The Birth of Cyber as a National Security Agenda

Nikola Schmidt

Ph.D. Thesis

2016

The Birth of Cyber as a National Security Agenda

Ph.D. Thesis

Nikola Schmidt

Department of International Relations

Institute of Political Studies

Faculty of Social Sciences

Charles University

Prague, Czech Republic

2016

Supervisor:

doc. PhDr. RNDr. Nikola Hynek, M.A., PgDip Res, Ph.D.

DECLARATION

I, Nikola Schmidt, hereby declare that this thesis has been written by me, that it is the result of work carried out by me and that all the sources used in this thesis are duly indicated and listed in the bibliographical references.

Date: .....

Signature: .....

ACKNOLEDGEMENTS

First, I would like to thank here to my friend and supervisor Nik Hynek for his numerous remarks during the writing of this dissertation. It has been tough time of friendly remarks and hard but inspirational coercion to move forward, but we have managed to come to this final point and I gratefully thank him.

I would also like to acknowledge the significant contribution of my friend Vít Střítecký, my first supervisor, who helped me to focus on this topic and who had the patience with me during the first steps of the research.

The dissertation would never exist in this final shape without continuous help of Michal Smetana, my longtime friend, who kept me focused on the target and helped me a lot with any administrative steps. In that perspective, many thanks goes to Běla Plechanovová who so patiently respected my minimal talent in any administrative preciseness during the doctoral studies, but still let me to arrive to this final point.

Two reviewers took their time and managed to read my first draft. I could not imagine better reviews that I received from both of them. Tim Stevens read through the whole work and gave me several amazing remarks that helped to develop the argument. Radim Polčák did the same with no different passion and quality. This work would not have reached the same level as it is without their inspirational ideas.

Last but not least, I should thank to my girlfriend Markéta Černohorská, a passionate scientist in molecular biology, that she had the patience to talk about (bio)politics during the frantic year of writing.

CONTENTS

KEY WORDS

International Relations; Cyber Security; Discourse Analysis; Cyberpunk; Post-Structuralism; Science and Technology Studies; Power; Liberal Democracy;

ABSTRACT

The following dissertation studies the question how cyber security has become a national security agenda and discusses implications of the observed processes to current international security status quo. I divided the research into three parts. The first part embodies theoretical and methodological approach. The second part studies three distinct discourses related to cyber security, the techno-geek discourse, the crime-espionage discourse and the nation-defense discourse using the method of Michel Foucault about archaeology of knowledge. The third part then draws on these three discourses and discusses implications through lens of several theoretical perspectives. Namely through concepts taken from science and technology studies, from actor network theory and network assemblages. The critical point of the research is a distinct reading of these discourses. While techno-geeks are understood as a source of semiosis, hackers' capability and crypto-anarchy ideology influenced by cyberpunk subculture, the cyber-crime and espionage discourse is read as a source of evidence of the hackers' capability. The inspiration in popular subculture is combined with current efforts in development of liberating technologies against oppression by authorities, oppression recognized by the eyes of the crypto-anarchist movement seeking the world without state regulation or nation states completely. If these visions of near future inspired by cyberpunk are combined with the evidence of cyber crime, I argue, that we can observe an emergence of overemphasized imaginations on a national security level, the national cyber defense that gives birth of cyber as a national security agenda. In the discussion part, I am elaborating on different kind of expertise, the first driven by curiosity and the second driven by policy. Whereas the former would tend to understand the natural dynamics, the latter reacts on policy requirements based on beliefs. As both, natural and cultural sources, are influencing our perceptual field on the given problem, we can observe a proliferation of hybrids into cyberspace governability. Cyber security as a national security agenda has been able to develop its own church of knowledge that is covered by policy driven expertise reacting on the security imaginations; however, certain technical characteristics are surely making systems vulnerable. The inability to distinct between the cultural and the natural source is rising technological radical uncertainty, which subsequently fuels the imaginations of a needed national cyber defense. However, as states are raising their national cyber defenses they were being caught in a supermassive surveillance operation against their own citizens, which is certainly fueling the will of crypto-anarchist movement to develop more liberating technologies. More liberating technologies driven by actualized power of crypto-anarchists means lower immanent power to nation states. In the end, I argue that if nation states continue to strengthen their power and the construction of panopticon by arguing with needed defenses against imagined cyber terrorists and continue to lower privacy and freedom of citizens, we might be heading toward a world of hybridized governance, towards an emergence of oligopticon, in which states do not play the most significant role of a sovereign actor.

LIST OF ABBREVIATIONS

AI	Artificial intelligence
API	Application Programming Interface (connection interface for 3rd party developers)
BMG	Bertelsmann Music Group
CEVRO	School of political studies
CIA	Central Intelligence Agency
DARPA	Defense Advanced Research Projects Agency
DDoS	Distribute Denial of Service
DHS	Department of Homeland Security
EMI	Electric and Musical Industries
ENISA	European Union Agency for Network and Information Security
EUROPOL	European Police Office
FBI	Federal Bureau of Investigation
ICT	Information and Communication Technology
IP	Internet Protocol
ITU	International Telecommunication Union
MITRE	The MITRE Corporatio
NISA	NATO International School of Azerbaijan
NSA	National Security Agency
PRISM	Clandestine surveillance program conducted by NSA
RFID	Radio-Frequency IDentification
SCADA	Supervisory Control And Data Acquisition
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TOR	The Onion Network

LIST OF FIGURES

LIST OF TABLES

FOREWORD

The following text is a result of mixed experience and research. First, I spent about seven years in IT business as a co-founder of software development company. Second, I have been interested in sociology of technology since my high-school studies, so I studied sociology and international relations with focus on international security and cyber security. Third, last four years I went through several phases of deep enthusiasm of newly emerging security field of cyber security I can cover thanks to my experience and a bitter skepticism about the new security discipline as well. Fourth, I found myself in a very critical point, when I realized how inappropriately is cyber security adopted on a national security level during two short employments at different state administrations where I worked during my PhD studies.

The experts I met during my international visits at cyber security institutions varied in their expertise, some of them were amazing experts knowing their issue from a technical perspective and approached the case with level-headed mind, but a lot of them just repeated mantras of international cooperation, better education, stronger cyber defense shields etc. I was surprised how some experts having decision making power are easily situated in their positions despite the fact that they could not participate in a general debate concerning a particular important and well know cyber-attack. I was asking myself how policy can be formulated when an expert responsible for the policy does not understand basic technical documents regarding cyber-attack e.g. on a turbine in a power plant. Moreover, some policy oriented conferences looked like mind recruitment events known from multi-level marketing business models that make their business on a serious brain-washing using argumentation that nobody can question. Maybe that is exaggerated and not fair, however, that suspicion motivated me to write the following dissertation as it is.

I am writing it this way as I feel responsibility to admit my skepticism; however, I did my best to keep myself in a rigorous analysis perspective, when I analyzed particular hypersecuritization discourses.

Here, I would like to state clearly that I am not principal denier, that I take threats from cyberspace seriously and I do not deny that some of them can cause really serious harm. However, I am convinced that the enormous political emphasization does not relate with the dynamics of technology evolution and threats that it brings up. It produces new authorities based on new *churches of knowledge* that is repeated in a circle as they become undisputable *fields of truth.*

Hence, the purpose of the following work is to unveil these processes and to discuss the political implications to current global society. I am not convinced that I covered everything, I rather tried to use some methods to provide a reader with a new critical perspective on cyberspace securitization, provide a reader with ideas for further research in possible implications on international order and in the end provide some fresh ideas to policy makers in the business to understand where the cyber security and the national defense thinking in terms of cyber security has its genesis.

“Where there is power, there is resistance.”

