and Communications Technologies. (2014). The NSA Report. Liberty and Security in a Changing World. *Zeitschrift für Außen & Sicherheitspolitk*, *7*(3), 417-419.
Diffie, W. (1993). The Impact of a Secret Cryptographic Standard on Encryption, Privacy, Law Enforcement and Technology.
Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, *22*(6), 644-654.
Director of National Intelligence. (2005). The National Intelligence Strategy of the United States of America. Transformation through Integration and Innovation. Office of the Director of National Intelligence.
Donati, P. R. (1992). Political discourse analysis. *Studying collective action*, 136-167.
Donohue, L. K. (2008). The Cost of Counterterrorism Power, Politics, and Liberty. Cambridge: Cambridge University Press.
Dourado, E., & Castillo, A. (2015). Federal Cybersecurity Breaches Mount Despite Increased Spending. http://mercatus.org/publication/federal-cybersecurity-breaches-mount-despite-increased-spending.
DPA (2017). Verfassungsschutz will Cybergegenangriffe starten. *Spiegel Online*. http://www.spiegel.de/netzwelt/netzpolitik/bundesamt-fuer-verfassungsschutz-plant-cyber-gegenangriffe-a-1129273.html.
DPA (2013). Dobrindt will Autobahnen zu Datenautobahnen machen. *FAZ*. http://www.faz.net/agenturmeldungen/dpa/dobrindt-will-autobahnen-zu-datenautobahnen-machen-13776332.html.
Drake, W. J. (1995a). The National Information Infrastructure Debate: Issues, Interests, and the Congressional Process. In W. J. Drake (Ed.), *The New Information Infrastructure: Strategies for U.S. Policy (A Twentieth Century Fund Book)* (English Language ed.). Twentieth Century Foundation.
Drake, W. J. (1995b). The New Information Infrastructure: Strategies for U.S. Policy (A Twentieth Century Fund Book) (English Language ed.). Twentieth Century Foundation.
Drake, W. J. (1995c). The Turning Point. In W. J. Drake (Ed.), The New Information Infrastructure: Strategies for U.S. Policy (A Twentieth Century Fund Book) (English Language ed.). Twentieth Century Foundation.
Dunn Cavelty, M. (2007). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (CSS Studies in Security and International Relations) (1 ed.). Routledge.
Dunn Cavelty, M. (2013a). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, *15*(1), 105-122.
Dunn Cavelty, M. (2015). Die materiellen Ursachen des Cyberkriegs Cybersicherheitspolitik jenseits diskursiver Erklärungen. *Journal of self-regulation and regulation*, *1*, 167-184.
Dunn Cavelty, M. (2010). Cyberwar. In G. Kassimeris & J. Buckley (Eds.), *The Ashgate Research Companion to Modern Warfare* (pp. 123-144). Farnham: Ashgate.

Dunn Cavelty, M. (2013b). Der Cyber-Krieg der (so) nicht kommt: Erzählte Katastrophen als (Nicht)Wissenspraxis. In L. Hempel & M. Bartels (Eds.), *Aufbruch ins Unversicherbare - Zum Katastrophendiskurs der Gegenwart* (pp. 209-233). Bielefeld: Transcript.

Dunn Cavelty, M., & Jaeger, M. D. (2015). (In)visible Ghosts in the Machine and the Powers that Bind: The Relational Securitization of Anonymous. *International Political Sociology*, *9*(2), 176-194.

Dutton, W. H. (2013a). Internet Studies: The Foundations of a Transformative Field. In W. H. Dutton (Ed.), *The Oxford Handbook of Internet Studies*. Oxford: Oxford University Press.

Dutton, W. H. (Ed.). (2013b). The Oxford Handbook of Internet Studies. Oxford: Oxford University Press.

DW. (2016). European Court of Justice rules against mass data retention in EU. http://www.dw.com/en/european-court-of-justice-rules-against-mass-data-retention-in-eu/a-36859714.

Dyson, E., Gilder, G., Keyworth, G. et al. (1994). Cyberspace and the American Dream: A Magna Carta for the Knowledge Age. http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html.

Eckstein, H. (1988). A Culturalist Theory of Political Change. *The American Political Science Review*, *82*(3), 789-804.

Economist. (2010). A virtual counter-revolution. http://www.economist.com/node/16941635.

Edmonds, A. J. (1996). C4I for the Warrior - Global Command and Control System: From Concept to Reality. Information Assurance Technology Analysis Center.

Edwards, P. N. (1997). The closed world: Computers and the politics of discourse in Cold War America. MIT Press.

Electronics (1972). Demonstration Heralds Next Wave: Connecting a Network of Networks. *Electronics*, pp. 34-36.

Ellul, J. (1990). *Technological Bluff* (1st ed.). Eerdmans Pub Co.

Elmer-Dewitt, P. (2016). Apple vs. FBI: What the Polls Are Saying. *Fortune* http://fortune.com/2016/02/23/apple-fbi-poll-pew/.

Elton, M. C. J., & Carey, J. (2013). The Prehistory of the Internet and its Traces in the Present: Implications for Defining the Field. In W. H. Dutton (Ed.), *The Oxford Handbook of Internet Studies*. Oxford: Oxford University Press.

Emirbayer, M., & Mische, A. (1998). What is agency? *The American Journal of Sociology*, *103*(4), 962-1023.

Engel, P. (2014). This World Map Shows Every Device Connected to the Internet. http://www.businessinsider.com/this-world-map-shows-every-device-connected-to-the-internet-2014-9?IR=T.

Engelkamp, S., Glaab, K., & Renner, J. (2012). In der Sprechstunde. *ZIB*, 101-128.

Engelkamp, S., Glaab, K., & Renner, J. (2013). Ein Schritt vor, zwei Schritte zurück? *ZIB*, 105-118.

Ensmenger, N. L. (2010). The Computer Boys Take Over: Computers, Programmers, and the Politics of Technical Expertise (History of Computing). Cambridge, London: The MIT Press.

EPIC. (2002). Communications Decency Act. https://epic.org/free_speech/cda/.

Epstein, C. (2008). The power of words in international relations: birth of an anti-whaling discourse. MIT Press.

Epstein, C. (2014). The postcolonial perspective: an introduction. *International Theory*, *6*(02), 294-311.

Eriksson, J. (2001). Cyberplagues, IT, and Security: Threat Politics in the Information Age. *Journal of Contingencies and Crisis Management*, *9*(4), 211-222.

Eriksson, J., & Giacomello, G. (2009). Forum: Who Controls the Internet? Beyond the Obstinacy or Obsoloscence of the State. *International Studies Review*, *11*(1), 205-230.

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review/ Revue internationale de science politique*, *27*(3), 221-244.

Erwin, M. C., & Belasco, A. (2013). Intelligence Spending and Appropriations: Issues for Congress.

Etling, B., Kelly, J., Faris, R. et al. (2010). Mapping the Arabic blogosphere: politics and dissent online. *New Media & Society*, *12*(8), 1225-1243.

Etymonline. (2016). Control. http://www.etymonline.com/index.php?term=control.
Ewen MacAskill, Borger, J., Hopkins, N. et al. (2013c). GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian*. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
Executive Office of the President of the United States. (2009). *Comprehensive National Cybersecurity Initiative.*
Fagerberg, J., Mowery, D. C., & Nelson, R. R. (2006). *The Oxford Handbook of Innovation* (1 ed.). Oxford University Press.
Farrell, T. (2001). Transnational Norms and Military Development: Constructing Ireland's Professional Army. *European Journal of International Relations*, *7*(1), 63-102.
Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, *53*(1), 23-40.
Fast, W. R. (1997). Knowledge Strategies: Balancing Ends, Ways, and Means in the Information Age. In R. E. Neilson (Ed.), Sun Tzu and information warfare: a collection of winning papers from the Sun Tzu art of war in information warfare competition. Washington, DC: National Defense University Press.
Feaver, P. D. (1998). Blowback: Information warfare and the dynamics of coercion. *Security Studies*, *7*(4), 88-120.
Ferran, L. (2014). Ex-NSA Chief: 'We kill people based on metadata'. http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata/.
Finnemore, M., & Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organization*, *52*(4), 887-917.
Finnemore, M., & Sikkink, K. (2001). Taking stock: the constructivist research program in international relations and comparative politics. *Annual Review of Political Science*, *4*(1), 391-416.
Fischer, E. A., Liu, E. C., Rollins, H. W. et al. (2013). The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress (CRS 7-5700). Congressional Research Service.
Fisher, D. (2013). What is a Man-in-the-Middle Attack? https://blog.kaspersky.com/man-in-the-middle-attack/1613/.
Florini, A. (1996). The evolution of international norms. *International Studies Quarterly*, 363-389.
Foschepoth, J. (2013). Überwachtes Deutschland: Post- und Telefonüberwachung in der alten Bundesrepublik (3. ed.). Vandenhoeck & Ruprecht.
Foucault, M. (1979). Discipline and punish: The birth of the prison. Penguin Books.
Freedom House. (2016). *Freedom on the Net. United States.* Freedom House. https://freedomhouse.org/sites/default/files/FOTN%202016%20United%20States.pdf.
Friedman, T. L. (2005). The world is flat: a brief history of the twenty-first century (1st ed. ed.). New York: Farrar, Straus and Giroux.
Fröhlich, M. (2011). Der Fall Libyen und die Norm der Schutzverantwortung. *Zeitschrift für Politikwissenschaft*, *21*(1), 135-150.
Fukuyama, F. (1992). The End of History & Last Man.
Fukuyama, F. (2000). The Great Disruption: Human Nature and the Reconstitution of Social Order (1st ed.). Free Press.
Fukuyama, F. (2002). Our Posthuman Future: Consequences of the Biotechnology Revolution. Farrar, Straus, Grioux.
G Data. (2015). *G Data publishes Analysis of Cyber-Espionage Programmes.* https://www.gdata-hongkong.com/en/news/article/article/g-data-publishes-analysis-of-cyber-espionage-programmes.
Gabbatt, A. (2013). Al Gore: Snowden 'revealed evidence' of crimes against US constitution. *The Guardian*. https://www.theguardian.com/world/2013/nov/06/al-gore-snowden-revealed-evidence-crimes-nsa.
Gabriel, G. (2006). Einführung in die Logik. Kurzes Lehrbuch mit Übungsaufgaben und Musterlösungen (2.). Jena.
Gadinger, F., Jarzebski, S., & Yildiz, T. (2014). Vom Diskurs zur Erzählung. Möglichkeiten einer politikwissenschaftlichen Narrativanalyse. *Politische Vierteljahresschrift*, *1*, 67-93.
Gallagher, R. (2015ac). From Paris to Boston, Terrorists were already known to authorities. *The Intercept*. https://theintercept.com/2015/11/18/terrorists-were-already-known-to-authorities/.

Gallagher, R. (2015bc). Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities. *The Intercept*. https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/.

Gallagher, R., & Greenwald, G. (2014c). How the NSA plans to infect 'Millions' of computers with malware. *The Intercept*. https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/.

Gallagher, R., & Maass, P. (2014). Inside the NSA's secret efforts to hunt and hack system administrators. *The Intercept* https://theintercept.com/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/.

Gallagher, S. (2013). You may already be a winner in NSA's "three-degrees" surveillance sweepstakes! *Ars Technica* http://arstechnica.com/information-technology/2013/07/you-may-already-be-a-winner-in-nsas-three-degrees-surveillance-sweepstakes/.

Galloway, A. R. (2006). Protocol: How Control Exists after Decentralization. The MIT Press.

Ganguly, S. (2010). *A constructivist analysis linking norm diffusion to policy networks*. Proceedings from Berlin Conference on the Human Dimensions of Global Environmental Change, Berlin 2010.

Gardner, J. M. (1994). The 1990-91 recession: how bad was the labor market? *Monthly Labor Review*.

Gartska, J. J., & Cebrowski, A. K. (1998). Network-Centric Warfare: Its Origin and Future. *U.S. Naval Institute*, *124*(1).

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security*, *38*(2), 41-73.

Gartzke, E., & Lindsay, J. R. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies*, *24*(2), 316-348.

Gates, B. (1995). *The Road Ahead* (First ed.). Viking.

Geers, K. (2011). *Strategic Cyber Security*. NATO Cooperative Cyber Defence Centre of Excellence Tallinn.

Geers, K. (Ed.). (2015). Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn: NATO CCD COE Publications.

Geier, B. (2015c). What Did We Learn From the Dotcom Stock Bubble of 2000? *Time Magazine*. http://time.com/3741681/2000-dotcom-stock-bust/.

Gellman, B., & Markon, J. (2013). Edward Snowden says motive behind leaks was to expose 'surveillance state'. *The Washington Post*. https://www.washingtonpost.com/politics/edward-snowden-says-motive-behind-leaks-was-to-expose-surveillance-state/2013/06/09/aa3f0804-d13b-11e2-a73e-826d299ff459_story.html?utm_term=.595b4fd91fa4.

Gellman, B., & Soltani, A. (2013). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post* https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

General Accounting Office. (1996). Computer Attacks at Department of Defense Pose Increasing Risks.

Gertz, B. (2011). Computer-based attacks emerge as threat of future, general says. *Washington Times*. http://www.washingtontimes.com/news/2011/sep/13/computer-based-attacks-emerge-as-threat-of-future-/.

Giacomello, G. (2005). National Governments and Control of the Internet. Routledge.

Giamoia, N. (2016). John MacAfee: We're on the Verge of Cyber War. *Fox Business*. http://www.foxbusiness.com/features/2016/02/19/john-mcafee-re-on-verge-cyber-war.html.

Gibson, J. J. (1979). The ecological approach to visual perception. Psychology Press.

Gibson, W. (1984). *Neuromancer* (1st ed.). Ace.

Giddens, A. (1984). The Constitution of Society: Outline of the Structuration Theory. Cambridge: Polity Press.

Gierow, H. (2016). China macht VPN genehmigungspflichtig. http://www.golem.de/news/internetzensur-china-macht-vpn-genehmigungspflichtig-1701-125749.html.

Gilardi, F. (2013). Transnational Diffusion: Norms, Ideas and Policies. In W. E. Carlsnaes, T. Risse, & B. A. Simmons (Eds.), *Handbook of International Relations* (Second Edition ed.). SAGE Publications Ltd.

Gillespie, T. (2006). Engineering a Principle: 'End-to-End' in the Design of the Internet. *Social Studies of Science*, *36*(3).

Glassman, J., Hassett, K., Glassman, J. K. et al. (1999). Dow 36,000: The New Strategy for Profiting from the Coming Rise in the Stock Market (1 ed.). Crown Business.

Glendinning, L. (2008). Obama, McCain computers 'hacked' during election campaign. *The Guardian*. https://www.theguardian.com/global/2008/nov/07/obama-white-house-usa.

Goertz, G., & Diehl, P. F. (1992). Toward a Theory of International Norms Some Conceptual and Measurement Issues. *Journal of Conflict Resolution*, *36*(4), 634-664.

Goertz, J., & Obermaier, F. (2013). Snowden enthüllt Namen der spähenden Telekomfirmen. *Süddeutsche Zeitung*. http://www.sueddeutsche.de/digital/internet-ueberwachung-snowden-enthuellt-namen-der-spaehenden-telekomfirmen-1.1736791.

Goffman, E. (1974). Frame Analysis: An essay on The Organization of Experience (1st THUS ed.). Harper Colophon.

Goldsmith, J., & Wu, T. (2008). Who Controls the Internet?: Illusions of a Borderless World. Oxford University Press, USA.

Goldstein, J., & Keohane, R. O. (1993a). Ideas and Foreign Policy: An analytical Framework. In J. Goldstein & R. O. Keohane (Eds.), *Ideas and Foreign Policy: Beliefs, Institutions, and Political Change (Cornell Studies in Political Economy)* (pp. 3-29). Cornell University Press.

Goldstein, J., & Keohane, R. O. (1993b). Ideas and Foreign Policy: Beliefs, Institutions, and Political Change. Cornell University Press.

Google. (2016). *Google Ngram Search with Terms Information Superhighway, Cyberwar, Global Village.* https://books.google.com/ngrams/graph?content=information+superhighway%2Ccyberwar%2Cglobal+village&year_start=1980&year_end=2000&corpus=15&smoothing=3&share=&direct_url=t1%3B%2Cinformation%20superhighway%3B%2Cc0%3B.t1%3B%2Ccyberwar%3B%2Cc0%3B.t1%3B%2Cglobal%20village%3B%2Cc0.

Google Trends. (2016). *Cyberwar Google Trends.* Google Inc. https://www.google.com/trends/explore?date=all&geo=US&q=cyberwar.

Gore, A. (1994a). Remarks Prepared for Delivery by Vice President Al Gore. Royce Hall, UCLA Los Angeles. http://www.ibiblio.org/icky/speech2.html.

Gore, A. (1989). National High-Performance Computer Technology Act. https://w2.eff.org/Legislation/Bills_by_sponsor/Old/gore_s1067_89.bill.

Gore, A. (1994b). Inauguration of the First World Telecommunication Development Conference. *World Telecommunication Development Conference (WTDC-94)*.

Gorman, S. (2006). System Error. The NSA has spent six years and hundreds of millions of dollars trying to kick-start a program, intended to help protect the United States against terrorism, that many experts say was doomed from the start. *Baltimore Sun*. http://articles.baltimoresun.com/2006-01-29/news/0601280286_1_intelligence-experts-11-intelligence- trailblazer.

Gorman, S. (2013). NSA officers spy on love interests. *The Wall Street Journal*. http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/.

Gramsci, A. (1971). Selections from the Prison Notebooks of Antonio Gramsci: Ed. and Transl. by Quintin Hoare and Geoffrey Nowell Smith. International Publishers.

Granovetter, M. S. (1973). The Strength of Weak Ties. *American Journal of Sociology*, *78*, 1360-1380.

Greenlee, M. J. (2008). National Security Letters and intelligence oversight. In R. A. Miller (Ed.), US National Security, Intelligence and Democracy: From the Church Committee to the War on Terror (Studies in Intelligence). Routledge.

Greenwald, G., & MacAskill, E. (2013). Boundless Informant: the NSA's secret tool to track global surveillance data. http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining.

Griffin, D. R. (2007). Neocon Imperialism, 9/11, and the Attacks on Afghanistan and Iraq. *Global Research*.

Grint, K., & Woolgar, S. (1997). The Machine at Work: Technology, Work and Organization (1 ed.). Polity.
Grove, G., Goodman, S., & Lukasik, S. (2010). Cyber-attacks and international law. *Survival: Global Politics and Strategy*, *42*(3), 89-104.
Haas, P. M. (1992). Introduction: Epistemic Communities and International Policy Coordination. *International Organization*, *46*(1), 1-35.
Habermas, J. (1970). Towards a theory of communicative competence. *Inquiry*, *13*(1-4), 360-375.
Hables Gray, C. (2003). Perpetual Revolution in Military Affairs, International Security and Information. In R. Latham (Ed.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security* (First Edition ed.). New Press, The.
Hafner, K., & Lyon, M. (1998). Where Wizards Stay Up Late: The Origins Of The Internet (First Paperback Edition ed.). Simon & Schuster.
Haggerty, R. V. E., Kevin. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605-622.
Hague, B. N., & Loader, B. D. (1999). Digital Democracy: Discourse and Decision Making in the Information Age. Routledge.
Hall, P. (1993). Policy Paradigms. Social learning, and the State. The Case of Economic Policymaking in Britain. *Comparative Politics*, *25*(3), 275-296.
Hall, S. (1996). The Problem of Ideology – Marxism without Guarantees'. In D. Morely & K.-H. Chen, Chen (Eds.), *Stuart Hall. Critical Dialogues in Cultural Studies*. London: Routledge.
Hallam-Baker, P. (2007). Security Protocol Failures. *IETF Journal*, *December*.
Halper, S., & Clarke, J. (2004). America Alone. The Neo-Conservatives and the Global Order (America Alone). Cambridge: Cambridge University Press.
Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*, 1155-1175.
Haraway, D. (1983). A Cyborg Manifesto. Science, technology and socialist-feminism in the late twentieth century. In D. Bell & B. M. Kennedy(pp. 296-324).
Harfoush, R. (2009). Yes We Did! An inside look at how social media built the Obama brand. New Riders.
Hargittai, E., & Hsieh, Y. P. (2013). Digital Inequality. In W. H. Dutton (Ed.), *The Oxford Handbook of Internet Studies*. Oxford: Oxford University Press.
Harknett, R. (2003). Integrated security: A strategic response to anonymity and the problem of the few. *Contemporary Security Policy*, *24*(1), 13-45.
Harris, S. (2006). Two controversial counter-terror programs share parallels. *Government Executive* http://www.govexec.com/defense/2006/06/two-controversial-counter-terror-programs-share-parallels/22064/.
Harris, S. (2007). NSA sought Data before 9/11. *National Journal*, *3*, 39-44.
Harris, S. (2014). @War: The Rise of the Military-Internet Complex (Reprint ed.). Eamon Dolan/Mariner Books.
Harvard Cyber Law. *Internet Quotation Appendix.* http://cyber.law.harvard.edu/archived_content/people/reagle/inet-quotations-19990709.html.
Häußling, R. (2010). Techniksoziologie. In G. Kneer & M. Schroer (Eds.), *Handbuch Spezielle Soziologien* (2010 ed.). VS Verlag für Sozialwissenschaften.
Häußling, R. (2014). *Techniksoziologie* (1. ed.). UTB GmbH, Stuttgart.
Hayden, M. V. (2016a). Hayden: The Pros and Cons of Access to Encrypted Files. https://www.youtube.com/watch?v=6HNnVcp6NYA.
Hayden, M. V. (2016b). Playing to the Edge: American Intelligence in the Age of Terror (1St Edition ed.). Penguin Press.
Hayes, B. (2012). The surveillance-industrial complex. In K. Ball, K. Haggerty, & D. Lyon (Eds.), *Routledge Handbook of Surveillance Studies* (Reprint ed., pp. 167-175). Routledge.
Healey, J., & Grindal, K. (2013). A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association.
Heart, F. (1990). An Interview with Frank Heart. *Cambridge, M.A.* https://archive.org/stream/NoTitle/BBND.txt.
Heart, F., McKenzie, A., McQuillan, J. et al. (1981). Completion Report No. 4799. A History of the ARPANET. The first decade. Bolt Beranek and Newman Inc.