— Michel Foucault —

INTRODUCTION

The dissertation you are holding in your hands is about cyber security, about the birth of cyber security as a national security agenda, about the process how states have become excessively interested in securing of their digital borders. The point of the dissertation is to unveil the processes that have led to the establishment of cyber as an international undisputable threat that is frequently put above the nuclear threat. One may expect a clear criticism of cyber security as a national security agenda and I elaborate on that criticism a lot, however, I did not want to be limited to a mere criticism. A pieces of policy recommendations can be found throughout the work, prevalently in the last discussion chapter. My distinction to the other works I have seen is in the critical analysis of political implications of current policy of imaginations avoiding or misinterpreting expert insight to the technical realities; thus the role of technical knowledge, its formation and resonation in policy sphere. I am directly criticizing the current international race towards establishing cyber security institutions and I am proposing an image using the approach of genealogy of discourse that explains the content behind this current wild policy of securing cyberspace against threats that seems to me to be severely overemphasized. There must be a reason why policy makers contribute to this process with so much low critical insight, especially when we simply do not observe any cyber doom around. However, there are also political implications I am discussing in the final part, which I understand as serious, but which are not too visible to those, who contribute to the hypersecuritization discourse based on overemphasized imaginations. I recognized this perspective as a valuable one for further policy making in cyber security and believe that this work can contribute to more level-headed reactions; reactions that Claudia Aradau and Rens van Munster understand as normalized reactions on possible catastrophe.[1]

In the recent history regarding security of computers and networking, history of about four decades ago from now, we have seen several moments when the security

[1] Claudia Aradau and Rens van Munster, *Politics of Catastrophe* (London and New York: Routledge, 2011).

issues of computer woke up policy makers such as Morris worm,[2] but not as much as recently. Events after the attack on Estonia in 2007 were unprecedented providing with the political implication we have observed until now. Scholars, companies or even states had been aware about cyber threats until this event, but the development since then has given a very structural national security agenda. A cyber-attack was understood as a possibility even before. The Mafia boy who conducted DDoS attacks on 7th February 2000 against servers of rising business stars such as Yahoo, Amazon, eBay or CNN[3] was found by FBI days later and made the agents shocked by his age of fifteen years. No significant political implications were observable that time despite the fact that a script-kiddie was able to ruin crucial online reputation of these massive global businesses, for a while. On the other hand, Estonia 2007 attacks were able to enchant policy makers with a vision of possible cyber doom, which was of course drawn before, but without significant resonation in the political sphere, in a visible materialization of national power in cyberspace, in so broad institutionalization of cyber security knowledge concerning national defense.

The aim of the research is to show how certain discursive practices form particular knowledge that is not necessarily the needed expertise for appropriate policy reaction. In that perspective, the research should serve as a policy extension, as a perspective for policy makers how their ideas have formed, where they come from, whether the current policy making leads into a desired state of national or international security and why the presumptive enemy to a liberal nation state will be stronger and why the policy itself can be the enemy if this policy of imaginations in cyber war prevails.

The pathway of this research has been since the beginning to read particular subcultural content not only as a *source of semiosis* for further cyber security policy driven discourse, but also as a *source of capability* and *source of ideology*. The source of language used in different, but comparable connotations, the source of fear in hackers' capabilities and the source of hostile ideology of crypto-anarchist movement willing to topple down states in their utopist visions. These three components constitute the

[2] E. H. Spafford, "Crisis and Aftermath," *Communications of the ACM* 32, no. 6 (1989): 678–87, doi:10.1145/63526.63527.

[3] A L Barabási, *Linked: The New Science of Networks* (Cambridge, Massachusetts: Perseus Publishing, 2002).

inspirational power in cyberpunk as translated to national security agenda. These three components would not be enough without a particular evidence, which has been found in discourse regarding crime and espionage. Crime represents will of non-state actors, while espionage would be the same if states were not included as hostile agents, of course by discourse as the confirmation methods of a state participation in espionage campaign is still far from being sufficient – the well-known attribution problem. These two steps, encircling in the part of evidence by agglomerating visible facts, are giving birth to cyber as a national security agenda. It would be audacious contention, if there were not been observable misunderstandings, bad technical readings and obvious exaggerations by policy makers working in high profile positions and visibly forming national cyber security policies. The aim of this research is focused on this link between cyberpunk subculture and nation defense policy materialization by reading three discourses as three different players crucial in unveiling of the *new power materialization*. It is not to be read as a confusion between crime and espionage, it is confused in these two sub-discourses already. If an operation is conducted by a company, it should be approached as an act of crime; however, if a state buys services of that company it should be approached as an act of espionage, but states are usually hidden behind the attribution problem and espionage usually works in secrecy; hence it is hard to make a real distinction between these two. I address this problem in detail further.

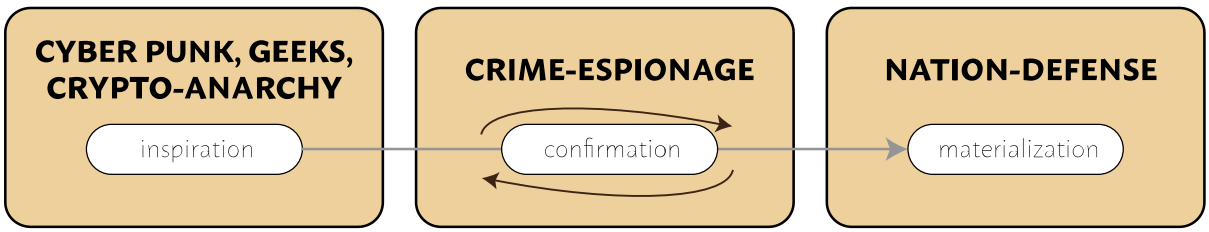


Figure 1 - The internal logic of studied discourses and their internal influence

The final message of the dissertation should be read in the light of a notion of liberal democracy principles embodied in current international system of nation states. If states continue securitizing cyberspace through doomy imaginations, they are probably going to miss the kind of threats that have the capability to do harm to the liberal society.

Bauman pertinently asks[4] that security policy is supposed to secure something, but what insecurity we are addressing by massive global surveillance operations aimed on our own citizens and allies with included transnational internet corporations? Is it a national security? Do we take into considerations the notion of liberal democracy values, while the core representatives of western-type liberal democracies actively deconstruct these principles by such acts? Moreover, that approach is giving motivation to the crypto-anarchist movement, which is working hard on liberating technologies such as bitcoin. These technologies, which are lowering power but also a reason of a nation state regulation, have potency to significantly redraw current global power distribution, which is certainly not in the interest of current players trying to preserve the status quo consisting of a nation state international system. The initial motivation might be clearly in a utopist crypto-anarchist vision of perfect Eden, but omitting the power of epistemic communities driven by crypto-anarchist ideology would not be a political virtue.

The structure of the dissertation follows the logical path of how I studied the flowing discourses. At the beginning, I am summarizing the method, prevalently how I am going to use the method of archaeology of knowledge provided us by Michel Foucault, which is clearly summarized in the end of the chapter and how I am going to apply it on each discourse. However, it is not applied rigidly as the shown method interpretation would presume. Each discourse and identified practices are approached and explained through the lens of Foucault. The summarization method serves in attuning the reader appropriately to read the empirical part through the Foucault's lens. If I recognize it as important, I directly point what processes are theoretically grasped by Foucault in the theoretical part; however, I would spend too much space to explain each part rigidly, so the approach of attuning the reader was chosen in order to have space for more empirical data interpretation.

The discursive approach is then challenged with some selected concepts from science and technology studies. Namely concepts introduced by Sheila Jasanoff such as co-production,[5] in which human and non-human actors play a role in co-producing our

[4] Zygmunt Bauman et al., "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology* 8, no. 2 (2014): 121–44, doi:10.1111/ips.12048.

[5] Sheila Jasanoff, *States of Knowledge: The Co-Production of Science and Social Order* (Routledge, 2004).

knowledge, our representation of the world about both nature and society. Co-production is epistemologically very close to the cyberpunk subculture, in which human is intermingled with technology by body augmentations. Moreover, the same logic of intermingling social with nature can be found in Latour's actor-network theory,[6] which is used in the final discussion and argumentation.