Heller, R., Kahl, M., & Pisoiu, D. (2012). The 'dark' side of normative argumentation – The case of counterterrorism policy. *Global Constiutionalism*, *1*(02), 278-312.
Heller, R., & Kahl, M. (2013). Tracing and understanding "bad" norm dynamics in counterterrorism: the current debates in IR research. *Critical Studies on Terrorism*, *6*(3), 414-428.
Herman, M. (2004). Ethics and Intelligence after September 2001. *Intelligence and National Security*, *19*(2), 342-358.
Hern, A. (2014). US government increases funding for Tor, giving $1.8m in 2013. *The Guardian*.
Hernes, G. (1998). Real Virtuality. In P. Hedström & R. Swedberg (Eds.), *Social Mechanisms: An Analytical Approach to Social Theory* (pp. 74-101). Cambridge MA: Cambridge University Press.
Herrera, G. L. (2003). Technology and International Systems. *Millennium - Journal of International Studies*, *32*(3), 559-593.
Himanen, P. (2001). The Hacker Ethic and the Spirit of the Information Age. Random House.
Hitchens, C. (2009). God Is Not Great: How Religion Poisons Everything. Twelve.
Hjern, B. (1984). Going Interorganisational: Weber meets Durkheim. *Scandinavian Political Studies*, *7*(3), 197-212.
Hofheinz, A. (2011). Nextopia? Beyond Revolution 2.0. *International Journal of Communication*, *5*, 1417-1434.
Hofmann, J. (2005). Internet Governance: Zwischen staatlicher Autorität und privater Koordination. *Internationale Politik und Gesellschaft*, *3*.
Hofmann, J. (2015). Internet Governance: Theoretische und empirische Annäherungen an einen schwer fassbaren Gegenstand. *Journal of self-regulation and regulation*, *1*, 30-45.
Holen, A. (2008). A Comparison of the Technology Policies of Barack Obama and John McCain. https://techpolicyinstitute.org/policy_paper/a-comparison-of-the-technology-policies-of-barack-obama-and-john-mccain/.
Homeland Security Council. (2007). National Strategy for Homeland Security.
Honig, O. A. (2010). The Impact of CIA's Organizational Culture on Its Estimates Under William Casey. *International Journal of Intelligence and CounterIntelligence*, *24*(1), 44-64.
Hope, J. (2015). 7 phases of the history of Artificial intelligence. http://www.historyextra.com/article/ancient-greece/7-phases-history-artificial-intelligence.
Hopf, T. (2010). The logic of habit in International Relations. *European Journal of International Relations*, *16*(4), 539-561.
Horne, C. (2001). Sociological Perspectives on the Emergence of Norms. In M. Hechter & K.-D. Opp (Eds.), *Social Norms* (pp. 3-35). New York: Russell Sage Foundation.
Horrigan, J. B. (2001). Risky Business: Americans see greed, cluelessness behind dot-coms' comeuppance. *Pew Internet Tracking Report*.
Hösl, M. (2016). Internetpolitik als Effekt von diskursiven Grenzkonflikten. In B. Bergemann, J. Hofmann, F. Irgmaier et al. (Eds.), *Entstehung von Politikfeldern - Vergleichende Perspektiven und Theoretisierung* (Vol. WZB Discussion Paper SP IV 2016–401).
Houck, C. (2013). Barack Obama on surveillance, then and now. http://www.politifact.com/truth-o-meter/article/2013/jun/13/barack-obama-surveillance-then-and-now/.
Huddleston, T. (2015). These Russian submarines could attack the Internet itself. http://fortune.com/2015/10/26/russian-submarines-internet/.
Hughes, T. P. (1987). The Evolution of Large Technological Systems. In W. E. Bijker, T. P. Hughes, & J. Trevor (Eds.), *The social construction of technological systems: New directions in the sociology and history of technology*. Cambridge, MA: MIT Press.
Hülsse, R. (2006). Imagine the EU: the metaphorical construction of a supra-nationalist identity. *Journal of International Relations and Development*, *9*(4), 396-421.
Humpenöder, U. (2016). NSA-Skandal. So begann die Überwachung. *Frankfurter Allgemeine Zeitung*.
Hurrell, A., & McDonald, T. (2013). Ethics and Norms in International Relations. In W. E. Carlsnaes, T. Risse, & B. A. Simmons (Eds.), *Handbook of International Relations* (Second Edition ed., pp. 57-84as). SAGE Publications Ltd.
Hutchby, I. (2001). Technologies, Texts and Affordances. *Sociology*, *35*(2), 441-456.
Hyde, S. D. (2011). Catch Us If You Can: Election Monitoring and International Norm Diffusion. *American Journal of Political Science*, *55*(2), 356-369.

Ikenberry, G. J., Lake, D. A., & Mastanduno, M. (1988). *The state and American foreign economic policy*. Cornell University Press.
Ikenberry, J. G. (2007). The End of the Neo-Conservative Moment. *Survival*, *46*(1), 7-22.
Information Infrastructure Task Force. (1993). The National Information Infrastructure: Agenda for Action.
Inman, B. R. (1979). The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector. *Cryptologia*, *3*, 129-135.
International Telecommunications Union. (1994). Buenos Aires Declaration on Global Telecommunication Development for the 21st Century.
Internet History Museum. (2016). *Browsers: Windows on the Web.* http://www.computerhistory.org/revolution/the-web/20/388.
Internet Live Stats. (2016). *Internet Usage Statistics.* http://www.internetlivestats.com.
Internet Society. (2011). *Global Internet User Survey 2011.* http://www.internetsociety.org/events/chapter-events/2011/global-user-survey.
Isenberg, D. (1997). Rise of the Stupid Network. *Computer Telephony*, 16-26.
ISideWith.com. (2016). *The quick guide to America's 2016 Presidential candidates stances on NSA.* https://www.isidewith.com/candidate-guide/elections/2016-presidential/issues/domestic-policy/nsa-domestic-surveillance.
Jachtenfuchs, M. (1995). Ideen und internationale Beziehungen. *Zeitschrift für internationale Beziehungen*, *2*(2), 417-442.
Jackson, R. (2005). Writing the War on Terrorism: Language, Politics and Counter-terrorism. Manchester.
Jacobs, A. M. (2014). Process tracing the effects of ideas. In A. Bennett & J. T. Checkel (Eds.), *Process Tracing: From Metaphor to Analytic Tool (Strategies for Social Inquiry)* (pp. 41-73). Cambridge University Press.
Jepperson, R., Wendt, A., & Katzenstein, P. J. (1996). Norms, Identity, and Culture in National Security. In P. J. Katzenstein (Ed.), *Norms, Identity and National Security in Germany and Japan* (Vol. The Culture of National Security: Norms and Identity in World Politics).
Jernigan, C., & Mistree, B. F. T. (2009). Gaydar: Facebook friendships expose sexual orientation. *First Monday* http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2611/2302.
Jervis, R. L. (2011). Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War (Cornell Studies in Security Affairs) (1 ed.). Cornell University Press.
Jobs, S. (2005). Stanford Commencement Speech 2005. https://www.youtube.com/watch?v=D1R-jKKp3NA&t=12m45s.
Joerges, B. (1997). *Die Brücken des Robert Moses oder: Do Politics Have Artifacts? Zur Konstruktion von Stadtraum und Stadtgesellschaft in technik- und planungssoziologischen Diskursen*. Proceedings from Schriftenreihe der Forschungsgruppe "Metropolenforschung" des Forschungsschwerpunkts Technik - Arbeit - Umwelt am Wissenschaftszentrum Berlin für Sozialforschung.
Joint Chiefs of Staff. (1996a). Information Warfare. A strategy for Peace… The Decisive Edge in War. Department of Defense.
Joint Chiefs of Staff. (1996b). Information Warfare. Legal, Regulatory, Policy and Organizational Considerations for Assurance. The Joint Staff.
Joint Chiefs of Staff. (1996c). *Joint Vision 2010.* Chairman of the Joint Chiefs of Staff, 5126 Joint Staff, Pentagon, Washington, D.C. 20318-5126.
Joint Chiefs of Staff. (1998). Joint Doctrine for Information Operations.
Joint Chiefs of Staff. (2006). *Information Operations.*
Jones, J. M. (2010). In U.S., 6 in 10 View Iran as Critical Threat to U.S. Interests. http://www.gallup.com/poll/125996/view-iran-critical-threat-interests.aspx.
Jones, J. M. (2013). In U.S., 83% Say North Korean Nukes Are a Critical Threat. http://www.gallup.com/poll/160541/say-north-korean-nukes-critical-threat.aspx.
Jordan, T., & Taylor, P. A. (2004). Hacktivism and cyberwars: Rebels with a cause. *books.google.com*.
Jørgensen, M., & Phillips, L. (2002). Discourse analysis as theory and method.
Jr, N. (2001). Spy agency taps into undersea cable. http://www.zdnet.com/article/spy-agency-taps-into-undersea-cable/.

Kagan, D., Schmitt, G. J., & Donnelly, T. (2000). Rebuilding America's Defenses: strategy, forces and resources for a new century.

Kahn, R. E. (1995). The Role of Government in the Evolution of the Internet. In N. A. O. Engineering (Ed.), *Revolution in the U.S. Information Infrastructure*. Washington D.C.: National Academy Press.

Kahn, R. E. (2004). ROBERT KAHN: An Interview Conducted by Michael Geselowitz, IEEE History Center, 17 February 2004.

Kaplan, D. A. (1999). The Silicon Boys: And Their Valley of Dreams (First Edition ed.). William Morrow.

Kaplan, F. (2016). Dark Territory: The Secret History of Cyber War. Simon & Schuster.

Kapor, M. (1993). Where is the Digital Highway Really Heading? The Case for a Jeffersonian Information Policy. *Wired*.

Katzenstein, P. J., Jepperson, R., & Wendt, A. (1996). Norms, identity, and culture in national security. In *The Culture of National Security: Norms and Identity in World Politics* (pp. 33-75). New York.

Kaufman, S. J. (2012). U.S. National Security Strategy from Bush to Obama. In B. M. Rajaee & M. J. Miller (Eds.), *National security under the Obama administration*. Palgrave Macmillan.

Keck, M. E., & Sikkink, K. (1994). Transnational Advocacy Networks in International and Regional Politics. In F. V. Kratochwil & E. D. Mansfield (Eds.), *International Organization And Global Governance: A Reader* (2 ed., pp. 162-176). Longman.

Kedzie, C. (1997). Communication and Democracy: Coincident Revolutions and the Emergent Dictators. RAND.

Kedzie, C., & Aragon, J. (2002). Coincident Revolutions and the Dictator's Dilemma. In J. Emmons Allison (Ed.), *Technology, Development, and Democracy: International Conflict and Cooperation in the Information Age*. Albana: State University of New York Press.

Keen, A. (2014). The Internet Is Not the Answer. Atlantic Monthly Press.

Kehl, D., Wilson, A., & Bankston, K. S. (2015). Doomed to repeat history? Lessons from the Crypto Wars of the 1990s. *Report from the New America Foundation*.

Kelley, J. (2008). Assessing the Complex Evolution of Norms: The Rise of International Election Monitoring. *International Organizations*, *62*(02).

Kellner, D. (2002). Postmodern War in the Age of Bush II. *New Political Science*, *24*(1), 57-72.

Kelly, K. (1999). The Roaring Zeros. *Wired* http://www.wired.com/1999/09/zeros/.

Kelly, K. (1998). *New Rules for the New Economy*. New York, London, Victoria, Toronto, Auckland, New Delhi: Viking.

Keohane, R. O. (1979). After Hegemony: Cooperation and Discord in the World Political Economy. Princeton University Press.

KGP (2013). 100-Millionen-Programm. BND will Internet-Überwachung massiv ausweiten. *Spiegel Online*.

Khazaeli, S., & Stockemer, D. (2013). The Internet: A new route to good governance. *International Political Science Review*, *34*(5), 463-482.

King, G. (2011). Edison vs. Westinthgouse: A shocking rivalry. http://www.smithsonianmag.com/history/edison-vs-westinghouse-a-shocking-rivalry-102146036/.

Kingdon, J. W. (2003). Agendas, Alternatives and Public Policies (second edition ed.). Longman.

Kingdon, J. W. (2010). Agendas, Alternatives, and Public Policies (2 ed.). Pearson.

Kirk, M. (2014). United States of Secrets. Part One: The Program : PBS Frontline.

Kleinrock, L. (1961). Information Flow in Large Communication Nets.

Kleinrock, L. (1990). An Interview with LEONARD KLEINROCK OH 190. *Los Angeles* http://conservancy.umn.edu/handle/11299/107411.

Kleinrock, L. (2015). Mail Correspondence.

Klotz, A. (1995). Norms reconstituting interests: global racial equality and US sanctions against South Africa. *International Organization*, *49*(3), 451-451.

Knightley, P. (2003). The Second Oldest Profession: Spies and Spying in the Twentieth Century. PIMLICO.

Kowert, P., & Legro, J. (1996). Norms, Identity, and Their Limits: A Theoretical Reprise. In *The Culture of National Security: Norms and Identity in World Politics*.

Kremer, J.-F., & Müller, B. (Eds.). (2014). Cyberspace and International Relations: Theory, Prospects and Challenges. Berlin, Heidelberg: Springer Berlin Heidelberg.
Krepinevich, A. F. (1992). *The Military-Technical Revolution: A Preliminary Assessment*. Proceedings from Prepared for the Office of Net Assessment, Washington D.C.
Kroft, S. (2012). Stuxnet: Computer Worm Opens New Era of Warfare. *CBS News* http://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/.
Krook, M. L., & True, J. (2012). Rethinking the life cycles of international norms: The United Nations and the global promotion of gender equality. *European Journal of International Relations*, *18*(1), 103-127.
Kuhn, T. S. (1970). The Structure of Scientific Revolutions. University of Chicago press.
Kurzweil, R. (1999). *Age of Spiritual Machines* (First Edition ed.). Viking.
Laclau, E., & Mouffe, C. (1987). Post-Marxism without apologies. *New Left Review*, *166*, 79-106.
Landau, S. (2010). Surveillance or Security. The MIT Press.
Landau, S. (2013). Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations. *IEEE Security & Privacy*, *11*(4), 54-63.
Landau, S. (2016). The real security issues of the iPhone case. Law enforcement needs 21st-century investigative savvy. *Sciencemag*, *352*(6292), 1398-1399.
Langner, R. (2013). To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve. *The Langner Group* http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.
Lapid, Y. (1989). The third debate: On the prospects of international theory in a post-positivist era. *International Studies Quarterly*, *33*(3), 235-254.
Latour, B. (1996). On Actor-Network Theory. A few clarifications plus more than a few complications. *Soziale Welt*, *47*, 369-381.
Latour, B. (2000). When things strike back: a possible contribution of science studies' to the social sciences. *British Journal of Sociology*, *5*(1), 107-123.
Latour, B. (2005a). On using ANT for studying information systems: a (somewhat) Socratic dialogue. In *Reassembling the Social: An Introduction to Actor-Network-Theory* (First Edition ed.). Oxford University Press.
Latour, B. (2005b). Reassembling the Social: An Introduction to Actor-Network-Theory (First Edition ed.). Oxford University Press.
Lawson, S. (2011). Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History. *Mercatus Center George Mason University*, *Working Paper 11-01*.
Lawson, S. (2012). Putting the war in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. *First Monday*, *17*(7).
Lee, N. (2015). Counterterrorism and Cybersecurity. Total Information Awareness. Heidelberg/London: Springer.
Legro, J. W. (2000). Whence American Internationalism. *International Organization*, *54*(2), 253-289.
Leiner, B. M., Cerf, V. G., Clark, D. D. et al. (2015). Brief History of the Internet. http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.
Lepri, C. (2012). Obama's New Intelligence Policy. Meeting new challenges. In B. M. Rajaee & M. J. Miller (Eds.), *National security under the Obama administration*. Palgrave Macmillan.
Lerner, C. S. (2003). The USA Patriot Act: Promoting the Cooperation of Foreign Intelligence Gathering and Law Enforcement. *George Mason Law Review*, *11*(3), 493-526.
Lessig, L. (2000). Code: And Other Laws of Cyberspace. Basic Books.
Lessig, L. (2006). Code: And Other Laws of Cyberspace, Version 2.0. Basic Books.
Levitas, R. (2010). Concept of Utopia (Utopianism and communitarianism) (1 ed.). Syracuse University Press.
Levy, S. (1993). Crypto Rebels. http://www.wired.com/1993/02/crypto-rebels/.
Levy, S. (1994). Battle of the Clipper Chip. *The New York Times* http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html.
Levy, S. (1995). This Changes Everything. *Newsweek*, *126/127*(27/1).
Levy, S. (2010). Hackers: Heroes of the Computer Revolution - 25th Anniversary Edition (1 ed.). O'Reilly Media.

Lewis, A. J. (1980c). Reviews the non-fiction book 'The Third Wave,' by Alvin Toffler. *Educational Leadership*, p. 226.
Lewis, J. A. (2002). Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats. *Center for Strategic & International Studies*.
Lewis, J. A. (2015). The Role of Offensive Cyber Operations in NATO's collective defence. *Tallinn Paper*, *9*.
Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. RAND Corporation.
Libicki, M. C. (2014). Why Cyber War Will Not and Should Not Have Its Grand Strategist. *Strategic Studies Quarterly*, *Spring*.
Lichtblau, E., & Risen, J. (2005). Spy Agency Mined Vast Data Trove, Officials Report. *The New York Times*. http://www.nytimes.com/2005/12/24/politics/spy-agency-mined-vast-data-trove-officials-report.html?_r=0.
Licklider, J. C. R. (1990). Man-Computer Symbiosis. In D. S. R. Center (Ed.), *In Memoriam: J. C. R. Licklider 1915-1990*.
Liese, A. (2009). Exceptional Necessity-How Liberal Democracies Contest the Prohibition of Torture and Ill-Treatment When Countering Terrorism. *Journal of International Law and International Relations*, *5*(1), 17-47.
Lilleker, D. G., & Vedel, T. (2013). The Internet in Campaigns and Elections. In W. H. Dutton (Ed.), *The Oxford Handbook of Internet Studies*. Oxford: Oxford University Press.
Lin, H. S., Dam, K. W., & Owens, W. A. (2009). Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities. National Academies Press.
Linchuan Qiu, J. (2013). Network Societies and Internet Studies: Rethinking Time, Space, and Class. In W. H. Dutton (Ed.), *The Oxford Handbook of Internet Studies*. Oxford: Oxford University Press.
Lindekilde, L. (2014). Discourse and Frame Analysis: In-depth Analysis of Qualitative Data in Social Movement Research. In D. Porta (Ed.), *Methodological Practices in Social Movement Research*.
Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, *22*(3), 365-404.
Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (2015). China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain (1 ed.). Oxford University Press.
Lukasik, S. (1991). An Interview with Stephen Lukasik OH 232. *Redondo Beach* http://conservancy.umn.edu/handle/11299/107446.
Lukasik, S. (2011). Why the ARPANET was built. *IEEE Annals of the History of Computing*, *33*(3), 4-20.
Lynn, W. J. (2010). Defending a New Domain. The Pentagon's Cyberstrategy. *Foreign Affairs*. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.
Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*.
MacAskill, E. (2016). 'Extreme surveillance' becomes UK law with barely a whimper. https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper.
Mackie, J. (1977). Ethics: Inventing right and wrong. Penguin UK.
MacKinnon, R. (2009). China's Censorship 2.0: How companies censor bloggers. *First Monday*, *14*(2).
Madrick, J. (2001). The Business Media and the New Economy. The Joan Shorenstein Center on the Press, Politics and Public Policy John F. Kennedy School of Government, Research Paper R-24.
Mandel, M. (1996). The Triumph Of The New Economy. A powerful payoff from globalization and the Info Revolution. *Bloomberg*. https://www.bloomberg.com/news/articles/1996-12-29/the-triumph-of-the-new-economy.
Manjoo, F. (2009). Apocalypse then. http://www.slate.com/articles/technology/technology/features/2009/apocalypse_then/was_y2k_a_waste.html.
Margetts, H. (2013). The Internet and Democracy. In W. H. Dutton (Ed.), *The Oxford Handbook of Internet Studies*. Oxford: Oxford University Press.
Matthewman, S. (2011). Technology and Social Theory (Themes in Social Theory). Palgrave Macmillan.

Matthews, J. T. (1997). Power Shift. *Foreign Affairs*.
Maull, H. W. (2000). Germany and the Use of Force: Still a 'Civilian Power'? *Survival*, *42*(2), 56-80.
Mauss, M. (1990). The Gift. The Form and Reason for Exchange in Archaic Societies. New York: Norton.
Mayer-Schönberger, V., & Cukier, K. (2014). Big Data: A Revolution That Will Transform How We Live, Work, and Think (Reprint ed.). Eamon Dolan/Mariner Books.
Mayer, J. (2006). The hidden power. The legal mind behind the White House's war on terror. *The New Yorker*.
Mazarr, M. J. (1994). *The Revolution in Military Affairs: A Framework for Defense Planning*. Proceedings from U.S. Army War College Fifth Annual Strategy Conference held April 26-28, 1994.
McCarthy, D. R. (2013). Technology and 'the International' or: How I Learned to Stop Worrying and Love Determinism. *Millennium - Journal of International Studies*, *41*(3), 470-490.
McCarthy, J. P. (1997). Managing Battlespace Information: The Challenge of Information Collection, Distribution, and Targeting. In R. L. Pfaltzgraff & R. H. Shultz (Eds.), *War in the Information Age: New Challenges for U S Security (Association of the United States Army)*. Brassey's UK Ltd.
McCarthy, J. (2016). Americans Cite Cyberterrorism Among Top Three Threats to U.S. http://www.gallup.com/poll/189161/americans-cite-cyberterrorism-among-top-three-threats.aspx.
McCarthy, T. (2014). Obama announces new limits on NSA surveillance programs – live reaction. *The Guardian*. https://www.theguardian.com/world/2014/jan/17/obama-nsa-surveillance-reforms-speech-live#block-52d99585e4b040bca45b4a9f.
McChesney, R. W. (1996). The Internet and US communication policy-making in historical and critical perspective. *Journal of Communication*, *46*(1), 98-124.
McConnell, M. (2009). Cyberwar is the New Atomic Age. *New Perspectives Quarterly*, *26*(3), 72-77.
McConnell, M. (2010). Mike McConnell on how to win the cyber-war were losing. *Washington Post*, *28*, B01.
McCullough, B. (2014a). The NSA and the 1990s Debate Over the Clipper Chip. http://www.internethistorypodcast.com/2014/09/the-nsa-and-the-1990s-debate-over-the-clipper-chip/.
McCullough, B. (2014b). Did Al Gore really invent the Internet? http://www.internethistorypodcast.com/2014/11/did-al-gore-really-invent-the-internet/.
McCullough, B. (2015). Chapter 6 - A history of Internet Porn. http://www.internethistorypodcast.com/2015/01/history-of-internet-porn/.

McEvoy Manjikian, M. (2010). From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly*, *54*, 381-401.
McKeown, R. (2009). Norm regress: US revisionism and the slow death of the torture norm. *International Relations*, *23*(1), 5-25.
McKnight, L., & Neumann, R. W. (1995). Technology Policy and the National Information Infrastructure. In W. J. Drake (Ed.), *The New Information Infrastructure: Strategies for U.S. Policy (A Twentieth Century Fund Book)* (English Language ed.). Twentieth Century Foundation.
McLeary, P. (2015). NATO Chief: Cyber can Trigger Article 5. http://www.defensenews.com/story/defense/policy-budget/warfare/2015/03/25/nato-cyber-russia-exercises/70427930/.
McLuhan, M. (1964). Understanding Media. The extensions of man. London, New York.
McPherson, S. S. (2012). War of the Currents: Thomas Edison Vs Nikola Tesla (Scientific Rivalries and Scandals). Twenty-First Century Books.
Merit Networks. (1995). NSFNET: A Partnership for High-Speed Networking. Final Report 1987-1955.
Metcalfe, R. (2004). Oral-History: Robert Metcalfe. *Waltham, MA* http://ethw.org/Oral-History:Robert_Metcalfe.

Metcalfe, R. (2006). Oral History of Robert Metcalfe. *Boston, MA* http://archive.computerhistory.org/resources/text/Oral_History/Metcalfe_Robert_1/Metcalfe_Robert_1_2.oral_history.2006.7.102657995.pdf.

Meyers, R. (1990). Metatheoretische und methodologische Betrachtungen zur Theorie der internationalen Beziehungen. *Politische Vierteljahresschrift (Sonderheft)*, *21/1990*, 48-68.

Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook. Sage.

Miller, R. A. (Ed.). (2008). US National Security, Intelligence and Democracy: From the Church Committee to the War on Terror (Studies in Intelligence). Routledge.

Minnesota Internet Traffic Studies. (2017). *Minnesota Internet Traffic Studies.* University of Minnesota. http://www.dtc.umn.edu/mints/home.php.

Mintrom, M., & Norman, P. (2009). Policy entrepreneurship and policy change. *Policy Studies Journal*, *37*(4), 649-667.

Misiroglu, G. (2015). American Countercultures: An Encyclopedia of Nonconformists, Alternative Lifestyles, and Radical Ideas in U.S. History: An Encyclopedia of Nonconformists. and Radical Ideas in U.S. History. Routledge.

Mitchell, W. J. (2000). *e-topia*. The MIT Press.

Molander, R. C., Riddle, A. S., & Wilson, P. A. (1996). Strategic Information Warfare. A New Face of War. Prepared for the Office of the Secretary of Defense. RAND Corporation.

Monten, J. (2005). The roots of the Bush doctrine: Power, nationalism, and democracy promotion in US strategy. *International Security*, *29*(4), 112-156.

Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival*, *58*(1), 7-38.

Morgan, P. M. (2000). The impact of the revolution in military affairs. *Journal of Strategic Studies*, *23*(1), 132-162.

Morozov, E. (2009). The exaggerated fears over digital warfare. *Boston Review*, *34*(4).

Morozov, E. (2011). The Net Delusion: The Dark Side of Internet Freedom (Reprint ed.). PublicAffairs.

Mosco, V. (2004). *The digital sublime*. Cambridge, London: MIT Press.

Mueller, M. (2005). Who Owns the Internet? Ownership as a Legal Basis for American Control of the Internet. *Fordham Intellectual Property, Media and Entertainment Law Journal*, *15*(3), 709-748.

Mueller, M. (2010). Networks and States. The Global Politics of Internet Governance. Cambridge, London: MIT Press.

Mueller, M., Schmidt, A., & Kuerbis, B. (2013). Internet Security and Networked Governance in International Relations. *International Studies Review*, *15*(1), 86-104.

Mulrine, A. (2011). CIA Chief Leon Panetta: The Next Pearl Harbor Could be a Cyberattack. *Christian Science Monitor*, *9*.

Murakami Wood, D. (2015). Before and After Snowden. *Surveillance & Society*, *13*(2), 132-138.

Murphy, T. (2012). Newt's New-Age Love Gurus. http://www.motherjones.com/politics/2012/01/newt-gingrich-new-age-love-gurus-alvin-toffler.

Mutaf, P. (1999). An Approach to the Security Problems in the TCP/IP Protocol Suite for a Network Security Monitor Design. Izmir Institute of Technology.

Mützel, D. (2016). BND-Reform: Was der Bundestag beschlossen hat, ist technisch gar nicht umsetzbar. http://motherboard.vice.com/de/read/was-der-bnd-ab-heute-machen-darf-ist-technisch-gar-nicht-moeglich.

Najafabadi, M. M., Villanustre, F., Khoshgoftaar, T. M. et al. (2015). Deep learning applications and challenges in big data analytics. *Journal of Big Data*, *2*(1), 886.

Nakashima, E. (2016). Obama moves to split cyberwarfare command from the NSA. https://www.washingtonpost.com/world/national-security/obama-moves-to-split-cyberwarfare-command-from-the-nsa/2016/12/23/a7707fc4-c95b-11e6-8bee-54e800ef2a63_story.html?utm_term=.ef3657183b93.

Nakashima, E., Miller, G., & Tate, J. (2012). U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

Nakashima, E., & Warrick, J. (2013). For NSA chief, terrorist threat drives passion to 'collect it all'. https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-

drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html?utm_term=.69fc703b456a.
NASDAQ. (2016). *NASDAQ Composite Index (COMP).* http://www.nasdaq.com/markets/nasdaq-composite.
National Research Council. (1988). *Toward A National Research Network.* National Research Network Review Committee, Computer Science and Technology Board, Commission on Physical Sciences, Mathematics, and Resources. http://www.nap.edu/read/10334/chapter/1.
National Research Council. (1991). Computers at Risk. Safe Computing In the Information Age. National Academy Press.
National Science Foundation. (1992). *The NSFNET Backbone Service Acceptable Use Policy.* https://w2.eff.org/Net_culture/Net_info/Technical/Policy/nsfnet.policy.
National Science Foundation. (2016). *A Brief History of NSF and the Internet.* https://www.nsf.gov/news/special_reports/cyber/internet.jsp.
Naughton, J. (1999). A brief history of the future. The origins of the Internet. Weidenfeld & Nicolson.
Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. *Journal of Cyber Policy*, *1*, 5-28.
NDR. (2014). *Snowden-Interview: Transcript.* https://web.archive.org/web/20140128224442/http://www.ndr.de/ratgeber/netzwelt/snowden277_page-7.html.
Negroponte, N. (1995). *Being Digital* (1 ed.). London: Hodder & Stoughton.
Nelson, T. N. (1974). *Computer Lib.* Sven Dollars.
Niskanen, W. A. (1988). Reagonomics. In D. R. Henderson (Ed.), *Concise Encyclopedia of Economics*.
Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media Society*, *6*(2), 195-217.
Nissenbaum, H. (2005). Where Computer Security Meets National Security. *Ethics in Information Technology*, *7*(2), 61-73.
Noam, E. M. (1995). Beyond Telecommunications Liberalization: Past Performance, Present Hype, And Future Direction. In W. J. Drake (Ed.), *The New Information Infrastructure: Stategies for U.S. Policy (A Twentieth Century Fund Book)* (English Language ed.). Twentieth Century Foundation.
Nye, J. (2010). *Cyber power*. DTIC Document.
Nye, J. (2011). *The Future of Power* (Reprint ed.). PublicAffairs.
O'Connell, M. E. (2012). Cyber Security without Cyber War. *Journal of Conflict and Security Law*, *17*(2), 187-209.
O'Neill, R. P. (1997). Integrating Offensive and Defensive Information Warfare. In R. L. Pfaltzgraff & R. H. Shultz (Eds.), *War in the Information Age: New Challenges for U S Security (Association of the United States Army)*. Brassey's UK Ltd.
Obama, B. (2007). Connecting and Empowering All Americans Through Technology and Innovation. http://www.presidency.ucsb.edu/ws/?pid=91809.
Obama, B. (2008). Network Neutrality. Snow and Dorgan's legislation to protect network neutrality. http://obamaspeeches.com/076-Network-Neutrality-Obama-Podcast.htm.
Obama, B. (2009a). Remarks by President Barack Obama at Town Hall Meeting with Future Chinese Leaders.
Obama, B. (2009b). Remarks by the President on Securing Our Nation's Cyber Infrastructure. https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.
Obama, B. (2012). Taking the Cyberattack Threat Seriously. *The Wall Street Journal*. http://www.wsj.com/articles/SB10000872396390444330904577535492693044650.
Obama, B. (2014). Remarks by the President on Review of Signals Intelligence.
Office of Homeland Security. (2002). National Strategy for Homeland Security.
Office of Personnel Management. (2015). *Cyber Security Incidents. What happened.* https://www.opm.gov/cybersecurity/cybersecurity-incidents/.
Office of Technology Assessment. (1990). Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage. U.S. Congress.
Office of Technology Assessment. (1993). *Advanced Network Technology.* U.S. Congress.

Office of Technology Assessment. (1995). Global Communications: Opportunities for Trade and Aid. U.S. Government Printing Office.
Ohmae, K. (1999). The Borderless World. Power and Strategy in the Interlinked Economy (Revised ed. ed.). HarperBusiness.
Onea, T. (2013). US Foreign Policy in the Post-Cold War Era. Palgrave Macmillan.
Oxford English Dictionary. (2017). *Design.* https://en.oxforddictionaries.com/definition/design.
Panetta, L. E. (2012). Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City. http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.
Papp, D. S., & Alberts, D. S. (Eds.). (2000). Information Age Anthology, Vol II: National Security Implications of the Information Age. (Vol. 2). CCRP Publication Series.
Pärna, K. (2010). *Believing the Net.* Leiden University Press.
Parsons, C. (2013). The Politics of Deep Packet Inspection: What Drives Surveillance by Internet Service Providers?
Passeri, P. (2016). November 2016 Cyber Attacks Statistics. http://www.hackmageddon.com/2016/12/21/november-2016-cyber-attacks-statistics/.
Payne, R. A. (2001). Persuasion, Frames and Norm Construction. *European Journal of International Relations*, *7*(1), 37-61.
Pelkey, J. (2014). Entrepreneurial Capitalism and Innovation: A History of Computer Communications 1968-1988. http://www.historyofcomputercommunications.info.
Penke, M. (2012). Like and Strike: Die Bedeutung der Neuen Medien im Arabischen Frühling. Interdisziplinäre Forschungsgruppe Abrüstung, Rüstungskontrolle und Risikotechnologien, Working paper.
Peoples Computer Company. (1972). *People's Computer Company.* https://purl.stanford.edu/ht121fv8052.
Peter, I. (2004). History of the Internet. http://www.nethistory.info/History%20of%20the%20Internet/.
Peters, B. (2016). How Not to Network a Nation: The Uneasy History of the Soviet Internet. The MIT Press.
Peterson, A. (2016). Are squirrels a bigger threat to the power grid than hackers? *The Washington Post*.
Pew Research Center. (2008). Even as Optimism About Iraq Surges. DECLINING PUBLIC SUPPORT FOR GLOBAL ENGAGEMENT. http://www.people-press.org/files/legacy-pdf/453.pdf.
Pew Research Center. (2016). *Public Uncertain, Divided over America's Place in the World.* http://www.people-press.org/files/2016/05/05-05-2016-Foreign-policy-APW-release.pdf.
Pew Research Center. (2013). *America's Place in the World 2013.* Pew Research Center. http://www.people-press.org/files/2013/12/12-3-13-APW-VI-release1.pdf.
Pfaffenberger, B. (1988). The Social Meaning of the Personal Computer: Or, Why the Personal Computer Revolution was no Revolution. *Anthropological Quarterly*, *61*(1), 39-47.
Pfaffenberger, B. (1992a). Technological Dramas. *Science, Technology & Human Values*, *17*(3), 282-312.
Pfaffenberger, B. (1992b). Social Anthropology of Technology. *Annual Review of Anthropology*, *21*, 491-516.
Pfaltzgraff, R. L., & Shultz, R. H. (Eds.). (1997). War in the Information Age: New Challenges for US Security (Association of the United States Army). Brassey's UK Ltd.
Pick, R. (2015). A Look at France's New Surveillance Laws in the Wake of the Paris Attacks. http://motherboard.vice.com/read/a-look-at-frances-new-surveillance-laws-in-the-wake-of-the-paris-attacks.
Pierson, P. (2000). Not just what, but when: Timing and sequence in political processes. *Studies in american political development*, *14*(01), 72-92.
Podesta, J. (2002). USA Patriot Act-The Good, the Bad, and the Sunset. *Human Rights*, *29*(1), 3.
Poindexter, J. (2002). Overview of the Information Awareness Office. Remarks as prepared for delivery by Dr. John Poindexter, Director, Information Awareness Office of DARPA, at DARPATech 2002 Conference, Anaheim, Calif., August 2, 2002 https://fas.org/irp/agency/dod/poindexter.html.

Poitras, L., Rosenbach, M., & Stark, H. (2014). 'A' for Angela: GCHQ and NSA Targeted Private German Companies and Merkel. http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html.

Poletta, F., & Kai Ho, M. (2008). Frames and their consequences. In R. E. Goodin & C. Tilly (Eds.), *The Oxford Handbook of Contextual Political Analysis (Oxford Handbooks of Political Science)*. Oxford University Press, USA.

Potter, W. C. (1978). Coping with MIRV in a MAD World. *Journal of Conflict Resolution*, *22*(4), 599-626.

Powell, W. W. (1990). Neither market nor hierarchy: Network forms of organization. *Research on Organizational Behavior*, *12*, 295-336.

Prensky, M. (2001). Digital Natives, Digital Immigrants. *On the Horizon*, *9*(5).

President's Commission on Critical Infrastructure Protection. (1997). Critical Foundations. Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection.

Priest, D., & Arkin, W. M. (2012). Top Secret America: The Rise of the New American Security State (Reprint ed.). New York, Boston, London: Back Bay Books.

Quarterman, J. (1989). The Matrix: Computer Networks and Conferencing Systems Worldwide (2 Sub ed.). Digital Press.

Radu, R. (2015). Data Control and digital regulatory space(s): towards a new European approach. *Journal on Internet Regulation*, *4*(2).

Ragin, C. C. (2008). Redesigning Social Inquiry: Fuzzy Sets and Beyond. University Of Chicago Press.

Rainie, L., & Maniam, S. (2016). Americans feel the tensions between privacy and security concerns. *Pew Research Center* http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/.

Rainie, L., Spooner, T., Kalsnes, B. et al. (2001). The dot-com meltdown and the Web. *Pew Internet Tracking Report* http://www.pewinternet.org/2001/11/14/the-dot-com-meltdown-and-the-web/.

Ralph, J. (2013). America's War on Terror: The State of the 9/11 Exception from Bush to Obama (America's War on Terror). Oxford University Press.

RAND. (1964). *Paul Baran and the Origins of the Internet.* RAND Corporation. http://www.rand.org/about/history/baran.html.

Rast, J. (2009). Critical Junctures, Long-Term Processes. *Social science history*, *33*(04), 393-426.

Rear, D. (2013). Laclau and Mouffe's Discourse Theory and Fairclough's Critical Discourse Analysis: An Introduction and Comparison.

Rechtin, E. (1983). *The Technology of Command* (Fall Lecture). Washington D.C.: National Academy Press.

Reich, C. A. (1971). The greening of America. *online.hillsdale.edu* http://online.hillsdale.edu/file/constitution-courses-library/constitution-101/week-9/The-Greening-of-America.pdf.

Rensfeldt, G. (2013). Read the Snowden Documents From the NSA. http://www.svt.se/ug/read-the-snowden-documents-from-the-nsa.

Renshon, S. A. (2009). National Security in the Obama Administration: Reassessing the Bush Doctrine. Routledge.

Reporters without Borders. (2014). *Enemies of the Internet.* https://12mars.rsf.org/wp-content/uploads/EN_RAPPORT_INTERNET_BD.pdf.

Reus-Smit, C. (2007). International Crises of Legitimacy. *International Politics*, *44*(2/3), 157-174.

Reuters. (2000). Y2K Money Well Spent. http://www.everything2000.com/news/computer/y2kmoneywellspent.asp.

RFC Archive. (2016). *Internet RFC Index.* http://www.faqs.org/rfcs/.

Rheingold, H. (1993). *The Virtual Community*.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5-32.

Rid, T. (2013). *Cyber War Will Not Take Place* (1 ed.). Oxford: Oxford University Press.

Rid, T. (2016). Maschinendämmerung: Eine kurze Geschichte der Kybernetik. Propyläen Verlag.

Risen, J. (2006). State of War: The Secret History of the CIA and the Bush Administration. Free Press.

Risen, J., & Lichtblau, E. (2005c). Bush lets US spy on callers without courts. *New York Times*. http://www.ftlcomm.com/ensign/desantisArticles/2006_934/desantis939/wiretap_NYT.pdf.

Risen, J., & Poitras, L. (2013c). NSA gathers data on social connections of US citizens. *The New York Times*. http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?smid=tw-bna&pagewanted=all.

Risen, J., & Poitras, L. (2014c). N.S.A. Collecting Millions of Faces From Web Images. *The New York Times*. http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html?_r=1.

Risse-Kappen, T. (1994). Ideas do not Float Freely: Transnational Coalitions, Domestic Structures, and the End of the Cold War. *International Organization*, *48*(2), 185-214.