Finally, the whole work is crossed with a debate how our knowledge is formed. It is still about a knowledge as an initial point of everything. Discourse produce perceptions, which resonate with our knowledge before we approach the problem by proposing a policy solution. During that process we depend directly on our ability to critically assess the proposed solution, but especially policy makers are directly dependent on experts and these may be asked to produce knowledge related to the addressed problem. Then, what knowledge is the relevant one? The one produced as a result on a particular policy requirement or the one which has been produced as an outcome of curiosity? These questions are crucial in assessing discursive practices and subsequent power materialization processes. I am unveiling some of these crystal clear policy motivated practices lacking an insight into technical aspects and ignoring reports of experts paid by the same administration. The combination of an empirical part unveiling these realities with the discursive practices forming our perception of the world out there is then finally challenged in a critical assessment of current efforts concerning cyber security including a debate where these cyber war and cyber terrorism imaginations may lead.

Science and technology is a part of our culture, it permeates our culture,[7] not only how we communicate, but also how we record, interpret, explain and govern things around us. There was a case worth to mention here as it shows how inappropriately and incompetently can be a simple technical feature translated into political implications and how *technological radical uncertainty* can produce global panic just by discourse. With coming end of millennium some experts had started calling for a solution of upcoming glitch in computers called Y2K. The glitch was based on a problem that due to saving some

[6] Bruno Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory*, Clarendon Lectures in Management Studies (OUP Oxford, 2005); Bruno Latour, "On Recalling ANT," in *Actor Network Theory and after*, ed. John Hassard and John Law (Oxford: Blackwell and the Sociological Review, 1999), 15–25.

[7] Jasanoff, *States of Knowledge: The Co-Production of Science and Social Order*, 1.

memory, programmers decided somewhere in 60s to save only two digits of year after 1900. Change of the last digits in 1999 would than roll back all the computers to the year 1900. In fact, the glitch was easy to patch, known from 1979, but despite the knowledge some particular persons were astonishingly successful in sounding global alarm of upcoming collapse of digital society. False fears about Y2K led to investments in hundreds of billions in US dollars without a clear clue whether the investment had been worth of it despite of the fact that the experts working on the problem were claiming Y2K as a simply resolvable error.[8] However, the end of the millennium had looked like before the end of the world as panic millenarians would predict uncontrollable civilization collapse: *"At the end of the twentieth century, many software applications will stop working or create erroneous results when the year switches from 1999 to 2000… [D]ate sensitive embedded chips could (also) stop working… [These] embedded business systems control traffic lights, air traffic control, security systems, time clocks and hospital operating systems."*[9] In fact, nothing serious happened and media were immediately full of articles asking who had built this panic and finally made profit from it.

For example, Michael Hyatt wrote two alarming and seriously influencing books about Y2K called "The Y2K Personal Survival Guide"[10] or "The Millennium Bug"[11] and made apologies of false alarm later.[12] Y2K problem was an exemplary event how a spread of fear based on *technological radical uncertainty* is hard to stop despite all the arguments developed by people preparing software patches for the year turnover. Experts, which were working on the software glitch, were also experts that provided recommendation to governments; however, no government was prepared to take the situation easy and govern the situation in belief of appropriateness and had acted in a preventive manner close to a panic before upcoming cyber-armageddon.

[8] "Panic Postponed," *The Economist*, January 6, 2000, http://www.economist.com/node/327829.

[9] Edna Ferguson Reid, *Why 2K?—A Chronological Study of the (Y2K) Millen- Nium Bug: Why, When and How Did Y2K Become a Critical Issue for Businesses?* (Singapore: Universal, 1999).

[10] Michael S. Hyatt, *The Y2K Personal Survival Guide: Everything You Need to Know to Get from This Side of the Crisis to the Other* (Regnery Pub., 1999).

[11] Michael S. Hyatt, *The Millennium Bug: How to Survive the Coming Chaos* (Regnery, 1998).

[12] Apology of Michael Hyatt and lots of other related information can be found in a plain text on a George Washington University website dedicated to Y2K problem written by Jim Lord, "My Y2K Apology," *GWU Website*, accessed August 17, 2015, http://www.gwu.edu/~y2k/categories/jimlord_apology.html.

The 1st January 2000 brought on the light the real implications as the event had arrived – no embedded chips stopped working and almost all related software was patched in time. When it comes to a possible cyber war, there is no such a judgment day, so the discourse of doom based on unsolvable uncertainty can blossom much more easily.[13] In situations when experts are under constant pressure during a crisis or in a situation that might precede a crisis, they might tend to produce results for policy makers in harsh; they might easily or be pushed to answer policy makers' fears by requested evidence. However, if there is no crisis, it is constructed as a constant state of unease based on politics of fear.[14] There are two identified transgresses, first, the fact that experts have to react quickly leads to taking knowledge from disciplines that are not their particular long-lasting background; they have to cross these disciplinary boundaries. Second, it is about the audiences receiving the expert crisis evaluation result, which understandably has to be brief to be understood by those who are not.[15] Uncertainty and related fear produce regulations that could preventively avoid possible future glitches, but limit our freedoms and deepen surveillance driven by imaginations calling for preventive countermeasures as well.

Governance of technology, and probably due to its inherent complexity and constant evolution of cyber-related communication technologies, seems to be inherently uncontrollable, unplanned and producing senseless sociotechnical dependencies and attributions. Especially because states will never possess power to control the process of technology development, e.g. cryptography technologies or communication protocols, they can play a role (maybe quite powerful in one or other way) in the web of decentralized technology government, fragmented responsibility and disconnected pools of knowledge. As the reaction of individuals or crypto-anarchist groups will be a development of alternative protocols or cryptographic technologies. For example, on 9th December 2014 Stockholm police raided a data center and shutdown The Pirate Bay. The result was a reaction of its current administrators (authors are in prison) leading to

[13] Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2012).

[14] Ruth Wodak, *The Politics of Fear* (SAGE Publications, 2015).

[15] Helga Nowotny, "Democratising Expertise and Socially Robust Knowledge," *Science and Public Policy*, 2003, doi:10.3152/147154303781780461.

complete decentralization of their database and redeveloping the architecture in a way to be completely resilient, saved in an international cloud rather than on one server and thus untouchable by governmental authorities (see page 138). Since then Pirate Bay has experienced some glitches, but is still on (tested on August 2015, May 2016, August 2016).

These actions of governments will much more probably lead to a completely ungovernable cyber realm where interactions between states, network assemblages and individuals independently contribute to sociotechnical change as separate actors and networks; to a self-governed world where security is not provided by states only and their regulation by law (we do not need to go so far to remember fight between sharing MP3 files and global music publishers BMG and EMI resulting in a legal digital distribution and streaming established by global corporations, not governments). These self-governed worlds already exist and will probably evolve to a form of a cyber realm where extremely specific knowledge creates perfectly detached and undetectable networks such as TOR or so called Dark Net, which is not visible to those who have not created it, but can be used for creators' own purposes against the outer world or being so decentralized that just habits of people give birth to their existence. Somebody created BitCoin that is constantly under pressure to become regulated by authorities,[16] but it will be much more probably the authorities who will have to change itself in order to govern these developments. The policy of consent between liberal nation states and the decentralized networks of geeks is my ending policy position I recommend. Block Chain, on which Bitcoin is based (see page 128), would serve as one empirical example, how such trust machine based on self-governance of technology is not utopia, but reality biting governments and their ability and credibility to govern technology development related to cyberspace.

The dissertation, is divided into the three parts, the first concerning theoretical and methodological approach and the following two parts, the empirical and the discussion.

[16] Nicholas A Plassaras, "Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF," *Chicago Journal of International Law* 14 (2013): 377–407.

In the theoretical chapter, I am reviewing several key literatures in critical studies strictly focused on cyber security or on policy of exceptional situations such as catastrophes. I am moving forward to discuss the social constructivism and how it is reflected in studies of cyber security. The social constructivism is put alongside with the question of technology governance and the section of the Science and Technology Studies (STS), particularly the discipline of STS governance to link these thoughts to the question how a relevant knowledge is formed for decision making over national security. This moment gives me the opportunity to discuss what kinds and types of expertise policy makers can expect and how the distinctive expertise form. Following this theoretical anchorage, I am moving forward prevalently with the already mentioned approach Archaeology of Knowledge written by Michel Foucault, which is used as an attuning tool of the reader to the questions above that are discussed using specific lens in the empirical part. The final sub-chapter discusses what particular actors operate in cyberspace and how I am perceiving them. This part I recognize as a very important, but still with a function of attuning the reader. Discussions over crime, espionage, cyber war etc. are much easier when we have a table of actors, their objectives, their methods and the implications of their actions. Hence, I am putting emphasis on this sub-chapter that should introduce the reader to the following empirical part.

In the empirical part is about the three discourses, which I already discussed above. Each discourse is approached differently. The aim is to study each culturally influenced environment in its specifics. Geeks are studied in the light of cyberpunk subculture as they are without doubt significantly influenced by the way of thinking about near dystopian future. This dystopian environment is explained using the philosophical perspective of Baudrillard who was not a cyberpunk writer, but the cyberpunk writers were influenced by Baudrillard's visions. The whole first chapter in this part about geeks serve as a source of semiosis, ideology and culture that bound the further worlds. Crime and espionage are producing enormous amount of evidence as the operations seeking national secrets and operations focused on bank frauds are visible everywhere; however, even mere citizens are becoming victims of these operations when their computers are found locked by ransomware. I am discussing what options are available for the enforcement agencies and what the geek community can provide the citizen to preserve

personal privacy and security. The fact that law enforcement agencies do not have too many options leads to a situation that states might have interests to construct threat that is only solvable by a sovereign. This move is the core aim of the third chapter of the empirical part that studies the discourse about the cyber war and related moves of institutions to preserve security against such threats.

The final discussion part analyses the implications of the birth of cyber as a national security agenda. I am introducing new theoretical perspectives from the writings of Bruno Latour, which are not discussed earlier to preserve the comprehensible flow of the argumentation. However, the final part is crucial in explaining the unintended implications of hypersecuritization policy, which might lead into seriously undesirable state of international security; a state, which will not be an overemphasized imagination, but a real dystopia of ungovernable chaos if liberal democratic nation states do not change their approach to the management of possible catastrophes.

THEORETICAL AND METHODOLOGICAL APPROACH

1. RESEARCH QUESTIONS

I am convinced that it is not desirable to take a theoretical approach that will precisely fit in the way how events and political dynamics are going to be interpreted or to take strictly a particular epistemological approach which will most likely work to support universality in social science.[17] Based on the criticism of emerging sects in international relations studies, the following research is taking an approach that made the best sense to me[18] to attune you[19] to a particular phenomenon; to take you through the path of specific observations how certain thinking over the particular phenomenon might have probably developed and to help us better understand the dynamics behind the emergence of new national security topic. I am not trying to develop a verifiable perspective, which some positivists would recommend, but rather using different theories, approaches and methods I am trying in combination to *better understand* and consequently unveil the *knowledge development* behind the security imaginations and discuss possible implications to the current, especially liberal democratic, world politics.

The dissertation has an ambition to answer or to elucidate a potential answer to the following research questions – ***why are states so concerned in cyber security? What drives certain policy experts to reproduce imaginative discourse? Where is the cultural source of dystopian imaginations concerning global cyber apocalypse? How these imaginations influence national cyber security perspective? And what might be the consequences to the international security?***

[17] David a. Lake, "Why 'isms' Are Evil: Theory, Epistemology, and Academic Sects as Impediments to Understanding and Progress," *International Studies Quarterly* 55, no. 2 (2011): 465–80, doi:10.1111/j.1468-2478.2011.00661.x.

[18] Ibid., 447.

[19] Thierry Balzacq, "The Three Faces of Securitization: Political Agency, Audience and Context," *European Journal of International Relations* 11, no. 2 (2005): 171–201, doi:10.1177/1354066105052960.

2. LITERATURE REVIEW ON CRITICAL CYBER SECURITY STUDIES

The current critical literature on cyber security politics can be divided into three branches. First, the social constructivist approach of international relations analysis, in particular the securitization theory known as Copenhagen school. Second, the post-structuralist school that works broadly with the discourse analysis and which has done respectable job on analysis of international terrorism that is subsequently applied on cyber-terrorism. Third, a combination which incline to post-structuralist works analyzing imaginations, their connection to the threat construction based on potentialities and pre-emptive reaction that builds on speculations. I am listing inspirational writings that significantly influenced my thinking in order to use them in further analysis; it is not meant to be extensive literature review on critical studies in cyber security.

The social construction theory has its roots in the sociology of 60s, when Peter Berger and Thomas Luckmann wrote their famous book The Social Construction of Social Reality,[20] which was later applied to the theory of international relations prevalently by Alexander Wendt[21] claiming that agent and structure around is mutually constituted. An idea, that is directly based on previous sociological writings of Anthony Giddens on structuration theory,[22] in which Giddens introduce the idea that nothing in a social reality can exist without a subjective influence and thus everything around is mutually socially constructed. Berger and Luckmann came up with the idea that the social reality is subjectively internalized based on concepts people construct during interactions resulting in institutional behavior. Wendt then applied this idea further to the international relations theory arguing against realist thought of systemic environment between states. In his very direct criticism of neorealists was that the *Anarchy is What States Make of It.*[23] It is a mind that construct the reality or explanations of the reality that

[20] Peter L Berger and Thomas Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*, *New York*, vol. First Irvi, 1966, doi:10.2307/323448.

[21] Alexander Wendt, "The Agent-Structure Problem in International Relations Theory," *International Organization* 41, no. 3 (1987): 335–70, http://journals.cambridge.org/production/action/cjoGetFulltext?fulltextid=4309572.

[22] Anthony Giddens, *The Constitution of Society* (Polity Press, 1984).

[23] Alexander Wendt, "Anarchy Is What States Make of It: The Social Construction of Power Politics," *International Organization* 46, no. 02 (March 1992): 391, doi:10.1017/S0020818300027764.

is familiar to us. Following these ideas, the Copenhagen school team led by Barry Buzan then established a new methodological framework how to study security dynamics in international relations, which quickly became a famous method in critical studies of international relations for further applications known under the key term of *securitization – or a theory of securitization*.[24] It studies how a particular concept used in depicting insecurity emerged: *"Thus the exact definition and criteria of securitization is constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects."*[25] The concepts are studied in the perspective how they have been brought to the political reality within the national security discourse, which is finally exactly the point of my further research, which I am methodologically enriching using method of Michel Foucault on discourse analysis explained in his book The Archaeology of Knowledge[26] (to be discussed in detail below).

When the cyber threats have become a topic, some scholars used Copenhagen school to establish some particular key concepts related to the new security topic.[27] Helen Nissenbaum and Lene Hansen did a respectful work when they applied Copenhagen school on cyber threats. Through application of the concept *securitization* on cyber threats they have developed three different types of securitization. *Hypersecuritization*, *everyday practices* and *technifications*. Under the concept of *hypersecuritization* they understand *"large-scale instantaneous cascading disaster scenarios"*, whereas the concept of *everyday practices* is securitizing practices of every single day to a citizen as full of threats one has to face; finally, under the concept of *technifications* they introduce the idea that politically unbound expert perspectives are unquestionable and thus desirable. [28] I will use prevalently the first and the third concept in the following analysis.