Roberts, H., & Palfrey, J. (2010). The EU Data Retention Directive in an Era of Internet Surveillance. In R. Deibert, J. Palfrey, R. Rohozinski et al. (Eds.), *Access Controlled. The Shaping of Power, Rights and Rule in Cyberspace*. Cambridge, London: MIT Press.

Roberts, H., Zuckerman, E., Faris, R. et al. (2011). The Evolving Landscape of Internet Control. A Summary of Our Recent Research and Recommendations. http://cyber.law.harvard.edu/publications/2011/Evolving_Landscape_Internet_Control.

Roberts, L. (1988). The ARPANET and Computer Networks. In G. A. (Ed.), *History of Personal Workstations* (pp. 143-167). ACM Press.

Roland, A., & Shiman, P. (2002). Strategic computing: DARPA and the quest for machine intelligence, 1983-1993. MIT Press.

Rona, T. P. (1976). Weapon Systems and Information War. *Boeing Aerospace Company*.

Rovner, J., & Long, A. (2005). The Perils of Shallow Theory: Intelligence Reform and the 9/11 Commission. *International Journal of Intelligence and CounterIntelligence*, *18*(4), 609-637.

Rueschmeyer, D. (2008). Why and How Ideas Matter. In R. E. Goodin & C. Tilly (Eds.), *The Oxford Handbook of Contextual Political Analysis*. Oxford University Press, USA.

Ruggie, J. G. (1998). Constructing the world polity: essays on international institutionalization (5). Psychology Press.

Rumsfeld, D. (2001). Remarks by the President and Secretary of Defense Donald Rumsfeld Swearing-In Ceremony. *The Oval Office* http://georgewbush-whitehouse.archives.gov/news/releases/20010126-6.html.

Rumsfeld, D. (2002). Transforming the Military. Riding into the Future. *Foreign Policy*, *81*(3), 20-32.

Rundle, M., & Birdling, M. (2008). Filtering and the International System: A Question of Commitment. In R. Deibert, J. Palfrey, R. Rohozinski et al. (Eds.), *Access Denied. The Practice and Policy of Global Internet Filtering*. London: MIT Press.

Russell, R. L. (2007). Sharpening Strategic Intelligence. Why the CIA Gets It Wrong and What Needs to Be Done to Get It Right (Sharpening Strategic Intelligence). Cambridge: Cambridge University Press.

Ryan, J. (2013). A History of the Internet and the Digital Future (Reprint ed.). Reaktion Books.

Saad, L. (1999). Public Concern Over Y2K Computer Glitch Drops As Awareness Grows. http://www.gallup.com/poll/4024/public-concern-over-y2k-computer-glitch-drops-awareness-grows.aspx.

Saalbach, K.-P. (2015). Cyberwar. Grundlagen-Methoden-Beispiele. Universität Osnabrück.

Sabatier, P. A. (2007). *Theories of the Policy Process* (Second Edition, Second Edition ed. Vol. Second Edition). Westview Press.

Sabatier, P. A. (1998). The advocacy coalition framework: revisions and relevance for Europe. *Journal of European Public Policy*, *5*(1), 98-130.

Sabatier, P. A. (1988). An Advocacy Coalition Framework of Policy Change and the Role of Policy-oriented learning therein. *Policy Sciences*, *21*, 129-178.

Sanders, R. (2012). Exceptional Security Practices, Human Rights Abuses, and the Politics of Legal Legitimation in the American "Global War on Terror". University of Toronto.

Sanger, D. E., & Perlroth, N. (2014c). N.S.A. Breached Chinese Servers Seen as Security Threat. *The New York Times*.

Schmidt, A. (2014). Secrecy versus Openness. Internet Security and the limits of Open Source and Peer Production. Uitgeverij BOXPress.

Schmidt, J. F. K. (1997). Der Personal Computer (1974-1985). Architektonische Innovation und vertikale Desintegration. In J. Weyer, U. Kirchner, L. Riedl et al. (Eds.), *Technik, die Gesellschaft schafft. Soziale Netzwerke als Ort der Technikgenese*.

Schmitt, M. N. (Ed.). (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Tallinn: T.

Segeberg, H. (Ed.). (2004). Technik und Krieg. Fragen und Überlegungen zur militärischen Herkunft von Computertechnologien am Beispiel des Internets. Marburg: Schüren Verlag.

Schulze, M. (2012). Die Sprache der (Un-)Sicherheit: Die Konstruktion von Bedrohung im Sicherheitspolitischen Diskurs der Bundesrepublik Deutschland (1., Aufl ed.). Tectum.

Schulze, M. (2015). Patterns of Surveillance Legitimization: The German Discourse on the NSA Scandal. *Surveillance & Society*, *13*(2), 192-217.

Schulze, M. (2016a). (Un-)Sicherheit hinter dem Bildschirm. Die Versicherheitlichung des Internets. In C. Masala & S. Fischer (Eds.), *Innere Sicherheit nach 9/11. Sicherheitsbedrohungen und (immer) neue Sicherheitsmaßnahmen?* (pp. 165-183). Wiesbaden: Springer VL.

Schulze, M. (2016b). Same old story: 40 years of debating encryption. https://tresorit.com/blog/encryption-debate/.

Schulze, M. (2017). Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016. *Media and Communication*, *5*(1).

Schwartau, W. (1997). An Introduction to Information Warfare. In R. L. Pfaltzgraff & R. H. Shultz (Eds.), *War in the Information Age: New Challenges for U S Security (Association of the United States Army)* (pp. 47-60). Washington: Brassey's UK Ltd.

Schwartz, P., Leyden, P., & Hyatt, J. (1999). The Long Boom: A Vision For The Coming Age Of Prosperity (Reprint ed.). Cambridge: Perseus Publishing.

Schwarz, F. A. O. (2008). The Church Committee, then and now. In R. A. Miller (Ed.), US National Security, Intelligence and Democracy: From the Church Committee to the War on Terror (Studies in Intelligence). Routledge.

Scott, W. R. (2008). Institutions and Organizations: Ideas and Interests (3rd ed.). SAGE Publications, Inc.

Seamon, R. H. (2008). NSA domestic surveillance: presidential power and the Fourth Amendment. In R. A. Miller (Ed.), US National Security, Intelligence and Democracy: From the Church Committee to the War on Terror (Studies in Intelligence) (pp. 120-138). Routledge.

Searle, J. R. (1995). The construction of social reality. Simon and Schuster.

Sessions, W. S. (1993). Leaked Letter Briefing Document "Encryption: The Threat, Applications, and Potential Solutions". https://epic.org/crypto/clipper/foia/crypto_threat_2_19_93.html.

Shafqat, N., & Masood, A. (2016). Comparative Analysis of Various National Cyber Security Strategies. *International Journal of Computer Science and Information Security*, *14*(1), 129.

Shah, R. C., & Kesan, J. P. (2007). The privatization of the Internet's backbone network. *Journal of Broadcasting & Electronic Media*, *51*(1), 93-109.

Shapiro, A. L. (2000). The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know (2nd.Printing ed.). PublicAffairs.

Shinal, J. (2005). Netscape: The IPO that launched an era. http://www.marketwatch.com/story/netscape-ipo-ignited-the-boom-taught-some-hard-lessons-20058518550.

Sholle, D. (2002). Disorganizing the "New Technology". In G. Elmer (Ed.), *Critical Perspectives on the Internet* (pp. 3-26). Rowman & Littlefield Publishers.

Shorrock, T. (2009). Spies for Hire: The Secret World of Intelligence Outsourcing (First Edition ed.). New York: Simon & Schuster.

Shubber, K. (2013). A simple guide to GCHQ's internet surveillance programme Tempora. http://www.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101.

Shultz, G. P. (1985). Shaping American Foreign Policy: New Realities and New Ways of Thinking. *Foreign Affairs*. https://www.foreignaffairs.com/articles/1985-03-01/shaping-american-foreign-policy-new-realities-and-new-ways-thinking.

Simon, H. A. (1965). The shape of automation for men and management ([1st ed.] ed.). New York: Harper & Row.

Sin, S., Blackerby, L. A., Asiamah, E. et al. (2016). Determining Extremist Organizations' Likelihood of Conducting Cyberattacks. In N. Pisssandis, H. Roigas, & M. Veenendaal (Eds.), *Cyber Power. 8th International Conference on Cyber Conflict* (pp. 81-98).

Singel, R. (2007). Point, click. eavesdrop: How the FBI wiretap net operates. *Wired*, *28*, 2008.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know (1 ed.). New York: Oxford University Press.

Singer, P. (2017). How America can beat Russia in Cyber War, Despite Trump. *Wired*. https://www.wired.com/2017/01/america-can-beat-russia-cyber-war-despite-trump/.

Slaughter, A.-M. (2009). America's Edge: Power in the Networked Century. *Foreign Affairs*, *January*.

Snow, D. A., & Benford, R. D. (1992). Master Frames and Cycles of Protest. In A. D. Morris & C. M. Mueller (Eds.), *Frontiers in Social Movement Theory* (pp. 133-155). New Haven, London: Yale University Press.

Snow, D. A., Rochford, B. E., Worden, S. K. et al. (1986). Frame Alignment Processes, Micromobilization and Movement Participation. *American Sociological Review*, *51*(4), 464-481.

Stallman, R. (1985). The GNU Manifesto. https://www.gnu.org/gnu/manifesto.en.html.

Starr-Deelen, D. (2014). Presidential Policies on Terrorism: From Ronald Reagan to Barack Obama. Palgrave Macmillan.

Stasi versus NSA. (2017). Wieviel Platz würden die Aktenschränke der Stasi und der NSA verbrauchen - wenn die NSA ihre 5 Zettabytes ausdrucken würde? https://apps.opendatacity.de/stasi-vs-nsa/.

Stebbins, R. A. (2012). Personal Decisions in the Public Square: Beyond Problem Solving into a Positive Sociology (Reprint ed.). Transaction Publishers.

Steele, C., & Stein, A. (2002). Communications Revolutions and International Relations. In J. Emmons Allison (Ed.), *Technology, Development, and Democracy: International Conflict and Cooperation in the Information Age* (pp. 25-53). Albana: State University of New York Press.

Stepanova, E. (2011). The Role of Communication Technologies in the "Arab Spring". Implications beyond the Region. *PONARS Eurasia Policy Memo*, *159*.

Sternstein, A. (2015). The Military's Cybersecurity Budget in 4 Charts. *Defense One* http://www.defenseone.com/business/2015/03/militarys-cybersecurity-budget-4-charts/107679/.

Stevens, G. M. (2003). Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws (RL31730). Congressional Research Service.

STRATCOM. (2010). *U.S. Cybercommand.* https://www.stratcom.mil/factsheets/2/Cyber_Command/.

Strohm, C. (2016). FBI and NSA Poised to Gain New Surveillance Powers under Trump. https://www.bloomberg.com/news/articles/2016-11-29/fbi-and-nsa-poised-to-gain-new-surveillance-powers-under-trump.

Suchman, M. C. (2003). The contract as social artifact. *Law & Society Review*, *37*(1), 91-142.

Sugrue, T. (1994). The Government's Role in the National Information Infrastructure. *Media Law & Policy*.

Surowiecki, J. (2000). The Financial Page of the Visionaries of the New Economy Dream On. http://www.newyorker.com/magazine/2000/05/29/the-financial-page-the-visionaries-of-the-new-economy-dream-on.

Swift, A., & Dugan, A. (2015). ISIS, Terrorism Seen as Graver Threats Than Russia, Ukraine. http://www.gallup.com/poll/181553/isis-terrorism-seen-graver-threats-russia-ukraine.aspx.

Symantec. (2016). *What is a Zero-Day Vulnerability?* http://www.pctools.com/security-news/zero-day-vulnerability/.

Szoldra, P. (2016). ISIS' favorite messaging app may be in jeopardy. *Business Insider* http://www.businessinsider.com/russia-anti-encryption-telegram-2016-6?IR=T.

Takahashi, D. (2016). New York Times columnist Thomas Friedman tells us how to live in accelerated times. http://venturebeat.com/2016/12/07/new-york-times-columnist-thomas-friedman-tells-us-how-to-live-in-accelerated-times/.

Tannenwald, N. (1999). The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use. *International Organization*, *53*(3), 433-468.

Tannenwald, N. (2005). Stigmatizing the Bomb: Origins of the Nuclear Taboo. *International Security*, *29*, 5-49.

Tapscott, D. (1995). The Digital Economy: Promise and Peril in the Age of Networked Intelligence. Mcgraw-Hill Co.
Taylor, R. (1999). An Internet Pioneer Ponders the Next Revolution. https://partners.nytimes.com/library/tech/99/12/biztech/articles/122099outlook-bobb.html.
Taylor, R. (2008). Oral History of Robert (Bob) Taylor. *Woodside, California* http://archive.computerhistory.org/resources/text/Oral_History/Taylor_Robert/102702015.05.01.acc.pdf.
Technopedia. (2015). Internet Backbone. https://www.techopedia.com/definition/20115/internet-backbone.
Technopedia. (2016). Mainframe Computers. https://www.techopedia.com/definition/24356/mainframe.
Intercept, T. (2014). The NSA and GCHQ's QUANTUMTHEORY Hacking Tactics. https://theintercept.com/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/.
The New York Times. (2013). Y2K Bug: Much Ado About Nothing? Retro Report. https://www.youtube.com/watch?v=SoGNiHV09BU.
The New York Times. (2016). *The New York Times Best Sellers.* http://www.nytimes.com/books/best-sellers/?_r=0.
The United States Senate Special Committee on the Year 2000 Technology Problem. (1999). *Investigating the Impact of the Year 2000 Problem.*
The Washington Post. (2003). Timeline: The U.S. Government and Cybersecurity.
The Washington Post. (2013a). *NSA slides explain the PRISM data-collection program.* http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.
The Washington Post. (2013b). *TRANSCRIPT: President Obama's August 9, 2013, news conference at the White House.* https://www.washingtonpost.com/politics/transcript-president-obamas-august-9-2013-news-conference-at-the-white-house/2013/08/09/5a6c21e8-011c-11e3-9a3e-916de805f65d_story.html?utm_term=.1286174cd3a6.
The White House. (1984). National Security Decision Directive Number 145: National Policy on Telecommunications and Automated Information Systems Security.
The White House. (1993a). *Fact Sheet: Public Encryption Management.* https://epic.org/crypto/clipper/white_house_factsheet.html.
The White House. (1993b). *Statement by the Press Secretary.* The White House. Office of the Press Secretary. https://epic.org/crypto/clipper/white_house_statement_4_93.html.
The White House. (1994). Questions and Answers about the Clinton Administation's Encryption Policy. https://epic.org/crypto/clipper/clipper_q_and_a_feb_94.html.
The White House. (1996). *Executive Order 13010 - Critical Infrastructure Protection.* The White House. http://www.presidency.ucsb.edu/ws/?pid=53066.
The White House. (1998a). *PRESIDENTIAL DECISION DIRECTIVE/NSC-63.* https://fas.org/irp/offdocs/pdd/pdd-63.htm.
The White House. (1998b). *Protecting Cyber Security.* http://clinton5.nara.gov/textonly/WH/EOP/NSC/html/nsc-22.html.
The White House. (1999). A National Security Strategy for a New Century.
The White House. (2001a). Executive Order 13228 of October 8, 2001. Establishing the Office of Homeland Security and the Homeland Security Council. The White House.
The White House. (2001b). New Counter-Terrorism and CyberSpace Security Positions announced. The White House. Office of the Press Secretary.
The White House. (2002). The National Security Strategy of the United States of America.
The White House. (2003). A National Strategy to Secure Cyberspace.
The White House. (2006). National Strategy for Combating Terrorism.
The White House. (2007). National Strategy for Information Sharing. Successes and Challenges in Improving Terrorism-Related Information Sharing.
The White House. (2008). National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23. The White House.
The White House. (2011). International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. The White House.
The White House. (2013). Administration White Paper. Bulk Collection of Telephony Metadata under Section 215 of the USA Patriot Act.

Thompson, M., & Waller, D. (1995c). Onward Cyber Soldiers. *Time Magazine*. http://content.time.com/time/magazine/article/0,9171,983318,00.html.

Tiles, M., & Oberdiek, H. (1995). Living in a technological culture: Human tools and human values. Psychology Press.

TIME Magazine. (1983). *The Computer Moves In.* http://content.time.com/time/covers/0,16641,19830103,00.html.

TIME Magazine. (1993). The Info Highway. Bringing a revolution in entertainment, news and communication. http://content.time.com/time/covers/0,16641,19930412,00.html.

TIME Magazine. (1999). *The End of the World!?!* http://content.time.com/time/covers/0,16641,19990118,00.html.

Toffler, A. (1980). *The Third Wave*. New York: William Morrow Company.

Torfing, J. (1999). New theories of discourse: Laclau, Mouffe and Zizek. Blackwell Publishing Ltd.

Torfing, J. (2005). Discourse Theory: Achievements, Arguments, and Challenges. In D. R. Howarth & J. Torfing (Eds.), *European Integration and Security: Analysing French and German Discourses on State, Nation, and Europe* (Vol. Discourse theory in European politics). Palgrave Macmillan Houndsmill, Basingstoke.

Townes, M. (2012). The Spread of TCP/IP: How the Internet Became the Internet. *Millennium - Journal of International Studies*, *41*(1), 43-64.

Tselikov, A. (2014). The Tightening Web of Russian Internet Regulation. *The Berkman Center for Internet & Society Research Publication Series*, *Research Publication No. 2014-15*.

Tsoukala, A. (2008). Defining the terrorist threat in post-September 11 era. In D. Bigo & A. Tsoukala (Eds.), *Terror, Insecurity and Liberty. Illiberal practices of liberal regimes after 9/11*. Abingdon, New York: 49-99.

Tucker, P. (2015). The Best Way To Stick It To Dictators, Help Dissidents, and Boost Privacy. http://www.defenseone.com/technology/2015/07/best-way-to-stick-it-to-dictators-help-dissidents-boost-privacy/117418/.

Turner, F. (2006). From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism.

Turner, K. (2016). Mass surveillance silences minority opinions, according to study. *Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/mass-surveillance-silences-minority-opinions-according-to-study/.

Turner, M. A. (2004). A Distinctive U.S. Intelligence Identity. *International Journal of Intelligence and CounterIntelligence*, *17*(1), 42-61.

U.S. Air Force. (1998). *Information Operations.* U.S. Air Force.

U.S. Census Bureau. (2005). *Computer and Internet Use in the United States: 2003.* U.S. Department of Commerce. Economics and Statistics Administration. https://www.census.gov/prod/2005pubs/p23-208.pdf.

U.S. Congress. (2008). *H.R. 6304 (110th): FISA Amendments Act of 2008.* https://www.govtrack.us/congress/bills/110/hr6304/text.

U.S. Congress. (1991). Computer security: hearing before the Subcommittee on Technology and Competitiveness of the Committee on Science. U.S. House of Representatives, One Hundred Second Congress.

U.S. Congress. (1994). Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services. Subcommittee on Technology and the Law of the Committee on the Judiciary United States Senate.

U.S. Department of Commerce. (1998). *Statement of Policy on the Management of Internet Names and Addresses.* National Telecommunications & Information Administration. https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses.

U.S. Department of Commerce. (2000). *Digital Economy 2000.* ECONOMICS AND STATISTICS ADMINISTRATION Office of Policy Development.

U.S. Department of State. (2013). *Internet Freedom.* http://www.state.gov/e/eb/cip/netfreedom/index.htm.

U.S. Department of the Air Force. (1995). *Cornerstones of Information Warfare.* Department of the Air Force. http://www.csse.monash.edu.au/courseware/cse468/2006/cornerstones-iw.html.

U.S. Senate. (1994). *The administration's clipper chip key escrow encryption program: hearing before the Subcommittee on Technology and the Law of the Committee on the Judiciary United States Senate.* Subcommittee on Technology and the Law of the Committee on the Judiciary United States Senate. https://archive.org/stream/administrationsclip00unit/administrationsclip00unit_djvu.txt.

United Nations General Assembly. (2014a). Resolution adopted by the General Assembly on 18 December 2013. 68/167. The right to privacy in the digital age. United Nations General Assembly.

United Nations General Assembly. (2014b). Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. United Nations.

United Nations General Assembly. (2016). Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development.

Valeriano, B., & Maness, R. C. (2015). Cyber War versus Cyber Realities: Cyber Conflict in the International System. *books.google.com*.

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001-11. *Journal of Peace Research*, *51*(3), 347-360.

Vegh, S. (2002). Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking. *First Monday*, *7*(19).

Venkatesh, A., Chuan-Fong Sih, E., & Stolzoff, N. C. (2000). A Longitudinal Analysis of Computing in The Home Census Data 1984-1997. *Center for Research on Information Technology and Organizations*.

Ventre, D. (2016). *Information warfare*. John Wiley & Sons.

Verbeek, P.-P. (2005). What things do: Philosophical reflections on technology, agency, and design. Penn State Press.

Vinge, V. (2001). True Names: And the Opening of the Cyberspace Frontier (2 ed.). Tor Books.