Nissenbaum and Hansen paved the road for further critical analysis of cyber security. However, this road is significantly inhabited by Myriam Dunn Cavelty who has

[24] Barry Buzan et al., *Security: A New Framework for Analysis*, *National Bureau of Economic Research Working Paper Series* (Lynne Rienner Publishers, 1998).

[25] Ibid., 25.

[26] Michel Foucault, *The Archeology of Knowledge* (London: Tavistock, 1972), doi:10.1177/053901847000900108.

[27] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53, no. 4 (2009): 1155–75, doi:10.1111/j.1468-2478.2009.00572.x.

[28] Ibid., 1157.

started studying cyber security from a critical viewpoint in the first half of 2000s by her writing on socio-political dimensions on critical infrastructure protection,[29] in which she is criticizing the approach of computer experts on critical infrastructure protection which was later conceptualized by Hansen and Nissenbaum as a security modality of *technifications.* The detachment between technical oriented experts and policy makers has been a hot topic since then and is one of the principal questions in the discipline of Science and Security Studies. Later on, Myriam Dunn Cavelty used the Copenhagen school several times in assessing the establishment of possible cyber terrorism, in which she used also the framing method to depict the establishment of cyber terrorism imaginary. She argued that certain stories helped to establish urgency in order to activate government officials.[30] Myriam continued her research on this topic and argued that the threat representations in these stories even influences the everyday practices of cyber security experts as the threat discourse reiterated its stories.[31]

As the world has convinced itself that we are slowly moving from the industrial age to the information age, the stories known from the modernization of industrial capacity found their metaphorical way to the information capability modernization causing an effect in giving the content to these metaphors. However, information age in contrast to the industrial age seems to produce much more complex and hard-to-comprehend knowledge giving the metaphors more space to engulf more content and thus more stories or shocking narratives.[32] The content thus can be easily inspired by the science fiction literature (or the one, which is not far away from science fiction, but tend to develop future imaginations on seriously approached fiction) and as Lawson argues, that popular literature produce military imaginations of future network-centric warfare[33]

[29] Myriam Dunn, "The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)," *International Journal of Critical Infrastructures* 1, no. 2/3 (2005): 258, doi:10.1504/IJCIS.2005.006122.

[30] Myriam Dunn Cavelty, "Cyber-Terror—looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate," *Journal of Information Technology & Politics* 4, no. 1 (2008): 19–36, doi:10.1300/J516v04n01_03.

[31] Myriam Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review* 15, no. 1 (2013): 105–22, doi:10.1111/misr.12023.

[32] Antoine Bousquet and Simon Curtis, "Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations," *Cambridge Review of International Affairs* 24, no. 1 (2011): 43–62, doi:10.1080/09557571.2011.558054.

[33] Sean Lawson, "Articulation, Antagonism, and Intercalation in Western Military Imaginaries," *Security Dialogue* 42, no. 1 (2011): 39–56, doi:10.1177/0967010610393775.

which are for example based on (inspirational, but certainly very fictional) writings such as Alvin and Heidi Toffler.[34] Military officials then produce ideas that the complexity and self-organizing manner of the networks and the technology that embrace it calls the military complex to react and alter itself into a complex adaptive system.[35] One of such adaptation is a strategy in which *"deterrence now has to be based on prevention."*[36] As Lawson puts it, it is important to take into consideration formal military theory when assessing the sources of these imaginaries as the military officials usually produce these imaginaries on their personal experience from a conventional warfare.[37] Approaching the so called new domain of cyberspace in a comparable manner to the four others (land, air, sea, space) is generating a self-fulfilling prophecy that strategies from other domains can be applied easily and that the new domain provides the same security dynamics or, as cyberspace is hard to grasp, that the threat can be even bigger. In that perspective, Gartzke wrote a critical article in which he analyses the differences of possible cyber war and a conventional war. Gartzke argues similarly that the imaginations of military officials are motivating policy makers to establish particular policies, but if grand strategies are read appropriately, these imaginations cannot survive face to face to the emerging experience with ongoing cyber-attacks.[38] However, the national security policy is still inspired with such imaginations based on speculative potentialities based on technical possibilities that in the end influence decision making and thus have impact on the politics.

In the comparable manner, but taking more rational perspective to the analysis, another very influential scholar analyzed cyber war from the perspective of grand strategy of Carl von Clausewitz. Thomas Rid published his idea that Cyber War Will Not Take Place several times. First, as a short article in Foreign Policy magazine,[39] then as a

[34] Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston, MA: Little Brown & Co., 1993).

[35] Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare : Its Origin and Future," *US Naval Institute Proceedings*, no. January (1998): 28–35.

[36] Arthur K. Cebrowski, "The State of Transformation. Presentation to Center for Naval Analyses on 20th November in Crystal City," 2002.

[37] Lawson, "Articulation, Antagonism, and Intercalation in Western Military Imaginaries."

[38] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (2013): 41–73, http://belfercenter.ksg.harvard.edu/files/IS3802_pp041-073.pdf.

[39] Thomas Rid, "Think Again: Cyberwar," 2012, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=0,0.

scientific article in Journal of Strategic Studies[40] and then as a book, in which he uses particular events in history to underscore his argumentation.[41] Rid argues that cyber war is a misnomer, because what we observe around are events of *sabotage, propaganda and espionage.* Cyber war will not take place, as he claims, because war must be lethal, instrumental and has political means. According to Rid, cyber war is not violent as we have not observed any casualties, it is not instrumental because we can hardly attribute it to a state and it does not possess political means as there is not observable *continuation of politics by other means* (classical Clausewitz quotation). Rid received a broad criticism, for example from a John Stone,[42] who argued for example with Rid's very problematic conceptualization of violence, which is very inconsistent in strategic thought according to Stone; for example Hannah Arendt understands violence as a "power of a man over a man", which does not need to include lethality.[43] Cyber war thus can be violent, but does not need to be lethal as conventional war. That violence is enough to call it war. Bernard Brodie argues in context with Cold War that the principal problem of strategists is a question "will the idea work"?[44] In that perspective, we can be more reserved in possible causalities in cyber war as Rid inspire us to be vigilant here, but the question whether a *continuation of politics by other means* is not fulfilled here is – at least to my opinion – unanswered. I see this problem as an absence of appropriate concepts rather than a game whether cyber war is real strategic concern.

While Erik Gartzke is taking down these imaginations by approaching grand strategies with cool head, Thomas Rid is proposing new perspective how to perceive cyber war using grand strategies. These works are rare, but significantly contributed to the debate despite some of their debatable parts as in the case with violence in Rid's case. Much more usual are works that focus on the opposite strategy of cyber war conceptualization and thus perception of cyber security dimensions. For example, whilst an influential policy analyst Jason Healey from Atlantic Council in Washington D.C.

[40] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (April 20, 2012): 5–32.
[41] Thomas Rid, *Cyber War Will Not Take Place* (Hurst, 2013).
[42] John Stone, "Cyber War Will Take Place!," *Journal of Strategic Studies* 36, no. 1 (November 10, 2013): 101–8, doi:10.1080/01402390.2012.730485.
[43] Hannah Arendt, "On Violence," in *Crises of the Republic* (San Diego, New York, London: Harcourt Brace Jovanovich, 1972), 105–98.
[44] Bernard Brodie, *War and Politics* (London: Cassell, 1972), 452.

contributed with an interesting categorization of responsibility scale for a nation state in a case of a cyber-attack,[45] he has also been productive in the application of military strategies into cyberspace.[46] It can be understood as a very insightful but in fact it is exactly the military driven imagination that was criticized by Lawson. Healey argues in the end of his contribution that *"In the traditional view of warfare, it is entirely possible, even probable, that large-scale warfare in cyberspace would follow the same model—a series of connected high-speed 'dogfights' strung together into operations which are in turn, part of larger campaigns."*[47] Such approach is exactly what Gartzke and other criticize. Moreover, to demonstrate that link Healey created analogue models called Cyber Pearl Harbor, Cyber 9/11. This one and a row of other attempts to apply experience from other domains and rigidly explain the future of cyber security in pure speculative potentialities are not rare. Such an analysis of speculative scenarios is usually in critical studies called "cyber doom scenarios".[48] Lawson criticized this boom of doom scenarios after the Estonia 2007 cyber-attack couple of years ago as being totally incorrect and urges to follow strategy of more decentralized, resilient and self-organized technological systems before the military put through the idea of fortification, centralization and control-oriented policy in order to develop the suggested "internet control switch".[49]

On the opposite side to Healey stand scholars such as Erik Gartzke who criticize the direct applications as being more imaginations based on potentialities rather than a real and imminent threat. Gartzke argues that there are plenty of moments in the world, in which people can attack each other, but they do not and thus there is no reason to think they will in cyberspace.[50] And if they do, it is highly possible that attacks causing blackout will be easily repaired and energy quickly restarted.[51] This is something what in fact

[45] Jason Healey, "The Spectrum of National Responsibility for Cyberattacks," *Brown Journal of World Affairs* 18 (2011): 57–70.

[46] Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," in *Proceedings of a Workshop on Deterring CyberAttacks : Informing Strategies and Developing Options for U. S. Policy*, ed. John D. Steinbruner (Washington, DC, USA: National Academies Press, 2010).

[47] Ibid., 97.

[48] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London and New York: Taylor & Francis, 2007).

[49] S Lawson, "BEYOND CYBER-DOOM: Cyberattack Scenarios and the Evidence of History," *Mercatus Center George Mason University*, 2011, http://www.voafanti.com/gate/big5/mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf.

[50] Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," 52.

[51] Ibid., 57.

happened in December 2015 in Ukraine two years after Gartzke wrote his article and is the point of my further analysis in the empirical part. Gartzke also shifting upside down the perspective of super-empowering of non-state actors in cyberspace by claiming that particularly militarily powerful states will be able to use cyber-attacks in continuation of their policy as the military power serves as a deterrent[52] and that cyber-attacks are extremely unlikely to be decisive.[53]

If I come back to imaginations, they have been very inspirationally analyzed by Robert Kaiser in the article Birth of Cyber War.[54] Kaiser put together three elements: an initial event, a global respect to expertise of one state and implications to the international regime. He analyzes using a post-structural perspective the event of Estonia 2007, but also moved forward to depict how such an event bended perspective on expertise of Estonian cyber experts. It was the event itself, which is the argument why Estonian possess so much expert knowledge. Moreover, selected experts from Estonia were invited to shape European cyber security strategy and thus we can conclude how one event constructed expertise that in the end institutionalized power structures on the international level by the deployment of NATO Cooperative Cyber Defense Center of Excellence. Kaiser argues that cyber war lives in a present day as a premediation that imagines multiple futures, which are in fact living in present as current potentialities against which we must be prepared. Here we can remind the point discussed earlier how military officials tend to focus on potentialities in cyber defense and Kaiser sees these officials in an enclosed circle of knowledge where ominous chains of citational practices produce discourse of unquestionable truth.[55] Kaiser's article contributes to the debate by looking back in recent history using Foucauldian perspective and doing clear post-structuralist analysis of the current cyber war image.

A different approach was taken by Claudia Aradau and Rens van Munster in their book Politics of Catastrophe which is a very specific contribution to the post-structuralist

[52] Ibid., 63.
[53] Ibid., 68.
[54] Robert Kaiser, "The Birth of Cyberwar," *Political Geography* 46 (2015): 11–20.
[55] Ibid., 17.

thought.[56] They approach catastrophes as an event being out of the limit of our knowledge and governmental practice and ask a question how can we be prepared on 'known unknowns' and 'unknown unknowns',[57] which they drew on Ulrich Beck's theorization of uncertainty.[58] According to Aradau and Munster *"imagination creates the future as a new epistemic 'reality' by mediating between the senses and understanding,"*[59] towards policy of normalized reaction. The point is not to produce politics of fear, but rather through politics of catastrophe[60] be prepared on events on which we react with normalized reactions. Possessing knowledge is what dissolve the catastrophe as the event is anticipated, thus they talk about possible anticipator regime created through fear and pleasure. Fear, that reacts on unknowns and pleasures produced through theatrical exercises producing knowns.[61] Under that perspective, imaginations are perceived as a needed preventive and predictive models[62] and thus even science fiction writers aside the governmental officials is understood as "*indispensable to the pursuit of knowledge and the problematization of the unknown*."[63] However, as I will show later it is hard to balance between dark dystopian world on the threshold of apocalypse and imaginations created in intelligence community providing policy makers with scenarios on which they should react, appropriately.

Another perspective has been provided by Tim Stevens, who understands discourses regarding cyber war as *catastrophic apocalypticism*.[64] As Stevens perceive the concept of cyber war from a post-structuralist perspective, his approach is analyzing our perception of reality in a development of stories in time. He argues that *"discourses of strategic cyber war are contingent upon an apocalyptic temporality that is itself an expression of postmodernity."*[65] According to Stevens, the *catastrophic apocalypticism* is giving opportunities of national security to expand its apparatus. These ideas are clearly close to thoughts of Michel Foucault and his materialization of power emanating from

[56] Aradau and Munster, *Politics of Catastrophe*.
[57] Ibid., 6–7.
[58] Ulrich Beck, "Risk Society: Towards a New Modernity" (London: SAGE, 1992).
[59] Aradau and Munster, *Politics of Catastrophe*, 84.
[60] Ibid., 112–113.
[61] Ibid., 85.
[62] Ibid., 68.
[63] Ibid., 69.
[64] Tim Stevens, "Apocalyptic Visions : Cyber War and the Politics of Time," *Available at SSRN*, 2013, 1–28, doi:10.2139/ssrn.2256370.
[65] Ibid., 2.

discursive practices, which I am using later in my analysis. Stevens approached a bit differently the imaginations of catastrophe than Aradau, he works with imaginations as to be apocalyptic future rather than an inspiration toward normalization of reactions. However, Stevens depicts apocalypse as dystopian future, but not as an apocalyptic end, rather as a beginning; moreover, apocalypse can be understood as a belief in possible transformation of human condition, thus even the utopist war on terror seeking the world without terrorism is similar to the apocalyptic visions of Jihadist in world-size Caliphate.[66] Stevens approaches the problem with balance; on the one hand the apocalyptic visions are depicting dystopian future, on the other hand as *cyber war is always coming* we should keep listening to these imaginations in order to not let these risks fulfill. Stevens has elaborated his thought on temporality in cyber politics further in his recent book,[67] in which he elaborated more visibly on ideas of Aradau and Munster by using the concept of inhabiting the future. As Aradau and Munster talked about the theatrical exercises, Stevens shows how the exercises are hard to communicate to the public due to the epistemological uncertainty and that these activities "serve to generalize an aesthetic of future cyber disruption."[68] The point of the exercises is to inhabit the space in order to show control over possible catastrophes despite the low probability of experiencing same scenario in real cyber-attack. And as the flow of history is inexorable things went differently and the Snowden revelations showed the extent of cyberspace inhabitation in different light.