Vydas, S. (1965). Cyborg: Evolution of the superman. *JAMA*, *194*(4), 474-475.

Walsh, P. F., & Miller, S. (2015). Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden. *Intelligence and National Security*, 1-24.

Waltz, K. N. (1979). Theory of International Politics. McGraw-Hill Higher Education.

Ware, W. H. (1967). Security and Privacy in Computer Systems. *RAND*.

Watson, S. D. (2011). 'Framing' the Copenhagen School: Integrating the Literature on Threat Construction. *Millennium - Journal of International Studies*.

Weber, F. D. (2013). Die Diskurstheorie von Ernesto Laclau und Chantal Mouffe. In *Soziale Stadt - Politique de la Ville - Politische Logiken* (pp. 43-64). Wiesbaden: Springer Fachmedien Wiesbaden.

Weber, M. (1968). Economy and society. *New York: Bedminster*.

Weiss, E. (1996). Creating a new civilization: The politics of the third wave. *Harvard Journal of Law & Technology*, *9*(1).

Weldes, J. (1996). Constructing National Interests. *European Journal of International Relations*, *2*(3), 275-318.

Wellbery, B. S. (1996). Privacy Protection on the Information Superhighway. *Journal of Civil Rights and Economic Development*, *11*(3), 10.

Wellman, B. (2004). The three ages of internet studies: ten, five and zero years ago. *New media & society*.

Wendt, A. (1994). Collective Identity Formation and the International State. *The American Political Science Review*, *88*(2), 384-396.

Wendt, A. E. (1987). The agent-structure problem in international relations theory. *International Organization*, *41*(03), 335.

Westmoreland, W. C. (1969). The electronic Battlefield. *Military Communications: A Test for Technology* http://25thaviation.org/history/id551.htm.

Weyer, J. (2008). Techniksoziologie. Genese, Gestaltung und Steuerung sozio-technischer Systeme. Weinheim, München: Juventa Verlag.

Weyer, J., Kirchner, U., Riedl, L. et al. (1997). Technik, die Gesellschaft schafft. Soziale Netzwerke als Ort der Technikgenese.

Wheeler, D. A., & Larsen, G. N. (2003). Techniques for cyber attack attribution. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859.

Wiegold, T. (2016c). Bundeswehr: ein Update ist verfügbar. *Zeit Online*. http://www.zeit.de/digital/internet/2016-04/bundeswehr-cyberkrieg-it-aufruestung-nachwuchs.
Wiener, A. (2007). Contested Meanings of Norms: A Research Framework. *Comp Eur Polit*, *5*(1), 1-17.
Wiener, A. (2009). Enacting meaning-in-use: qualitative research on norms and international relations. *Rev. Int. Stud.*, *35*(01), 175.
Wiener, N. (1965). Cybernetics, Second Edition: or the Control and Communication in the Animal and the Machine (second edition ed.). The MIT Press.
Wiggins, R. (2000). Al Gore and the creation of the Internet. *First Monday*, *5*(10).
Owens, W. A. (1996). The Emerging U.S. System-of-Systems. *National Defense University Strategic Forum*, *63*.
Williams, B. (1984). Morality, skepticism and the nuclear arms race. In N. Blake & K. Pole (Eds.), *Objections to Nuclear Defence*. London: Routledge.
Williams, M. C. (2011). Securitization and the liberalism of fear. *Security Dialogue*, *42*(4-5), 453-463.
Williams, R., & Edge, D. (1996). The social shaping of technology. *Research Policy*, *25*, 865-899.
Wilson, C. (2006). Information Operations and Cyberwar: Capabilities and Related Policy Issues (RL31787).
Winner, L. (1980). Do artifacts have politics. *Daedalus*, *109*(1), 121-136.
Winner, L. (1993). Social constructivism: Opening the black box and finding it empty. *Science as Culture*, *3*(3), 427-452.
Winner, L. (1997). Cyberlibertarian myths and the prospects for community. *ACM Sigcas Computers and Society* http://dl.acm.org/citation.cfm?id=270864.
Wired. (1993). First Issue. http://archive.wired.com/wired/archive/1.01/.
Wirtz, J. J. (2015). Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. In K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* (pp. 29-37). Tallinn: NATO CCD COE Publications.
Wolff, J. (2016). What we talk about when we talk about cybersecurity: security in internet governance debates. *Internet Policy Review*, *5*(3).
Wong, W. H., & Brown, P. A. (2013). E-Bandits in Global Activism: WikiLeaks, Anonymous, and the Politics of No One. *Perspectives in Politics*, *11*(04), 1015-1033.
Woolgar, S. (1991). The Turn to Technology in Social Studies of Science. *Science, Technology & Human Values*, *16*(1), 20-50.
Woollacott, E. (2016). UK joins Russia and China in legalizing Bulk Surveillance. *Forbes*. http://www.forbes.com/sites/emmawoollacott/2016/11/16/uk-joins-russia-and-china-in-legalizing-bulk-surveillance/#37d08afa65f4.
WorldBank. (2016a). *World Development Indicators.* http://data.worldbank.org/data-catalog/world-development-indicators.
WorldBank. (2016b). *Internet users (per 100 people).* http://data.worldbank.org/indicator/IT.NET.USER.P2.
Zittrain, J., & Palfrey, J. (2008). Internet Filtering: The Politics and Mechanisms of Control. In R. Deibert (Ed.), *Access Denied: The Practice of Global Internet Filtering* (pp. 29-56). MIT Press.
Zittrain, J. L. (2006). The generative Internet. *Harvard Law Review*, 1974-2040.
Zuckerman, E. (2010a). Internet Freedom: Beyond Circumvention. http://www.ethanzuckerman.com/blog/2010/02/22/internet-freedom-beyond-circumvention/.
Zuckerman, E. (2010b). Intermediary Censorship. In R. Deibert, J. Palfrey, R. Rohozinski et al. (Eds.), *Access Controlled. The Shaping of Power, Rights and Rule in Cyberspace*. Cambridge, London: MIT Press.

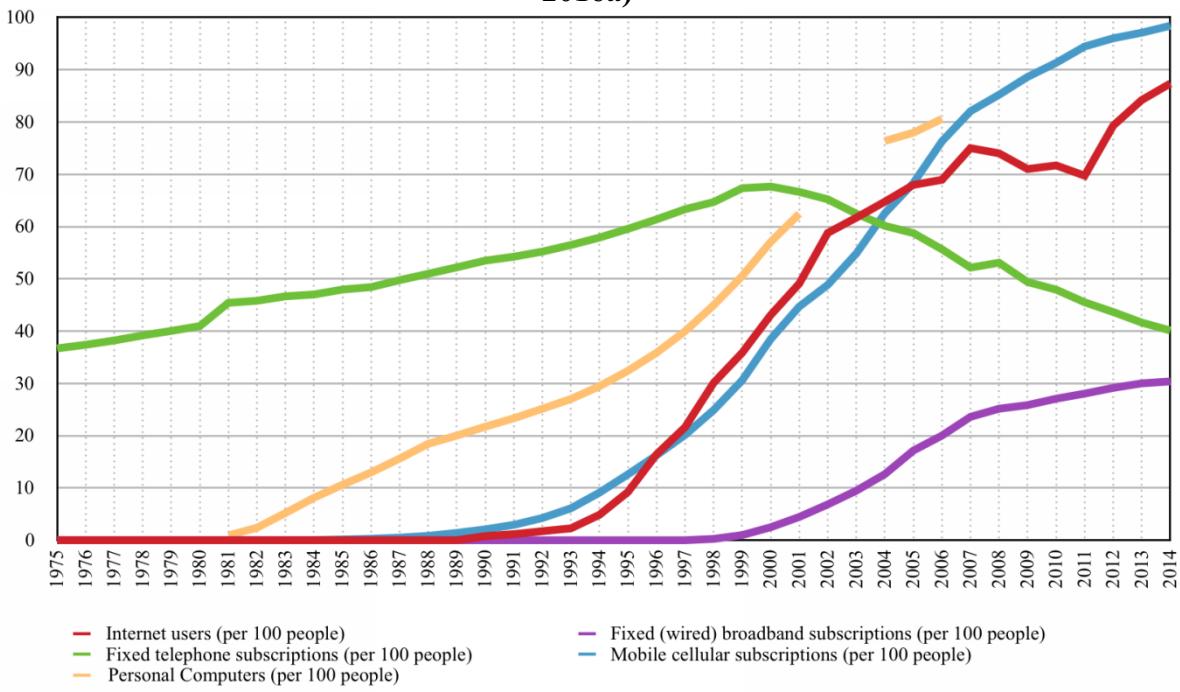
All Internet Sources have been accessed and checked for availability on 02.03.2017.

Appendix

Quantifying the Internet and the Digital Revolution

This appendix provides some basic statistics that shed light on the evolution of the Internet and its growth. It includes dominant usage and users and is therefore a precondition for understanding many current topics such as the prevalence of cyber-security or the Big-Data hype.

Figure 33. Diffusion of ICT in the USA between 1975-2015, Source: (WorldBank, 2016a)



The graphic shows the diffusion of Internet users, broadband subscriptions, telephone subscriptions and personal computers per 100 people in the U.S.. The data was obtained from the WorldBank Development indicators, which did not include data for PC usage between the years 2002-2004 and since 2006. Nevertheless, the early growth period is covered. Since the U.S. is the home market of these technologies, no other country shows similar growth rates at the respective points in time.

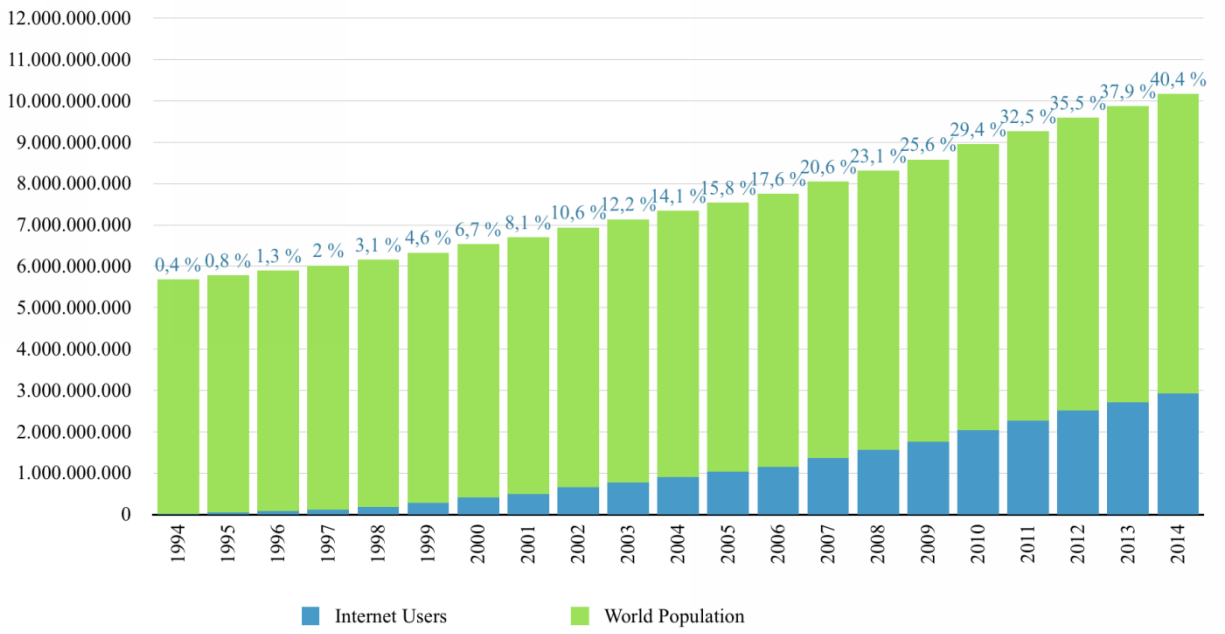
To qualify this growth, some additional information from the US Department of Commerce Census Bureau is included (U.S. Census Bureau, 2005). In early 1984, the technology users were mostly white (8,6%), had a middle-class income of $30-50000 per year (15,2%) or were families with high education (college degree 12,8%, graduate degree 18,3%) and no children (14,1%). These users represented the majority until 1997 (Venkatesh, Chuan-Fong Sih, & Stolzoff, 2000, p. 207). In terms of gender equality,

computers in the early days tended to be male-dominated (64,8% male) but over time the gender-gap disappeared (Venkatesh et al., 2000). What were computers used for? In 1984 the largest proportion was "learning to use a computer", directly followed by "video games". In 1989, as computers spread through business, the most common task became "word-processing", followed by "games". The user demographic in the early days is quite narrow: white, young males with high education predominantly using the computer for games. This most likely corresponds with the early users of the ARPANET during the 1970s, although demographic data is missing in this case.

The period between 1994 and 1997 is described as a "watershed transition" during which computer and Internet uses across all demographic criteria shifted dramatically (Venkatesh et al., 2000, p. 215). This is attributed to the introduction of the Internet which also transforms the dominant use of computer as work or game-stations to communication technologies. Elton and Carey (Elton & Carey, 2013) argue that the inventor's dilemma, the chicken-egg problem, was effectively circumvented because the PC was popular enough to provide a first user base, who benefited from new Internet services and who e-mailing and surfing the web as dominant activities. The Internet's decentrality and openness enabled new usage scenarios, because there was no central regulation instance that prevented services (for example because of copyright reasons) such as "e-commerce" and "online-shopping". The victory of the Internet is indicated by the decline of traditional land-line phone connections since 2000. What is remarkable about this growth in the early days is that, the percentage of Internet users in the U.S. almost doubles in each following year (1993 2,2%; 1994 4,8%; 1995 9,2%; 1996 16,4%; 1997 21,6%). The 50% mark was reached in 2001 (WorldBank, 2016a)

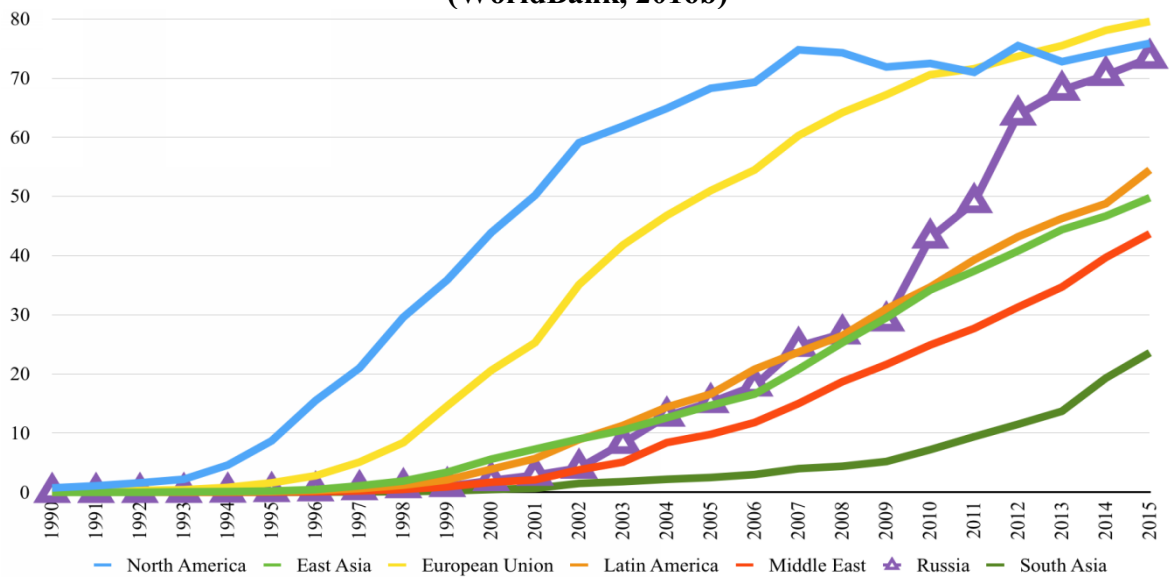
Globally, the Internet diffusion is a bit slower, showing a clear gab between so called first, second and third worlds, as the following graph shows.

Figure 34. Percentage of Internet Users of the World Population, Source: (Internet Live Stats, 2016)



With the new millennium, only 6.7% of the world population had access to the Internet. In 2007 the smartphone revolution began with the introduction of the Apple iPhone, expanding the user base of the Internet to a wider demographic. Around 20,6% of the world population had Internet access then, growing steadily to around 40% in 2014.

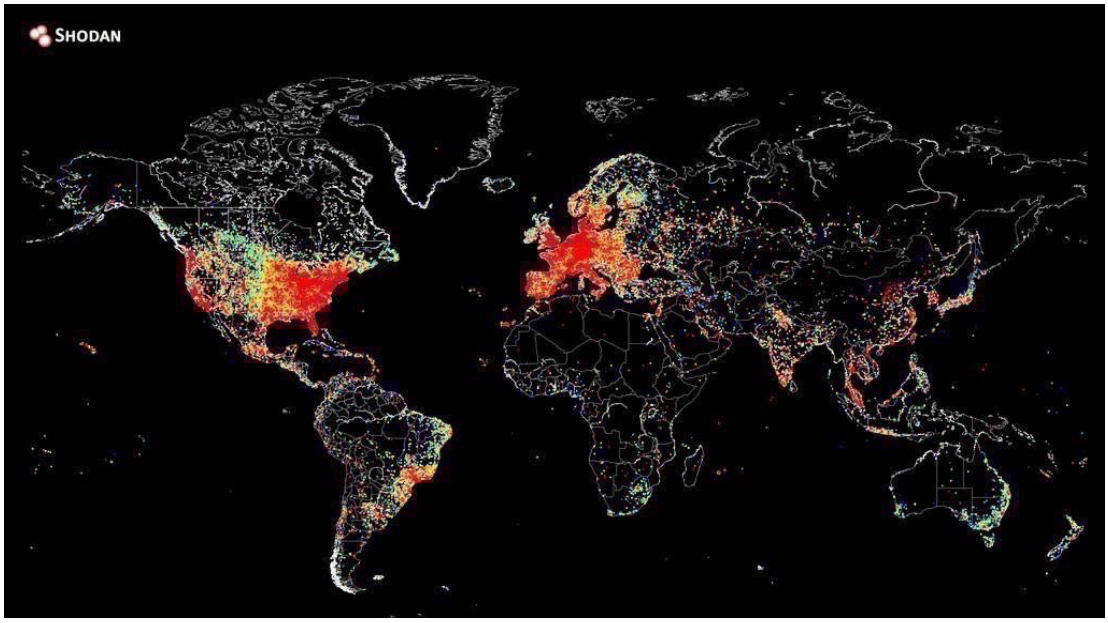
Figure 35. Longitudinal Internet Diffusion per Region in percent, Source: (WorldBank, 2016b)



This graph shows the distribution by region based on the World Bank Development Indicators (WorldBank, 2016b). The developed world (OECD, North America, EU) were the first movers, reaching an Internet penetration of 50% and more between 2000 and 2005.

Other industrial countries like China and the Russian Federation reached this threshold between 2011 (Russia) and 2014 (China). What becomes clear is that within the next ten years, the global Internet population will grow reaching a similar Internet penetration like the OECD countries (around 80% of the population)[180]. Studies suggest that the early adopters of a new technology tend to be the younger, wealthy, educated (and technologically savvy) progressive users, while older (Linchuan Qiu, 2013). Older people and technical conservative users more often adopt a "wait and see approach" or ignore new technologies in general. Users from poorer regions of the world simply lack access because of costs or lacking availability of infrastructure. This pattern is called "digital divide" (Prensky, 2001) and can be found not just with the diffusion of the Internet during the 1990s, but also with newer technologies (such as Smartphones or Social Media Services of the mid 2000s).

Figure 36. Internet Devices per Region, Source: (Engel, 2014)



This graph shows the physical topology of the Internet, based on the geolocation of devices connected to the Internet as of 2014. It clearly It shows that the global village is highly biased towards major cities and industrial centers of the world, creating a large digital gap towards the country side and remote regions of the Earth (Siberia, Africa, Australia). The same is true for the basic physical infrastructure that carries the global Internet traffic. The major IXP that are the largest switching locations that interconnect the different regional subnetworks are also biased towards western countries. Most of these

[180] The very young and the very old seldom connect to the Internet, which might explain the lacking 20%.

IXP located in OECD countries handle the majority of Internet traffic (Chatzis et al., 2013). This means that most of the data packets are routed through the West.

Table 9. List of Internet Milestones and Security Incidents

Date	Internet Milestone	Noteworthy Security Incident
1957	- ARPA founded	
1964	- Paul Baran writes "On Distributed Communications Networks"	
1966	- ARPANET Project begins	
1967		- Willis Ware warns Lawrence Roberts of network security issues
1968	- Whole Earth Catalog launches	
1969	- ARPANET Prototype running	
1971	- Ray Tomlinson presentes E-Mail	- Blue Box phone phreaking hits the news
1972	- ARPANET public presentation	
1972	- Begin of Internetworking project	
1974	- TCP proposed by Cerf and Kahn	
1975	- Altair 8800 & Apple 1 initiate PC revolution	
1977	- First successful TCP networking test	
1979	- TCP/IP becomes DoD standard	
1980	- BSD includes TCP/IP	
1981		- AT&T hacked, Captain Zap changes billing rates to get late-night discounts
1983	- ARPANET transition to TCP/IP	- Hackers break into Los Alamos National Laboratory and make news headlines. First hearings on computer security in the house of representatives follow - War Games released
1984	- The WELL launches - Gibson coins Cyberspace in Neuromancer	
1986	- NSFNET launches	
1988	- NSFNET Internet backbone	- First self-replicating worm

Table 9. List of Internet Milestones and Security Incidents

	transition from ARPANET	(Morris') spreads through ARPANET, causes $10 million damage
1989	- Berners-Lee proposes WWW	- Malicous Computer Worm found in NASA Computer "Worms Against Nuclear Killers"
1990	- ARPANET is decommissioned - Electronic Frontier Foundation founded	
1991	- First Website, release of HTML	
1993	- Mosaic Web Browser - Information Superhighway - Windows 3.1 released	- NSA developed plans for CNA against Haiti Radar Systems
1994	- Amazon founded - Yahoo founded - Netscape Navigator and SSL Encryption - www.whitehouse.gov launch	- Intension into Rome Laboratory at Griffith Air Force Base
1995	- First item sold on ebay.com - Windows 95 released - first online banking with Wells Fargo - Internet is privatized - Netscape Initial Public Offering initiates dot-com frenzy	- China and Russia begin to emulate US information war doctrine
1996	- 15 % of Americans are Online - Barlow publishes Declaration of Independence of Cyberspace	- First documented phishing & DDoS attacks
1997	- WIFI invented - AOL messenger released	- NSA conducts Eligible Receiver Simulation, uncovers network vulnerabilities
1998	- Google founded - Bill Clinton's first Email - ICANN takes over Internet stewardship	- Solar Sunrise, 18 year old hacker penetrates DoD Servers - Moonlight Maze attack, military maps and troop configurations stolen from Pentagon, Russian origin - Hacking during Kosovo War
1999	- Napster launches	- Y2K Panic
2000	- .com bubble bursts - Blogger launches	- ILOVEYOUVIRUS infects millions PCs and causes $15 billion financial damage.
2001	- Wikipedia created - 50% of Americans are online	- 9/11

Table 9. List of Internet Milestones and Security Incidents

2002	- TOR launches	
2003	- Apple iTunes Store launch - Piratebay launch - Myspace launch	- Begin of Titan Rain attacks (massive data extraction from US government), F-35 Fighter schematics stolen
2004	- Facebook founded, global launch 2007 - World of Warcraft launched	
2006	- Google buys Youtube	
2007	- iPhone & Google Android released, begin of smartphone revolution - Dropbox founded, start of Cloud computing - Twitter global launch - Begin of Big Data with Hadoop - IBM releases Watson AI	- Aurora Generator tests physical destruction of a generator by a CNA - Estonia DDoS Attacks - Operation Orchard in Syria (disrupting Syrian Radar with CNA) - CNA against Iraqi insurgents
2008	- HTML5 introduced - Google Android released - First Presidential Tweet by Candidate Obama	- Hybrid Warfare in Georgia - Republican and Democrat election campaign data stolen by CNE - Agent.btz penetrates classified and air-gapped DoD Networks - Conficker infects 11 million hosts, causing $9.1 billion financial damage
2009	- Cloud Computing Hype - WhatsApp messenger released - electronic currency Bitcoin launches	- Iraqi insurgents hack into UAV drones
2010		- Stuxnet discovered - US Cybercommand opens
2011	- Arab Spring - Wikileaks Cables - Smartphones overtake PC as dominant Internet device	- First Sony PSN hack, affects 77 million gamer accounts, $171 million outage costs - Anonymous launches operation payback on VISA, Paypal as a result of Wikileaks affair - Pentagon hacked, 24000 files stolen by unknown intruders - Creech Air Force based hacked, Predator drones infected by malware - 2 US GPS satellites hacked
2013	- Snowden Leaks	- Patriot Missile System, and Navy's Aegis defense system hacked - Department of Energy employee data (security numbers, payroll) stolen

Table 9. List of Internet Milestones and Security Incidents

2014	- 88% of Americans are online	- Federal Employee Database at OPM hacked, millions security clearances stolen - Heartbleed vulnerability discovered, affected millions of Internet services - White House advisors hacked - Sony hacked by Korean Hackers after release of 'The Interview' film

This table gives a more detailed overview over computer security events such as network breaches or digital espionage. This list was compiled while screening computer security books and articles. I included those events that either where the "first" of some kind (for example using a new attack vector), or that were regarded as historically important by different authors or the media (for example events generating enormous costs). Because of space limitations it is not complete.

Polls on the Dominance of Cyber-Realism

The purpose of this appendix is to provide different statistics and polls on the dominance of cyber-utopian and realist ideas.

Table 10. Pew Research Surveys - % Saying each is a major threat to the U.S.

	2016[181]	**2013**[182]	**2009**[183]	**2008**[184]	**2005**[185]
Islamic extremist groups like al Qaeda, ISIS	80	75	-	72	-
Cyberattacks from other countries	**72**	**70**	-	-	-
Global Economic Instability	67	-	-	-	-
Iran's nuclear program	-	68	72	60	61
North Korea's nuclear program	-	67	69	55	66
spread of infectious diseases	60	-	-	-	-
Refugees from fragile states	55	-	-	-	-
climate change	53	45	44	-	-
China's emergence as world power	50	54	53	48	52
tensions with Russia	42	-	-	44	-
Economic Problems in EU	-	37	-		-
Pakistan's political instability	-	-	-	43	-

This data was compiled using different, representative Pew telephone surveys conducted in the respective years. The participants were given a list of threats and they had to select the top problems facing the world each year.

[181] (Pew Research Center, 2016)
[182] (Pew Research Center, 2013)
[183] (Pew Research Center, 2013)
[184] (Pew Research Center, 2008)
[185] (Pew Research Center, 2013)

Table 11.Gallup Poll - Percentage of people who see an issue as a critical threat to the U.S.

	2016[186]	**2015**[187]	**2013**[188]	**2010**[189]	**2004**[190]
International Terrorism	79	84	81	81	82
Development of nuclear weapons by Iran	75	77	83	-	-
Cyberterrorism, the use of computers top cause disruption or fear in society	**73**	-	-	-	-
The spread of infectious diseases	63	-	-	-	-
The conflict in Syria	58	-	-	-	-
The military power of North Korea	58	64	-	-	-
Development of nuclear weapons by North Korea	-	-	83	-	-
Large numbers of refugees trying to come to Europe and North America	52	-	-	-	-
Global warming or climate change	50	-	-	-	-
The conflict between Israeli and the Palestenians	45	49	44	47	58
The military power of China	41	-	51	46	39
The economic power of China	41	40	52	-	-
The military power of Russia	39	49	29	23	18

[186] (McCarthy, 2016)
[187] (Swift & Dugan, 2015)
[188] (Jones, 2013)
[189] (Jones, 2010)
[190] (Jones, 2010)

The conflict between Russia and Ukraine	-	44	-	-	-
The conflict between India and Pakistan	-	-	25	23	18

National security threat perceptions depend on daily political events which explains why some indicators are present at different points in time. Additionally, the polling agencies used different questions over time which is why the China indicators are divided between military power and economic power.

Table 12. Internet Society Survey 2011, Source: (Internet Society, 2011)

15. Has the Internet reached its full potential, or will it become even more important in the future?	**Global (%)**	**US (%)**	**Russia (%)**
The Internet will be even more important in the future	95	94	98
The Internet has already reached its full potential	5	6	2
16. Please choose the top 3 areas in which you believe the Internet currently plays an important role.			
Social engagement (e.g. connecting with friends/family)	60	64	81
Education (e.g. online courses)	47	57	41
Communication efficiency (e.g. collaboration)	45	44	44
Entertainment (e.g. music, art)	45	43	55
Global commerce/global economic development	27	21	18
Access to information about governance (e.g. making sure citizens get information needed to keep governments accountable)	26	31	30
Scientific endeavors (e.g.	18	20	11

medical research)			
National commerce/national economic development	13	12	9
Other (SPECIFY)	1	0	1
None—The internet currently does not play an important role	0	1	0
19. What is the biggest concern facing the Internet today?			
User privacy	26	30	13
Spam and other unwanted traffic	23	21	39
Security of Internet infrastructure	20	26	18
Copyright and intellectual property issues	8	2	10
Government control	8	12	8
Lack of Internet access	6	2	6
Net neutrality (the idea that companies providing Internet service should not give preferential treatment to some websites, or content providers, over others)	5	5	2
Usability by multiple languages	3	0	2
Nothing	1	1	2
16. Please choose the top 3 areas in which you believe the Internet currently plays an important role.			
Social engagement (e.g. connecting with friends/family)	60	64	81
Education (e.g. online courses)	47	57	41
Communication efficiency (e.g. collaboration)	45	44	44
Entertainment (e.g. music, art)	45	43	55
Global commerce/global economic development	27	21	18
Access to information about governance (e.g. making sure citizens get information needed to keep governments	26	31	30

accountable)			
Scientific endeavors (e.g. medical research)	18	20	11
National commerce/national economic development	13	12	9
Other (SPECIFY)	1	0	1
None—The internet currently does not play an important role	0	1	0
19. What is the biggest concern facing the Internet today?			
User privacy	26	30	13
Spam and other unwanted traffic	23	21	39
Security of Internet infrastructure	20	26	18
Copyright and intellectual property issues	8	2	10
Government control	8	12	8
Lack of Internet access	6	2	6
Net neutrality (the idea that companies providing Internet service should not give preferential treatment to some websites, or content providers, over others)	5	5	2
Usability by multiple languages	3	0	2
Nothing	1	1	2
20. There should be no restrictions on accessing lawful content via the Internet.			
Agree strongly	44	40	63
Agree somewhat	36	33	28
Disagree somewhat	14	18	7
Disagree strongly	6	9	2
21. There should be no restrictions on lawful software or services on the Internet.			
Agree strongly	41	32	64
Agree somewhat	37	34	26
Disagree somewhat	16	24	8
Disagree strongly	6	10	2
23. The ability to share and access information privately using the Internet is important to me.			
Agree strongly	57	59	41

Agree somewhat	35	35	40
Disagree somewhat	6	4	14
Disagree strongly	2	1	5
24. The Internet needs to be controlled to protect end-users.			
Agree strongly	42	24	34
Agree somewhat	39	40	41
Disagree somewhat	13	24	16
Disagree strongly	6	12	9
25. The Internet needs to remain as uncontrolled as possible to promote innovation.			
Agree strongly	21	24	21
Agree somewhat	34	34	33
Disagree somewhat	30	29	30
Disagree strongly	15	13	15
58. How concerned are you that Internet Service Providers are monitoring your use of the Internet?			
Very concerned	29	31	20
Somewhat concerned	43	43	31
Not very concerned	22	21	34
Not concerned at all	6	5	16
64. How concerned are you that the Government is monitoring your use of the Internet?			
Very concerned	37	46	36
Somewhat concerned	36	32	30
Not very concerned	21	17	23
Not concerned at all	7	5	11
Source: Internet Society, 2011			

This table presents the findings of the Internet Societies 2011 global Internet survey with over 6000 online participants worldwide and 1001 in the U.S.. A downsides of this survey are that there is no longitudinal measurement and that only online participants were asked, which reduces representativity. For this overview, I only selected these items that came close to the identified cyber-utopian and realist ideas and frames discovered in this thesis. I also chose to include two comparable cases, the global average and Russia, a more authoritarian democracy. In theory, we should expect stronger support for Internet control in Russia, however this is not always the case.

Table 13. 2016 Presidential Candidates' Opinion on Cyber-Realist Ideas

	Donald Trump (Rep)	Hillary Clinton (Dem)	Jill Stein (Green)	Gary Johnson (Lib)	American Voters
Do you support the Patriot Act?	Yes	Yes	No, and pass strict laws prohibiting any government surveillance	No, and pass strict laws prohibiting any government surveillance	Yes 55% / No 45%
Should the NSA be allowed to collect basic metadata of citizen's phone calls such as numbers, timestamps, and call durations?	Yes, basic data collection is necessary to track suspected terrorists	No	No, only with a warrant showing probable cause of criminal activity	No, only with a warrant showing probable cause of criminal activity	Yes 31% / No 69%
Should the U.S. government grant immunity to Edward Snowden?	No, he should be returned to the U.S. to stand trial and face the consequences of his actions	No, he should be returned to the U.S. to stand trial and face the consequences of his actions	Yes, he should be protected under the Whistleblower Protection Act	Yes, he should be protected under the Whistleblower Protection Act	Yes 48% / No 52%
Should Apple unlock the iPhones of suspected terrorists for the FBI?	Yes, but only in situations where the owner is a proven threat to national security	Yes, but only in situations where the owner is a proven threat to national security	No, backdoors can expose innocent owners to malicious hackers	No	Yes 53% / No 47%
Should the U.S. continue NSA surveillance of its allies?	Yes, surveillance of all foreign countries is essential to tracking potential terrorist threats	No	No, spying on our allies severely damages our reputation abroad	No, and abolish the NSA	Yes 52% / No 48%
Should internet service providers be allowed to speed up access to popular websites (that pay higher rates) at the expense of slowing down access to less popular websites (that pay lower	Yes	No, treat all traffic equally and continue the openness of the Internet	No, treat all traffic equally and continue the openness of the Internet	Yes	Yes 17% / No 83%

Table 13. 2016 Presidential Candidates' Opinion on Cyber-Realist Ideas

rates)?					
(ISideWith.com , 18.01.2016)					

This table presents the summarized position of each presidential candidate before the 2016 election and contrasts it with an online poll that Isidewith.com conducted on its website. Although each item received millions of votes, the downside of this methodology is it is online only and the participants could answer multiple times. As such, the public's position is not quite representative. I have selected only these items that addressed topics of this thesis.

Table 14. Intelligence Community Directors

<table>
<tr><th></th><th>FBI</th><th>CIA</th><th>DCI/DNI</th><th>DHS</th><th>NSA</th><th>CYBERCOM</th></tr>
<tr><td>1990</td><td rowspan="3">William S. Sessions November 1987 – July 1993</td><td>William Hedgcock Webster May 1987 – August 1991</td><td>William Hedgcock Webster May 1987 – August 1991</td><td rowspan="12"></td><td rowspan="2">William O. Studeman August 1988 – May 1992</td><td rowspan="12"></td></tr>
<tr><td>1991</td><td colspan="2" rowspan="2">Robert Michael Gates November 1991 – January 1993</td></tr>
<tr><td>1992</td><td rowspan="3">J. Michael McConnell May 1992 – February 1996</td></tr>
<tr><td>1993</td><td>Floyd I. Clarke (acting), July 1993 – September 1993</td><td colspan="2" rowspan="2">R. James Woolsey February 1993–January 1995</td></tr>
<tr><td>1994</td><td rowspan="6">Louis J. Freeh September 1993 – June 2001</td></tr>
<tr><td>1995</td><td colspan="2">John Mark Deutch May 1995–December 1996</td><td rowspan="3">Kenneth A. Minihan February 1996 –</td></tr>
<tr><td>1996</td><td colspan="2" rowspan="5">George John Tenet July 1997–July 2004</td></tr>
<tr><td>1997</td></tr>
<tr><td>1998</td><td rowspan="4">Michael V. Hayden March 1999 – 2005</td></tr>
<tr><td>1999</td></tr>
<tr><td>2000</td></tr>
<tr><td>2001</td><td>Thomas J. Pickard (acting), June 2001 – September 2001</td></tr>
<tr><td>2002</td><td rowspan="5">Robert S. Mueller III September 2001 – September 2013</td><td rowspan="3">Porter J. Goss September 2004 – May 2006</td><td rowspan="2">Porter J. Goss September, 2004–April 2005</td><td rowspan="3">Tom Ridge January 2003 – February 2005</td></tr>
<tr><td>2003</td></tr>
<tr><td>2004</td></tr>
<tr><td>2005</td><td rowspan="3">John Negroponte April 2005 – February 2007</td><td rowspan="4">Michael Chertoff February 2005 – January 2009</td><td rowspan="4">Keith B. Alexander August 2005 –April 2014</td></tr>
<tr><td>2006</td><td rowspan="3">Michael V. Hayden May 2006 – February 2009</td></tr>
<tr><td>2007</td><td>John Michael</td></tr>
</table>

Table 14. Intelligence Community Directors

2008			**McConnell** February 2007 – January 2009			
2009		**Leon E. Panetta** February 2009 – July 2011	**Dennis C. Blair** January 2009 – May 2010	**Janet Napolitano** January 2009 – September 2013		
2010			**David C. Gompert** May 2010 – August 2010			
2011		**Michael J. Morell** July 2011 – September 2011	**James R. Clapper** August 2010 – present			**Keith B. Alexander** May 2010 – March 2014
		David H. Petraeus September 2011 – November 2012				
2012		**Michael J. Morell** November 2012 – March 2013				
2013	**James B. Comey** September 2013 – present	**John O. Brennan** March 2013 – present		**Jeh Johnson** December 2013 – present	**Michael S. Rogers** April 2014 – present	**Jon M. Davies (acting)** March 2014 – April 2014
2014						
2015						**Michael S. Rogers** April 2014 – present
Source	https://www.fbi.gov/about–us/history/directors	https://en.wikipedia.org/wiki/Director_of_the_Central_Intelligence_Agency	https://www.cia.gov/news–information/featured–story–archive/2008–featured–story–archive/directors–of–central–	http://www.dhs.gov/secretaries–homeland–security	https://www.nsa.gov/about/leadership/former_directors.shtml	

Table 14. Intelligence Community Directors

			intelligence.html (bis 2004)			

Corpora

These sources were identified by using the snowball technique. I screened secondary sources for key political documents and worked backwards in time. Then I analyzed these documents for their most reoccurring themes, ideas (problem definitions, goals, instruments) and norms. I inductively build codes for reappearing concepts and marked them in MaxQDA. Afterwards I deductively applied these codes to the rest of the material. I stopped this process after nothing new was found. These documents focus on much more than the Internet so I chose to limit myself on the Internet and Cyberspace, ignoring for example Drone technology. Afterwards I screened White House documents such as policy directives or national security strategies for the appearances of the identified code to infer, whether there was an idea spillover. The corpus surely is not complete but it provided a large enough overview to grasp the most important elements. Note that not all of these texts necessary appear as quotes or citation in the text. I used only the most illustrative quotes as representatives for certain codings.