The next important contribution to the critical perception that influenced significantly further analysis comes from Myriam Dunn Cavelty. The short paper presented at the CyCon conference in Estonia divided current security discourses into three branches: technical, crime/espionage and national defense.[69] I am using this division to analyze each discourse in a separate chapter. The point of Myriam is that each group of people approach the threat differently. She argues that a glitch in the system for a geek is a concern to national security for a governmental official. However, the

[66] Ibid., 8–9.
[67] Tim Stevens, *Cyber Security and the Politics of Time* (Cambridge University Press, 2015).
[68] Ibid., 160.
[69] Myriam Dunn Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better," in *4th International Conference on Cyber Conflict*, ed. Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (Tallin: NATO CCD COE, 2012), 141–53.

conclusion from such a misinterpretation of technical inequalities in the system draws the idea that the potentialities are deduced from a vast variety of unimportant glitches, while the trouble can be completely elsewhere. As Myriam puts it: "*Using too many resources for high impact, low probability events – and therefore having less resources for the low to middle impact and high probability events – does not make sense, neither politically, nor strategically and certainly not when applying a cost-benefit logic",* we should ourselves rather point to the question *"who has the interest and the capability to attack us and why would they?"*[70]

Rod Deibert in a reaction to the Snowden revelations[71] reminds us that the actors in cyberspace are various, that inhabitation of cyberspace by states in order to take control of vast environment does not need to be the desirable outcome and that the idea of spreading norm of free speech by Western world is jeopardized two folds. First, by the West through its unveiled massive surveillance hydra, however, second, by the new South with its authoritarians regimes, which never asked a question whether to use the internet for social control or not and which certainly and openly regulate internet in state's interest. Nevertheless, according to Deibert, the mixture of national security expectations and business interests opens a very specific *unknown future* that is currently invisible, but already spills tensions between both.[72] However, these two are not the only actors in cyberspace and as both Aradau and Stevens recommend, we should take some imaginations as a needed precursor of future development. Such a situation awaits analysis from a perspective of the related actors and my quest here is to study the cultural roots of several actors through discourse analysis to depict that not only states (both democratic and authoritarian) and corporations are here trying to shape the cyberspace to their advantage, but that also less visible actors, non-state actors, depicted by states as cyber terrorists, do not need to take down national critical infrastructure necessarily, but can still successfully shape cyberspace to their advantage.

As Cox puts it, there are two distinct approaches, a critical approach of current state focused on its historical evolution and a problem-solving one focused on an analysis

[70] Ibid., 150–151.
[71] Ron Deibert, "The Geopolitics of Cyberspace after Snowden," *Current History* 114, no. 768 (2015): 9–15.
[72] Ibid., 12.

how the current institutional architecture should work smoothly.[73] Despite the fact that I am trying to provide a reader with a particular insight which should help to narrow the current cyber security policy with cool head, my central aim is exactly the first one, a critical approach describing the historical evolution, the genealogy of current state. The text is not trying to solve how particular institutions should operate, but try to explain – and thus understand – how the current policy architecture to solve cyber security issues came about and what does it mean for the world politics. I am rather providing a specific reading with possible implications of current policy that produce *hypersecuritization* effects. To be concrete, I am taking exactly the perspective about security as Booth: *"security is what we make of it. It is an epiphenomenon intersubjectively created. Different worldviews and discourses about politics deliver different views and discourses about security. New thinking about security is not simply a matter of broadening the subject matter."*[74]

Main argument of this research is based on a conviction that the process of increasing of technological complexity enlarges *radical uncertainty* of policy and decision makers that consequently causes construction of an imaginative world of insecurity in cyberspace by performative materialization through securitization discourse. These imaginations are not necessarily desirable in the perspective of Clauda Aradau approach, but they rather produce thoughts of upcoming apocalypse. Such a permanent state of exception gives enormous power to people, who tend to solve all the glitches in the system preventively and thus produce a significant reaction in form of a growing resistance within ultra-libertarian world and crypto-anarchist movement. The research questions delve from this concern and are aimed on unveiling securitization processes by discursive materialization of birth of cyber security agenda as a national security concern.

The process of materialization might be an opportunity to install new institutions, establish new power structures and introduce new agenda that might in the future alter to something relatively different in the domain of cyber security, but that is exactly not

[73] Robert W Cox, "Social Forces, States and World Orders: Beyond International Relations Theory," *Millenium* 10, no. 2 (1981): 129.

[74] Ken Booth, "Security and Self: Reflections of a Fallen Realist," in *Critical Security Studies: Concepts and Cases*, ed. Keith C. Krause and Michael C. Williams, 1997.

my concern here. I am not going to judge that moves; my objectives are to uncover, unveil or unhide the origins of such process using the genealogical approach to discourse analysis. One may argue, that a causal relation can be delved from such a research. I am not doing that deliberately and if you find such a discussion inside, please understand it as a comment, which I could not be silent about. The core of the research focuses on a discourse formation, its co-production, consequent power materialization and finally the debate of its possible implications on world politics.

I am using one prevalent epistemological approach based on Foucault's method of knowledge production. It is used in a combination of concepts from Science and Technology Studies and concepts produced by experts in cyber security. The aim is to unveil the dynamics between cyber-technologically related knowledge production for policy makers using concepts and perspectives used in science and technology studies. This approach enables us to see how threat politics concerning cyber security have emerged, how it is divided into different currents concerned with different problems and why the technology driven *technological radical uncertainty* is causing production of new institutions with specific technology oriented expertise to solve the emerging, constructed and materialized problems and how the institutions in return tend to preserve their newly adopted power based on imaginative threats, in the discursive fields of presence and enclosed discourse dimensions.

3. CONSTRUCTION OF SECURITY CRISES UNDER TECHNOLOGICAL RADICAL UNCERTAINTY

3.1. Theoretical and conceptual framework from STS

Science and technology studies is a discipline closely related to centuries or millennia long debate concerning philosophy of science. Its relation to philosophy of science is the assessment how particular knowledge has been produced within particular scientific community. The three steps in modern historical development of philosophy of science in 20th Century can be considered important. First, the logical positivism, which have its roots in Descart's call for rationalism. Second, the Thomas Kuhn's contribution with paradigms. Third, the contribution of social constructivists.

Logical positivism emerged in 20s within the Vienna Circle and Berlin Society for Empirical Philosophy.[75] Their approach to science development was strictly oriented to testable statements; all interpretations are rejected from the scientific knowledge development. They also aspired to reduce math into a logical symbolism as in the case of Bertrand Russel.[76] The only cognitively meaningful knowledge was by the logical positivist the one, which was verifiable. Even the scientific language was intended to be developed into a logical syntax that can develop a scientific theory, but the theory needed to be verified by logical or empirical confirmation to develop the truth. Early sociology was significantly influenced by this way of thinking. We can rightly assume that Comte's approach was a product of the positivist school call and this perspective had last for decades. However, Durkheim's reaction to Comte's positivism was that we study social phenomena sui generis, as *social facts* that are consequences of human interaction, nevertheless hardly influenced by human action or agency.[77] Ludwik Fleck was one of the critics of logical positivism who built his ideas on Emile Durkheim's. He focused on theorization of *scientific facts* production and came up with the idea that interactions between people lead into a *thought collective,* which is a predecessor to theory-ladenness

[75] The Prehistory of Science and Technology Studies In Serge Sismondo, *An Introduction to Science and Technology Studies* (Wiley-Blackwell, 2010).
[76] Bertrand Russell, *Mysticism and Logic: And Other Essays* (Longmans, Green and Company, 1919).
[77] Emile Durkheim, *The Rules of Sociological Method* (New York: Free Press, 1950).

of observations and thus later more radical to positivism, the social construction.[78] Positivism due to the criticism it received, started to be called later a naïve empiricism. However, the mission of STS has been since the beginning to *renew the empiricism*[79] not to deny science as it positivists have tended to argue since the science wars.

While positivists were looking for a verifiable method that unveils truth, Kuhn, influenced by Ludwik Fleck, came up in 60s with a revolutionary perspective of paradigm as a response to logical positivism.[80] In his thought, the efforts to develop a scientific knowledge is dependent on a viewpoint of particular researcher. The research then develop in iterations as the researcher is adding partial results to the method in order to scale the knowledge in a pile. In a puzzle solving research, researchers conduct normal science, while in developing different paradigm to the examined phenomena researches conduct a revolutionary science, which should be to Kuhn the most desired approach of any researcher. During the process of a research and forthcoming development of a paradigm, researchers have to critically approach each other to be able to develop a new perspective, a new paradigm, a new coherent body of knowledge. Kuhn was revolutionary in his thinking as he provided a perspective that even different streams within philosophy of science do not need to be in conflict, but just provide different coherent bodies of knowledge that works in their own enclosed worlds. If researchers tend to accept these boundaries, they produce knowledge within the particular paradigm, whereas the revolutionary researchers topple down these boundaries to develop new methods leading to new knowledge, to new paradigms, to new bodies of coherent knowledge.