Engineering Corpus

Corpus of Engineering Texts

Source (chronological)	Type of Document
Bush, V. (1945). As we may think. The atlantic monthly, 176(1), 101-108.	media publication
Kleinrock, L. (1961). *Information Flow in Large Communication Nets.*	academic publication
Center, D. S. R. (Ed.). (1990[1962]). *In Memoriam: J. C. R. Licklider 1915-1990*.	academic publication
Baran, P. (1964). *On distributed communications. I. Introduction to Distributed Communication Networks*. Proceedings from Prepared for Unites States Air Force Project RAND, Santa Monica.	academic publication
RAND. (1964). Paul Baran and the Origins of the Internet. http://www.rand.org/about/history/baran.html.	academic publication
Davies, D. W. (1965). *Proposal for the Development of a National Communications Service for On-Line Data Processing*.	academic publication
Roberts, L. (1967). Multiple Computer Networks and Intercomputer communication. *67 Proceedings of the first ACM symposium on Operating System Principles*.	academic publication
Ware, W. H. (1967). Security and Privacy in Computer Systems. *RAND*.	academic publication
Electronics (1972c). Demonstration Heralds Next Wave: Connecting a Network of Networks. *Electronics*, pp. 34-36.	media publication
McKenzie, A. (1972). *Host/Host Protocol for the ARPA Network*. Proceedings from Prepared for the Network Working Group by BBN.	academic publication
Cerf, V. G., & Kahn, R. E. (1974). A protocol for packet network intercommunication. *IEEE*, *22*(5).	academic publication
Baran, P., & Farber, D. (1977). The Convergence of Computing and Telecommunications Systems. *Science*, *Vol.195*, 1166-1170.	academic publication
Cohen, D. (1978). *On Interconnection of Computer Networks*. Proceedings from Proceedings of Interlinkining of Computer Networks., Bonas.	academic publication
Cerf, V. (1979). DARPA Activities in Packet-Network Interconnection. The military requirement for Network Interconnection Technology. *U.S. Department of Defense, Advanced Research Projects Agency*.	academic publication
Haughney, J. (1980). ARPANET News from DCA. *ARPANET Newsletter*.	newsletter
Heart, F., McKenzie, A., McQuillan, J., Walden, D., McCarthy, J. D., & Zald, M. N. (1981). Completion	report

Report No. 4799. A History of the ARPANET. The first decade.	
Denning, P. J., Hearn, A., & Kern, W. C. (1983). *History and Overview of CSNET*. Proceedings from CSNET Project at the ACM SIGCOMM symposium on data communications, March 8-9, 1983.	academic publication
Davies, D. (1986). An Interview with Donald W. Davies. *National Physical Laboratory*, *Charles Babbage Institute, University of Minnesota, Minneapolis, Minnesota*.	interview
Lukasik, S. (1987). Oral History Transcript — Dr. Stephen Lukasik. *Santa Monica, CA*, *American Institue of Physics*.	interview
Licklider, J. C. R. (1988). An Interview with J.C.R. Licklider, Oral History 150. Cambridge, M.A. *Charles Babbage Institute. The Center for the History of InformationProcessing University of Minnesota, Minneapolis*.	interview
Ruina, J. (1989). An Interview with Jack P. Ruina OH 163. Cambridge. M.A.*, Charles Babbage Institute. The Center for the History of InformationProcessing University of Minnesota, Minneapolis.*	interview
Roberts, L. G. (1989). An Interview with LAWRENCE G. ROBERTS OH 159. San Mateo, CA. *Charles Babbage Institute. The Center for the History of InformationProcessing University of Minnesota, Minneapolis.*	interview
Taylor, R. (1989). An Interview with Robert Taylor OH 154. Palo Alto. *Charles Babbage Institute. The Center for the History of InformationProcessing University of Minnesota, Minneapolis*.	interview
Berners-Lee, T. (1989). Information Management: A Proposal. *CERN*.	academic publication
Quarterman, J. (1989). *The Matrix: Computer Networks and Conferencing Systems Worldwide* (2 Sub ed.). Digital Press.	academic publication
Heart, F. (1990). An Interview with Frank Heart. Cambridge, M.A., *Charles Babbage Institute. The Center for the History of InformationProcessing University of Minnesota, Minneapolis.*	interview
Kleinrock, L. (1990). An Interview with LEONARD KLEINROCK OH 190. Los Angeles, *Charles Babbage Institute. The Center for the History of InformationProcessing University of Minnesota, Minneapolis.*	interview
Cerf, V. G. (1990). An Interview with VINTON CERF OH 191. Reston, VA, *Charles Babbage Institute. The Center for the History of InformationProcessing University of Minnesota, Minneapolis.*	interview
Berners-Lee, T., & Cailliau, R. (1990).	academic publication

WorldWideWeb: Proposal for a HyperText Project. *CERN*.	
Lukasik, S. (1991). An Interview with Stephen Lukasik OG 232. Redondo Beach, *Charles Babbage Institute. The Center for the History of InformationProcessing University of Minnesota, Minneapolis.*	interview
Clark, D. D. (1992). *A Cloudy Crystal Ball – Visions of the Future*. Proceedings from Presentation given at the 24th Internet Engineering Task Force.	academic publication
Networks, M. (1995). NSFNET: A Partnership for High-Speed Networking. Final Report 1987-1955.	report
Engineering, N. A. O. (Ed.). (1995). *Revolution in the U.S. Information Infrastructure*. Washington: National Academy Press.	academic publication
Kahn, R. E. (1995). The Role of Government in the Evolution of the Internet. In N. A. O. Engineering (Ed.), *Revolution in the U.S. Information Infrastructure*. Washington D.C.: National Academy Press.	academic publication
Isenberg, D. (1997). Rise of the Stupid Network. *Computer Telephony*, 16-26.	academic publication
Hafner, K., & Lyon, M. (1998). *Where Wizards Stay Up Late: The Origins Of The Internet* (First Paperback Edition ed.). Simon & Schuster.	academic publication
Naughton, J. (1999). *A brief history of the future. The origins of the Internet.* Weidenfeld & Nicolson.	academic publication
Taylor, R. (1999). An Internet Pioneer Ponders the Next Revolution. *Outlook 2000.*	interview
Cerf, V. (2000). Internet Society Panel on Business Method Patents.	media publication
Abbate, J. (2000). *Inventing the Internet*. The MIT Press.	academic publication
Berners-Lee, T. (2000). *Weaving the Web. The Original Design and Ultimate Destiny of the World Wide Web*. New York: Harper Business.	media publication
Burman, E. (2003). *Shift!: The Unfolding Internet-Hype, Hope and History*. John Wiley & Sons.	academic publication
Peter, I. (2004). History of the Internet. http://www.nethistory.info/History%20of%20the%20Internet/.	media publication
Metcalfe, R. (2004). Oral-History:Robert Metcalfe. *Waltham, MA*, *IEEE History Center*.	interview
Kahn, R. E. (2004). ROBERT KAHN: An Interview Conducted by Michael Geselowitz, IEEE History Center, 17 February 2004.	interview
Taylor, R. W. (2004). Robert W. Taylor im Interview mit Lutz Dammbeck. https://www.youtube.com/watch?v=41yZbovMe_8.	interview

Bureau, U. S. C. (2005). Computer and Internet Use in the United States: 2003. *P23-208*.	report
Gillespie, T. (2006). Engineering a Principle: 'End-to-End' in the Design of the Internet. *Social Studies of Science*, *36*(3).	academic publication
Metcalfe, R. (2006). Oral History of Robert Metcalfe. *Boston, MA*, *Computer History Museum*.	interview
Russell, A. L. (2006). 'Rough Consensus and Running Code' and the Internet OSI Standards War. *IEEE Annals of the History of Computing*.	academic publication
Taylor, R. (2008). Oral History of Robert (Bob) Taylor. *Woodside, California*, *Computer History Museum. CHM Reference number: X5059.2009*.	interview
Salus, P. H. (2008). *The ARPAnet Sourcebook: The Unpublished Foundations of the Internet (Computer Classics Revisited)*. Peer-to-Peer Communications Inc.	academic publication
(2009). "Get Linked or Get Lost" A history of the Internet. http://www.randomhistory.com/2009/01/12_internet.html.	media publication
Crocker, S. D. (2009c). Op-Ed Contributor. How the Internet Got its Rules. *The New York Times*.	media publication
Naughton, J. (2009). The internet at 40. A brief history of the future. *The Open University*.	media publication
McKenzie, A. (2011). INWG and the Conception of the Internet: An Eyewitness Account. *The Institute of Electrical and Electronics Engineers*, *33*(1), 66-71.	media publication
Lukasik, S. J. (2011). Why the ARPANET was built. *IEEE Annals of the History of Computing*, *33*(3), 4-20.	academic publication
Crocker, S. D. (2012c). Meet the man who intend the instructions for the Internet. *WIRED*.	media publication
Townes, M. (2012). The Spread of TCP/IP: How the Internet Became the Internet. Millennium - Journal of International Studies, 41(1), 43-64.	academic publication
McCullough, B. (2014). On the 20th Anniversay - An oral history of Netscape's founding.	media publication
Pelkey, J. (2014). "ENTREPRENEURIAL CAPITALISM AND INNOVATION: A HISTORY OF COMPUTER COMMUNICATIONS 1968-1988". http://www.historyofcomputercommunications.info.	media publication
Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C. et al. (2015). Brief History of the Internet. http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.	media publication
Cerf, V. (2015). Mail correspondence.	interview

Crocker, S. D. (2015). Mail to Steve Crocker.	interview
Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. *Journal of Cyber Policy*, *1*, 5-28.	academic publication

Cyber-Utopian Corpus

Corpus of Cyber-Utopian Sources

Source (chronological)	Type of Document
Digital Systems Research Center. (Ed.). (1990[1962]). *In Memoriam: J. C. R. Licklider 1915-1990*.	academic publication
McLuhan, M. (1964). *Understanding Media. The extensions of man*. London, New York.	academic publication
Wiener, N. (1965). *Cybernetics, Second Edition: or the Control and Communication in the Animal and the Machine* (second edition ed.). The MIT Press.	academic publication
Vydas, S. (1965). Cyborg: Evolution of the superman. *JAMA*, *194*(4), 474-475.	academic publication
Simon, H. A. (1965). *The shape of automation for men and management* ([1st ed.] ed.). New York: Harper & Row.	academic publication
Brand, S. (1968). Whole Earth Catalog Fall 1968. http://www.wholeearth.com/issue-electronic-edition.php?iss=1010.	media publication
Reich, C. A. (1971). The greening of America. *online.hillsdale.edu*.	academic publication
Company, P. C. (1972). *People's Computer Company*. (1(1)).	media publication
Brand, S. (1972). Spacwewar. *Rolling Stone*.	media publication
Nelson, T. N. (1974). *Computer Lib.* Sven Dollars.	media publication
Gates, B. (1976). Open Letter to Hobbyists. https://commons.wikimedia.org/wiki/File:Bill_Gates_Letter_to_Hobbyists.jpg.	media publication
Toffler, A. (1980). *The Third Wave*. New York: William Morrow Company.	media publication
Anderson, B. (1981). *Imagined Communities*.	academic publication
Vinge, V. (2001[1982]). *True Names: And the Opening of the Cyberspace Frontier* (2 ed.). Tor Books.	media publication
Haraway, D. (1983). A Cyborg Manifesto. Science, technology and socailist-feminism in the late twentieth cenutry. In D. Bell & B. M. Kennedy(pp. 296-324).	media publication
Magazine, T. I. M. E. (1983). The Computer Moves In. http://content.time.com/time/covers/0,16641,19830103,00.html.	media publication
Gibson, W. (1984). *Neuromancer* (1st ed.). Ace.	media publication
Stallman, R. (1985). The GNU Manifesto. https://www.gnu.org/gnu/manifesto.en.html.	media publication
Barlow, J. P. (1990). Crime & Puzzlement.	media publication

https://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/crime_and_puzzlement_1.html.	
Ellul, J. (1990). *Technological Bluff* (1st ed.). Eerdmans Pub Co.	academic publication
Barber, B. (1992). Jihad vs. McWorld. *The Atlantic*, *March*.	media publication
Levy, S. (1993). Crypto Rebels. http://www.wired.com/1993/02/crypto-rebels/.	media publication
Wired. (1993). First Issue. http://archive.wired.com/wired/archive/1.01/.	media publication
Rheingold, H. (1993). *The Virtual Community*.	academic publication
Kapor, M. (1993c). Where is the Digital Highway Really Heading? The Case for a Jeffersonian Information Policy. *Wired*.	media publication
Dyson, E., Gilder, G., Keyworth, G., & Toffler, A. (1994). Cyberspace and the American Dream: A Magna Carta for the Knowledge Age.	academic publication
Levy, S. (1994). *Hackers: Heroes of the computer revolution* (4). Penguin Books New York.	media publication
Levy, S. (1995). This Changes.Everything. *Newsweek*, *126/127*(27/1).	media publication
Negroponte, N. (1995). *Being Digital* (1 ed.). London: Hodder & Stoughton.	academic publication
Tapscott, D. (1995). *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*. Mcgraw-Hill Co.	academic publication
Gates, B. (1995). *The Road Ahead* (First ed.). Viking.	media publication
Brand, S. (1995). We ow it all to the Hippies. *Time Magazine*, *145*(12).	media publication
Barbrook, R., & Cameron, A. (1996). The Californian Ideology. *Science as Culture*.	academic publication
Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. *wac.colostate.edu*.	media publication
Winner, L. (1997). Cyberlibertarian myths and the prospects for community. *ACM Sigcas Computers and Society*.	academic publication
Cairncross, F. (1997). *Death of Distance: How the Communications Revolution Will Change Our Lives* (First Printing ed.). Harvard Business School Press.	media publication
Matthews, J. T. (1997). Power Shift. *Foreign Affairs*.	media publication
Kelly, K. (1998). *New Rules for the New Economy*. New York, London, Victoria, Toronto, Auckland, New Delhi: Viking.	media publication
Dyson, E. (1998). *Release 2.1: A Design for Living*	media publication

in the Digital Age (1st ed.). Crown Business.	
Kurzweil, R. (1999). *Age of Spiritual Machines* (First Edition ed.). Viking.	media publication
Castells, M. (1999). *The Information Age, Volumes 1-3: Economy, Society and Culture (Information Age Series) (v. 1-3)*. Wiley-Blackwell.	academic publication
Hague, B. N., & Loader, B. D. (1999). *Digital Democracy: Discourse and Decision Making in the Information Age*. Routledge.	academic publication
Glassman, J., Hassett, K., Glassman, J. K., & Hassett, K. A. (1999). *Dow 36,000: The New Strategy for Profiting from the Coming Rise in the Stock Market* (1 ed.). Crown Business.	media publication
Ohmae, K. (1999). *The Borderless World. Power and Strategy in the Interlinked Economy* (Revised ed. ed.). HarperBusiness.	media publication
Schwartz, P., Leyden, P., & Hyatt, J. (1999). *The Long Boom: A Vision For The Coming Age Of Prosperity* (Reprint ed.). Cambridge: Perseus Publishing.	media publication
Kelly, K. (1999). The Roaring Zeros. *Wired* http://www.wired.com/1999/09/zeros/.	media publication
Kaplan, D. A. (1999). *The Silicon Boys: And Their Valley of Dreams* (First Edition ed.). William Morrow.	media publication
U.S. Department of Commerce (2000). Digital Economy 2000.	congress hearing/report
Mitchell, W. J. (2000). *e-topia*. The MIT Press.	academic publication
Castells, M. (2000). *The information age: economy, society and culture. Vol. 1, The rise of the network society* (1). Blackwell Oxford.	academic publication
Shapiro, A. L. (2000). *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know* (2nd.Printing ed.). PublicAffairs.	media publication
Bell, D. (2000). *The End of Ideology: On the Exhaustion of Political Ideas in the Fifties, with "The Resumption of History in the New Century"* (2nd ed.). Harvard University Press.	academic publication
Surowiecki, J. (2000). The Financial Page of the Visionaries of the New Economy Dream On. http://www.newyorker.com/magazine/2000/05/29/the-financial-page-the-visionaries-of-the-new-economy-dream-on.	media publication
Fukuyama, F. (2000). *The Great Disruption: Human Nature and the Reconstitution of Social Order* (1st ed.). Free Press.	academic publication
Himanen, P. (2001). *The Hacker Ethic and the Spirit of the Information Age*. Random House.	academic publication

Horrigan, J. B. (2001). Risky Business: Americans see greed, cluelessness behind dot-coms' comeuppance. *Pew Internet Tracking Report*.	academic publication
Madrick, J. (2001). The Business Media and the New Economy. *The Joan Shorenstein Center on the Press, Politics and Public Policy John F. Kennedy School of Government*, *Research Paper R-24*.	academic publication
Steele, C., & Stein, A. (2002). Communications Revolutions and International Relations. In J. Emmons Allison (Ed.), *Technology, Development, and Democracy: International Conflict and Cooperation in the Information Age* (pp. 25-53). Albana: State University of New York Press.	academic publication
Vegh, S. (2002). Hacktivists or Cyberterrorists? The Changeing Media Discourse on Hacking. *First Monday*, *7*(19).	academic publication
Fukuyama, F. (2002). *Our Posthuman Future: Consequences of the Biotechnology Revolution*. Farrar, Straus, Grioux.	academic publication
Wagner, P. R. (2003). Information wants to be free. Intellectual property and the mythologies of control. *Columbia Law Review*, *103*(995), 995-1034.	academic publication
Mosco, V. (2004). *The digital sublime*.	academic publication
Shinal, J. (2005). Netscape: The IPO that launched an era. http://www.marketwatch.com/story/netscape-ipo-ignited-the-boom-taught-some-hard-lessons-20058518550.	media publication
Friedman, T. L. (2005). *The world is flat : a brief history of the twenty-first century* (1st ed. ed.). New York: Farrar, Straus and Giroux.	media publication
Turner, F. (2006). From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism. *books.google.com*.	academic publication
Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (9/23/07 ed.). Yale University Press.	academic publication
Pärna, K. (2010). *Believing the Net.* Leiden University Press.	academic publication
Zuckernman, E. (2010). Internet Freedom: Beyond Circumvention. http://www.ethanzuckerman.com/blog/2010/02/22/internet-freedom-beyond-circumvention/.	media publication
Clinton, H. R. (2010). Remarks on Internet Freedom. http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.	policy document
Coleman, E. G. (2013). *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton University Press.	academic publication
Rid, T. (2016). *Maschinendämmerung: Eine kurze*	academic publication

Geschichte der Kybernetik. Propyläen Verlag.	

These sources were identified by using the same technique as the cyber-realist corpus. It also included a new method. To identify the most relevant cyber-utopian books I did not just rely on secondary sources, but also screened the New York Times bestseller list (1980 - 2000) for technology books dealing with the Internet or describing the digital revolution. I picked those for deeper investigation that stayed more than four weeks on a best-seller list (The New York Times, 2016). The bestseller lists are a good proxy to gauge the relative societal impact of a book, especially during the 1990s where most people still read physical books. Not in all cases I have read *and* coded the entire book. In many instances I relied on summaries or press reviews.

Information Superhighway Corpus

Corpus of Information Superhighway Initiative of the Clinton/Gore Administration

Source (chronological)	Type of Document
Shultz, G. P. (1985c). Shaping American Foreign Policy: New Realities and New Ways of Thinking. *Foreign Affairs*.	media publication
Gore, A. (1989). National High-Performance Computer Technology Act. https://w2.eff.org/Legislation/Bills_by_sponsor/Old/gore_s1067_89.bill.	policy document
Broad, W. J. (1992c). Clinton to Promote High Technology, With Gore in Charge. *The New York Times*.	media publication
Headquarters, C.-G. C. (1992). TECHNOLOGY: THE ENGINE OF ECONOMIC GROWTH A National Technology Policy for America September 18, 1992.	policy document
U.S. Congress, O. O. T. A. (1993). Advanced Network Technology. OTA-BP-TCT-101, NTIS order #PB93-203735.	congress hearing/report
U.S. Congress, O. O. T. A. (1993). Making Government Work: Electronic Delivery of Federal Services. OTA-TCT-578, NTIS order #PB94-107067.	congress hearing/report
Clinton, W. J., & Gore, A. (1993). Technology for America's Economic Growth, A New Direction to Build Economic Strength.	policy document
Magazine, T. I. M. E. (1993). The Info Highway. Bringing a revolution in entertainment, news and communication. http://content.time.com/time/covers/0,16641,19930412,00.html.	Media publication
Information Infrastructure Task Force (1993). The National Information Infrastructure: Agenda for Action.	policy document
Debnam, B. (1994c). Answers from Vice President Al Gore: The Information Superhighway. Observer-Reporter.	media publication
Noam, E., & Pogorel, G. (Eds.). (1994). *Asymmetric deregulation and the transformation of the international telecommunications regime*.	academic publication
International Telecommunication Union (1994). Buenos Aires Declaration on Global Telecommunication Development for the 21st Century.	policy document
Subcommittee on Technology and the Law of the Committee on the Judiciary United States Senate (1994). Digital Telephony and Law Enforcement	policy document

Access to Advanced Telecommunications Technologies and Services. *H.R. 4922 and S.2375*.	
Clinton, W. J. (1994). Electronic Mail Message to Prime Minister Carl Bildt of Sweden. http://www.presidency.ucsb.edu/ws/?pid=49664.	policy document
Lippman, J., & Harmon, A. (1994c). Gore Calls for All-Inclusive Information Superhighway. Los Angeles Times.	media publication
Gore, A. (1994). *INAUGURATION OF THE FIRST WORLD TELECOMMUNICATION DEVELOPMENT CONFERENCE (WTDC-94)*. Proceedings from WORLD TELECOMMUNICATION DEVELOPMENT CONFERENCE.	policy document
Gore, A. (1994). Remarks Prepared for Delivery by Vice President Al Gore. Royce Hall, UCLA Los Angeles.	policy document
Sugrue, T. (1994). The Government's Role in the National Information Infrastructure. *Media Law & Policy*.	academic publication
U.S. Department of Commerce. Technology Administration (1994). The Information Infrastructure: Reaching Society's Goals. Report of the Infrastructure Task Force Committee on Applications and Technology. *NIST Special Publication 868*.	policy document
Cate, F. H. (1994). The National Information Infrastructure: Policymaking and Policymakers. *Stan. L. & Pol'y Rev.*, *6*, 43.	academic publication
Auletta, K. (1994c). Under the Wire. Will the telecommunications revolution end in monopoly or Big Brotherhood? Neither, if Al Gore gets his way. *The New Yorker*.	media publication
Cohen, N. (1994). Wiretapping and the Digital Telephony Bill: Past and Present. http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall94-papers/cohen-digital-telephony.html.	academic publication
Noam, E. M. (1995). Beyond Telecommunications Liberalization: Past Performance, Present Hype, And Future Direction. In W. J. Drake (Ed.), *The New Information Infrastructure: Stategies for U.S. Policy (A Twentieth Century Fund Book)* (English Language ed.). Twentieth Century Foundation.	academic publication
U.S. Congress, Office of Technology Assessment(1995). Global Communications: Opportunities for Trade and Aid. *OTA-ITC-642*.	congress hearing/report
Reidenberg, J. R. (1995). Information Flows on the Global Infobahn: Toward New U.S. policies. In W. J. Drake (Ed.), *The New Information Infrastructure: Stategies for U.S. Policy (A Twentieth Century Fund Book)* (English Language ed.). Twentieth Century Foundation.	academic publication

Lehman, B. A., & Brown, R. H. (1995). Intellectual Property and the National Information Infrastructure. The Report of the Working Group on Intellectual Property Rights.	congress hearing/report
Geller, H. (1995). Reforming the U.S. Telecommincations Policymaking Process. In W. J. Drake (Ed.), *The New Information Infrastructure: Stategies for U.S. Policy (A Twentieth Century Fund Book)* (English Language ed.). Twentieth Century Foundation.	academic publication
McKnight, L., & Nuemann, R. W. (1995). Technology Policy and the National Information Infrastructure. In W. J. Drake (Ed.), *The New Information Infrastructure: Stategies for U.S. Policy (A Twentieth Century Fund Book)* (English Language ed.). Twentieth Century Foundation.	academic publication
Steering Committee on the Changing Nature of Telecommunications/Information Infrastructure (Ed.). (1995). *The Changing Nature of Telecommunications/Information Infrastructure*. Washington D.C.: The National Academies.	congress hearing/report
Besser, H. (1995). The information superhighway: Social and cultural impact. In J. Boal & I. Boal. San Francisco: City Lights Press.	media publication
Drake, W. J. (1995). The National Information Infrastructure Debate: Issues, Interests, and the Congressional Process. In W. J. Drake (Ed.), *The New Information Infrastructure: Stategies for U.S. Policy (A Twentieth Century Fund Book)* (English Language ed.). Twentieth Century Foundation.	academic publication
Drake, W. J. (1995). *The New Information Infrastructure: Stategies for U.S. Policy (A Twentieth Century Fund Book)* (English Language ed.). Twentieth Century Foundation.	academic publication
Kahn, R. E. (1995). The Role of Government in the Evolution of the Internet. In N. A. O. Engineering (Ed.), *Revolution in the U.S. Information Infrastructure*. Washington D.C.: National Academy Press.	academic publication
Drake, W. J. (1995). The Turning Point. In W. J. Drake (Ed.), *The New Information Infrastructure: Stategies for U.S. Policy (A Twentieth Century Fund Book)* (English Language ed.). Twentieth Century Foundation.	academic publication
Weiss, E. (1996). Creating a new civilization: The politics of the third wave. *Harvard Journal of Law & Technology*, *9*(1).	academic publication
Clinton, W. J. (1996). Executive Order 13010 - Critical Infrastructure Protection.	executive order
Wellbery, B. S. (1996). Privacy Protection on the Information Superhighway. *Journal of Civil Rights and Economic Development*, *11*(3), 10.	academic publication
Kedzie, C. (1997). *Communication and Democracy:*	academic publication

Coincident Revolutions and the Emergent Dictators. RAND.	
President's Commission on Critical Infrastructure Protection (1997). Critical Foundations. Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection.	congress hearing/report
Clinton, W. J. (1997). Message to Internet Users on Electronic Commerce.	policy document
Cohen, H. (1997). The Communications Decency Act of 1996. *CRS Report for Congress*.	congress hearing/report
Clinton, W. J. (1998). Commencement Address at the United States Naval Academy in Annapolis, Maryland.	policy document
White House (1998). PROTECTING CYBER SECURITY. http://clinton5.nara.gov/textonly/WH/EOP/NSC/html/nsc-22.html.	policy document
Hamblen, M. (1999). Clinton commits $1.46 B to fight cyberterrorism.	media publication
Makulowich, J. (1999). Clinton's Cyber-Security Plan Takes Shape. https://washingtontechnology.com/Articles/1998/06/17/Clintons-CyberSecurity-Plan-Takes-Shape.aspx.	media publication
The United States Senate Special Committee on the Year 2000 Technology Problem (1999). Investigating the Impact of the Year 2000 Problem. *S. Prt. 106-10*.	congress hearing/report
Saad, L. (1999). Public Concern Over Y2K Computer Glitch Drops As Awareness Grows. http://www.gallup.com/poll/4024/public-concern-over-y2k-computer-glitch-drops-awareness-grows.aspx.	media publication
Wiggins, R. (2000). Al Gore and the creation of the Internet. *First Monday*, *5*(10).	academic publication
Cerf, V., & Kahn, R. E. (2000). Al Gore and the Internet.	academic publication
Computerworld. (2000). Some Key Facts and Events in Y2K History.	media publication
Reuters. (2000). Y2K Money Well Spent. http://www.everything2000.com/news/computer/y2kmoneywellspent.asp.	media publication
EPIC. (2002). Communications Decency Act. https://epic.org/free_speech/cda/.	policy document
CNN. (2006). Looking at the Y2K Bug. https://web.archive.org/web/20060207191845/http://www.cnn.com/TECH/specials/y2k/.	media publication

Shah, R. C., & Kesan, J. P. (2007). The privatization of the Internet's backbone network. *Journal of Broadcasting & Electronic Media*, *51*(1), 93-109.	academic publication
Manjoo, F. (2009). Apocalypse then. http://www.slate.com/articles/technology/technology/features/2009/apocalypse_then/was_y2k_a_waste.html.	media publication
Bennett, A. J. (2013). *The Race for the White House from Reagan to Clinton*. Palgrave Macmillan.	academic publication
New York Times. (2013). Y2K Bug: Much Ado About Nothing? Retro Report. https://www.youtube.com/watch?v=SoGNiHV09BU.	media publication
McCullough, B. (2014). Did Al Gore really invent the Internet? http://www.internethistorypodcast.com/2014/11/did-al-gore-really-invent-the-internet/.	media publication
Allen-Ebrahimian, B. (2016). The Man Who Nailed Jello to the Wall. *Foreign Policy* http://foreignpolicy.com/2016/06/29/the-man-who-nailed-jello-to-the-wall-lu-wei-china-internet-czar-learns-how-to-tame-the-web/.	media publication

These sources were identified by using the same technique as the cyber-realist corpus. Due to the changing positions of the Clinton administration, there is a partial overlap of sources with the cyber-realist corpus, for example in terms of critical infrastructure protection or the Y2k panic.

Cyber-Realism Corpus

Corpus of Cyber-Realism Carrier Texts

Source (chronological)	Type of Document
Rona, T. P. (1976). Weapon Systems and Information War. *Boeing Aerospace Company*.	academic publication
Rechtin, E. (1983). The Technology of Command. *The Charles H. Davies Lecture Series*, *Fall Lecture*.	academic publication
White House (1984). *National Security Decision Directive Number 145:* National Policy on Telecommunications and Automated Information Systems Security.	national security directive
Naval-Studies-Board. (1988). Implications of Advancing Technology for Naval Operations in the Twenty-First Century. *Naval Studies Board*, *Volume 1: Overview*.	academic publication
Congress. (1991). Computer security: hearing before the Subcommittee on Technology and Competitiveness of the Committee on Science.	congress hearing/report
National Research Council (1991). Computers at Risk. Safe Computing In the Information Age.	research report
Department of Defense (1992). Directive Number TS-3600.01. Information Operations. *Department of Defense*.	classified (inaccessible) national security directive
White House (1993). Statement by the Press Secretary. https://epic.org/crypto/clipper/white_house_statement_4_93.html.	policy document
United States Department of the Air Force (1995). Cornerstones of Information Warfare., 13.	military doctrine document
National Research Council (1991). Computers at Risk. Safe Computing In the Information Age.	research report
Krepinevich, A. F. (1992). The Military-Technical Revolution: A Preliminary Assessment. Proceedings from Prepared for the Office of Net Assessment, Washington D.C.	research report
Defense Science Board (1994). Summer Study Task Force on Information Architecture for the Battlefield.	research report
Communications Assistance for Law Enforcement Act (CALEA) or Digital Telephony Bill (1994)	policy document
White House (1995). A National Security Strategy of Engagement and Enlargement.	national security strategy
United States Department of the Air Force (1995). Cornerstones of Information Warfare., 13.	military doctrine document
General Accounting Office (1996). Computer Attacks at Department of Defense Pose Increasing Risks. *AIMD-96-84*.	research report

Clinton, W. J. (1996). Executive Order 13010 - Critical Infrastructure Protection.	executive order
Edmonds, A. J. (1996). C4I for the Warrior - Global Command and Control System: From Concept to Reality., 25.	military doctrine document
Joint Chiefs of Staff (1996). Information Warfare. A strategy for Peace… The Decisive Edge in War.	military doctrine document
Joint Chiefs of Staff (1996). Information Warfare. Legal, Regulatory, Policy and Organizational Considerations for Assurance. *2nd Edition*.	military doctrine document
Joint Chiefs of Staff (1996). Joint Vision 2010.	military doctrine document
U.S. Senate Permanent Subcommittee on Investigations. (1996). Security in Cyberspace. Appendix B. The Case Study: Rome Laboratory Griffis Air Force Base, NY Intrusion.	congress hearing/report
Molander, R. C., Riddle, A. S., & Wilson, P. A. (1996). *Strategic Information Warfare. A New Face of War. Prepared for the Office of the Secretary of Defense*. RAND Corporation.	academic publication
Owens, W. A. (1996). The Emerging U.S. System-of-Systems. *National Defense University Strategic Forum*, *63*.	academic publication
Schwartau, W. (1997). An Introduction to Information Warfare. In R. L. Pfaltzgraff & R. H. Shultz (Eds.), *War in the Information Age: New Challenges for U S Security (Association of the United States Army)* (pp. 47-60). Washington: Brassey's UK Ltd.	academic publication
President's Commission on Critical Infrastructure Protection (1997). Critical Foundations. Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection.	congress hearing/report
Thompson, M. J. (1997). Information Warfare - Who is Responsible? Coordinating the Protection of our Nationalk Information Infrastructure. *U.S. Army War College*.	academic publication
Cowen, W. S. (1997). Report of the Quadrennial Defense Review.	military doctrine document
Pfaltzgraff, R. L., & Shultz, R. H. (Eds.). (1997). *War in the Information Age: New Challenges for US Security (Association of the United States Army)*. Brassey's UK Ltd.	academic publication
U.S. Air Force (1998). Information Operations. *Air Force Doctrine Document*, *2-5*.	military doctrine document
Joint Chiefs of Staff (1998). Joint Doctrine for Information Operations. *Joint Publication 3-13*.	military doctrine document
White House (1999). A National Security Strategy for a New Century.	national security strategy

White House (1998). PRESIDENTIAL DECISION DIRECTIVE/NSC-63. https://fas.org/irp/offdocs/pdd/pdd-63.htm.	national security directive
Department of Defense. Office of General Counsel (1999). AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS.	congress hearing/report
Joint Chiefs of Staff (2000). Joint Vision 2020. America's Military Preparing for Tomorrow.	military doctrine document
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act)	policy announcement
Rice, C., & Ridge, T. (2001). New Counter-Terrorism and CyberSpace Security Positions announced. *The White House*.	policy announcement
Rumsfeld, D. (2001). Remarks by the President and Secretary of Defense Donald Rumsfeld Swearing-In Ceremony. *The Oval Office*.	policy announcement
Office of Homeland Security (2002). National Strategy for Homeland Security.	national security strategy
White House (2002). The National Security Strategy of the United States of America.	national security strategy
White House (2003). A National Strategy to Secure Cyberspace.	national security strategy
Department of Defense (2003). Information Operations Roadmap.	military doctrine document
Joint Chiefs of Staff (2004). Information Operations. *JP 3-13*.	military doctrine document
Porter, C. D. (2004). Network Centric Warfare - Transforming the U.S. Military.	academic publication
Director of National Intelligence. (2005). The National Intelligence Strategy of the United States of America. Transformation through Integration and Innovation.	national security strategy
White House (2006). National Strategy for Combating Terrorism.	national security strategy
White House (2006). The National Security Strategy of the United States of America.	national security strategy
Department of Defense (2006). Directive Number TS-3600.01. Information Operations. *Department of Defense*.	military doctrine document
Joint Chiefs of Staff (2006). Information Operations. *JP 3-13*.	military doctrine document
Wilson, C. (2006). Information Operations and Cyberwar: Capabilities and Related Policy Issues. *CRS Report for Congress*, *RL31787*.	congress hearing/report

Department of Defense (2006). Quadrennial Defense Review Report.	military doctrine document
Joint Chiefs of Staff (2006). The National Military Strategy for Cyberspace Operations. *20318*.	military doctrine document
White House (2007). National Strategy for Information Sharing. Successes and Challenges in Improving Terrorism-Related Information Sharing.	national security strategy
Homeland Security Council (2007). National Strategy for Homeland Security.	national security strategy
Department of Defense (2007). Department of Defense Global Information Grid Architectural Vision. Vision for a Net-Centric, Service-Oriented DoD Enterprise. *Department of Defense*.	military doctrine document
White House (2008). National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23.	national security directive
Executive Office of the President of the United States (2009). Comprehensive National Cybersecurity Initiative.	policy announcement
United States Government Accountability Office (2010). Cyberspace Policy. Executive Branch is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership is Needed. *GAO-11-14*.	congress hearing/report
White House (2010). National Security Strategy.	national security strategy
White House (2011). International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World.	national security strategy
Department of Defense (2010). Quadrennial Defense Review Report.	military doctrine document
Joint Chiefs of Staff (2012). Capstone Concept for Joint Operations. Joint Force 2020.	military doctrine document
Joint Chiefs of Staff (2013). Information Operations. *JP 3-13*.	military doctrine document
White House (2012) Presidential Policy Directive PPD 20	classified (inaccessible) national security directive
Fischer, E. A., Liu, E. C., Rollins, H. W., & Theohary, C. A. (2013). The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress. *CRS 7-5700*.	academic publication
Department of Defense (2011 & 2015). The DOD Cyber Strategy.	military doctrine document

Hybrid Obama Presidency Corpus

Corpus of Obama Administration

Source (chronological)	Type of Document
Obama, B. (2007). Connecting and Empowering All Americans Through Technology and Innovation.	policy announcement
Holen, A. (2008). A Comparison of the Technology Policies of Barack Obama and John McCain.	academic publication
Obama, B. (2008). Network Neutrality. Snow and Dorgan's legislation to protect network neutrality. http://obamaspeeches.com/076-Network-Neutrality-Obama-Podcast.htm.	policy announcement
Glendinning, L. (2008). Obama, McCain computers 'hacked' during election campaign. https://www.theguardian.com/global/2008/nov/07/obama-white-house-usa.	media publication
Executive Office of the President of the United States (2009). Comprehensive National Cybersecurity Initiative.	policy announcement
Renshon, S. A. (2009). *National Security in the Obama Administration: Reassessing the Bush Doctrine*. Routledge.	academic publication
McConnell, M. (2009). Cyberwar is the New Atomic Age. *New Perspectives Quarterly*, *26*(3), 72-77.	media publication
Obama, B. (2009). Remarks by President Barack Obama at Town Hall Meeting with Future Chinese Leaders.	policy announcement
Obama, B. (2009). Remarks by the President on Securing Our Nation's Cyber Infrastructure. https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.	policy announcement
White House (2010). National Security Strategy.	national security strategy
McConnell, M. (2010). Mike McConnell on how to win the cyber-war were losing. *Washington Post*, *28*, B01.	media publication
Clinton, H. R. (2010). Remarks on Interent Freedom.	policy announcement
STRATCOM. (2010). U.S. Cybercommand. https://www.stratcom.mil/factsheets/2/Cyber_Command/.	national security strategy
Lynn, W. J. (2010c). Defending a New Domain. The Pentagon's Cyberstrategy. *Foreign Affairs*.	policy announcement
White House (2011). International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World.	national security strategy
Mulrine, A. (2011). CIA Chief Leon Panetta: The Next Pearl Harbor Could be a Cyberattack. *Christian Science Monitor*, *9*.	media publication

Gertz, B. (2011c). Computer-based attacks emerge as threat of future, general says. *Washington Times*.	media publication
Rajaee, B. M., & Miller, M. J. (Eds.). (2012). *National security under the Obama administration*. Palgrave Macmillan.	academic publication
Kroft, S. (2012c). Stuxnet: Computer Worm Opens New Era of Warfare. *CBS News*.	media publication
Lepri, C. (2012). Obama's New Intelligence Policy. Meeting new challenges. In B. M. Rajaee & M. J. Miller (Eds.), *National security under the Obama administration*. Palgrave Macmillan.	academic publication
Panetta, L. E. (2012). Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City. http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.	media publication
Obama, B. (2012c). Taking the Cyberattack Threat Seriously. *The Wall Street Journal*.	policy announcement
Bumiller, E., & Shanker, T. (2012). Panetta Warns of Dire Threat of Cyberattack on U.S. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0.	media publication
Kaufman, S. J. (2012). U.S. National Security Strategy from Bush to Obama. In B. M. Rajaee & M. J. Miller (Eds.), *National security under the Obama administration*. Palgrave Macmillan.	academic publication
Bumiller, E., & Shanker, T. (2012). Panetta Warns of Dire Threat of Cyberattack on U.S. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0.	media publication
Houck, C. (2013). Barack Obama on surveillance, then and now. http://www.politifact.com/truth-o-meter/article/2013/jun/13/barack-obama-surveillance-then-and-now/.	media publication
Nakashima, E., & Warrick, J. (2013). For NSA chief, terrorist threat drives passion to 'collect it all'. https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html?utm_term=.69fc703b456a.	media publication
Fischer, E. A., Liu, E. C., Rollins, H. W., & Theohary, C. A. (2013). The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress. *CRS 7-5700*.	academic publication
White House (2013). Administration White Paper. Bulk Collection of Telephony Metadata under Section 215 of the USA Patriot Act.	policy announcement
Post, W. (2013). TRANSCRIPT: President Obama's	media publication

August 9, 2013, news conference at the White House. https://www.washingtonpost.com/politics/transcript-president-obamas-august-9-2013-news-conference-at-the-white-house/2013/08/09/5a6c21e8-011c-11e3-9a3e-916de805f65d_story.html?utm_term=.1286174cd3a6.	
Post, T. W. (2013). TRANSCRIPT: President Obama's August 9, 2013, news conference at the White House.	policy announcement
Onea, T. (2013). *US Foreign Policy in the Post-Cold War Era*. Palgrave Macmillan.	academic publication
Clarke, R. A., Morell, M. J., Stone, G. R., & Sunstein, C. R. (2014). The NSA Report: Liberty and Security in a Changing World. The President's Review Group on Intelligence and Communications Technologies.	report
Breslow, J. (2014). Obama on Mass Government Surveillance, Then and Now. http://www.pbs.org/wgbh/frontline/article/obama-on-mass-government-surveillance-then-and-now/.	media publication
Starr-Deelen, D. (2014). *Presidential Policies on Terrorism: From Ronald Reagan to Barack Obama*. Palgrave Macmillan.	academic publication
Obama, B. (2014). Remarks by the President on Review of Signals Intelligence.	policy announcement
Hern, A. (2014c). US government increases funding for Tor, giving $1.8m in 2013. *The Guardian*.	media publication
Dourado, E., & Castillo, A. (2015). Federal Cybersecurity Breaches Mount Despite Increased Spending. http://mercatus.org/publication/federal-cybersecurity-breaches-mount-despite-increased-spending.	academic publication
McLeary, P. (2015). NATO Chief: Cyber can Trigger Article 5. http://www.defensenews.com/story/defense/policy-budget/warfare/2015/03/25/nato-cyber-russia-exercises/70427930/.	media publication
Childress, S. (2015c). How the NSA Spying Programs Have Changed Since Snowden. *Frontline*.	media publication
Department of Defense (2015). The DOD Cyber Strategy.	national security strategy

Ehrenwörtliche Erklärung

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe; die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Ferner bestätige ich hiermit die Kenntnis der Promotionsordnung der Fakultät für Sozial- und Verhaltenswissenschaften der Friedrich-Schiller Universität Jena-

Bei der Auswahl und Auswertung des Materials sowie bei der Herstellung des Manuskripts habe ich Unterstützungsleistungen von folgenden Personen erhalten:

1. Karl Franz Fritsch (engl. Lektorat)
2. Anna-Sophia Fritsch (engl. Lektorat)
3. Christian Opitz (Korrektur des Theorieteils)
4. Helena Falk (Kontakt ARPA Entwickler)

Weitere Personen waren an der geistigen Herstellung der vorliegenden Arbeit nicht beteiligt. Insbesondere habe ich nicht die Hilfe einer Promotionsberaterin bzw. eines Promotionsberaters in Anspruch genommen. Dritte haben von mir weder unmittelbar noch mittelbar geldwerte Leistungen für Arbeiten erhalten, die im Zusammenhang mit dem Inhalt der vorgelegten Dissertation stehen.

Die Arbeit wurde bisher weder im Inland noch im Ausland in gleicher oder ähnlicher Form einer anderen Prüfungsbehörde als Dissertation vorgelegt.

Matthias Schulze, Leipzig den 1.3.2017