At the same decade, some new ideas emerged. The whole efforts in reconsidering the process of knowledge production was a reaction to the praise of technological innovation as the *right* policy in the Western liberal democracy development after the World War II, which won thanks to extremely successful technology innovation that led to the invention of nuclear bomb, but then sparked resistance in anti-nuclear and

[78] Sophia Roosth and Susan Silbey, "Science and Technology Studies: From Controversies to Posthumanist Social Theory," in *The New Blackwell Companion to Social Theory*, ed. Bryan S. Turner, 2009, 451–74.

[79] Bruno Latour, *Politics of Nature: How to Bring the Sciences Into Democracy* (Cambridge: Harvard University Press., 2004).

[80] Thomas Kuhn, *The Structure of Scientific Revolutions*, *The Philosophical Review*, 2nd ed., vol. II (Chicago: The University of Chicago Press, 1972), http://www.jstor.org/stable/2183664.

environmentalist movement of 60s. Moreover, the Vietnam War and the initial ethically questionable results of scientific discoveries stipulated firstly at the Asilomar Conference on Recombinant of DNA in 1975 led to normative regulation of research efforts. The chain of these events gave birth to the new interdisciplinary program later called Science and Technology Studies significantly influenced by social constructivist thought. The initial position was that social forces does not constitute the context, but also content of science.[81] Later on, scholars added to this claim that government policies and programs create expert authority to particular scientific disciplines.[82] These authorities then link themselves in epistemic authorities as the government backing gives them relevance to their knowledge as knowledge needed for the state governance. The knowledge of these authorities then become a *relevant knowledge*, relevant to the governance of particular issue than requires insight of experts.

Bruno Latour and Steve Wolgar came up with the idea that the production of scientific knowledge cannot be detached from social aspects. Each idea how to conduct particular research is preceded by developed methods that are clearly socially influenced, thus the results must be socially constructed as the social component played a crucial role.[83] As the Kuhn's book on scientific revolutions was a response to the positivism in science, the constructivist move was as well. Steve Woolgar after a decade of debates about social construction of science and technology that the knowledge produced by scientists is simply a *"contingent product of various social, cultural and historical processes"*[84] added a reflexive argument to the debate that even the sociology of scientific knowledge is a social construct itself as it is produced purely by social and cultural processes.[85] As Knorr-Cetina argued, scientific facts are a result of previously predicted solutions, as each researcher is forced to predict the results and possible impacts of the

[81] Roosth and Silbey, "Science and Technology Studies: From Controversies to Posthumanist Social Theory," 456.

[82] Brian Wynne, *Risk Management and Hazardous Waste: Implementation and the Dialectics of Credibility* (London: Springer-Verlag, 1987); Stephen Hilgartner, *Science on Stage: Expert Advice as Public Drama* (Stanford: Stanford University Press, 2000).

[83] Bruno Latour and Steve Woolgar, *Laboratory Life* (Princenton: Princeton University Press, 1979).

[84] K. D. Knorr-Cetina and M. J. Mulkay, *Observed: Perspectives on the Social Study of Science* (London: SAGE, 1983).

[85] Steve Woolgar, *Knowledge and Reflexivity: New Frontiers in the Sociology of Knowledge.* (Thousand Oaks, CA, US: Sage Publications Inc., 1988).

research in their research proposals in order to conform so called applicable science, thus they are forced to use analogical reasoning, they need to manipulate with concepts using analogy and metaphors[86] in order to conform their ideas to the expectations of the others, in this example to the research proposal evaluators. Researchers need to stay within the community of others, who understand their research. Scientific results are thus interpreted in the cultural cloud, they are culturally bounded.

However, later Latour added to this debate some influential ideas by saying that these *scientific facts* we are keenly looking for are becoming facts as much as they are socially accepted as facts by supporters in a network of actors to the threshold of the costs of a resistance.[87] As Latour combines natural and social conditions to the production of knowledge, the knowledge is then enabled or constrained by available material resources, technological preconditions, equipment, current technological and social knowledge, but finally also by our collaboration and also imagination. Additionally, if these scientific facts are socially constructed they should also be contestable, they should also have a value oriented assessment whether they are good or bad, thus they are not inevitable. As Hacking put it: *"we would be much better off if X were done away with, or at least radically transformed."*[88]

As the whole dissertation aims on a question how the uncertainty of new technology implications on society gave birth to cyber as a national security agenda, relation between technology and society, interpretation or social construction of its consequences and the dynamics how these consequences translate into decision making and establishment and legitimization of new institutions are in such research inevitable. These dynamics will be studied through lens of Bruno Latour and his concept of actor-network theory, which works with the idea of co-constructed sociotechnical world.[89] Similar concerns inspired scholars introducing concepts like *ethno-epistemic*

[86] K. D. Knorr-Cetina, *The Manufacture of Knowledge: An Essay on the Constructivist and Contextual Nature of Science* (Oxford: Pergamon Press, 1981).

[87] Bruno Latour, *Science in Action: How to Follow Scientists and Engineers Through Society* (Harvard University Press, 1987).

[88] Ian Hacking, *THE SOCIAL CONSTRUCTION OF WHAT ?* (Cambridge, Massachusetts and London, England: Harvard University Press, 1999), 6.

[89] Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory*.

assemblage,[90] where both, science and society, are co-constructed, or differently said mutually constituted. As ideas of scientists develop technologies that have in return effect on society itself, the society require additional way of its further development. Part of the society use technologies, another part is in the process of its development; both, users and developers, construe the way how they are used, understood, treated and finally governed. In car industry, switch from crash avoidance to crash survival by introducing e.g. air bags can be observed in cyber security as well. The switch from decades long perspective of firewalls and communication filtering to a call of cyber-attack resilient technologies development can be understood similarly; both examples show how the governance of technology development is decentralized[91] producing also a web of responsibility. In cyber security discourse, especially from the one on the national security level, policy makers argue that the responsibility has to be centralized into a state administration, a special institution that will provide relevant knowledge to those who operate critical systems. State then force operators to run particular technologies in accordance with standards and specific law that mark their systems as critical to the national security – the birth of the term *critical infrastructure*. All of this has been done over the whole world to different extents without witnessing serious attacks that have been disturbing critical infrastructures. There are examples on "huge" cyber-attack s on critical infrastructure, which will be discussed below, but majority of them could be avoided using very simple security measures such as multi-factor authentication as it was proved in the case of Ukrainian blackout.[92]

3.2. States, technology and the governability

Foucault, as will be shown below, is used as a theoretical-methodological lens how to perceive formation of discourse leading to the birth of cyber security agenda in discourse. Concepts used by the actors of discursive practices are analyzed and

[90] Alan Irwin and Mike Michael, *Science, Social Theory and Public Knowledge* (Maidenhead, U.K.: Open University Press, 2003).

[91] Jameson M. Wetmore, "Redefining Risks and Redistributing Responsibilities: Building Networks to Increase Automobile Safety," *Science, Technology, & Human Values* 29, no. 3 (2004): 377–405, doi:10.1177/0162243904264486.

[92] SANS ICS, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (SANS ICS, E-ISAC, Electricity Information and Analysis Center, 2016), https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

deconstructed in their historical evolution, however, particular conceptual framework is taken from sociological approach of science and technology (STS), especially sociology of its governance. In the end of the dissertation, I combine three pillars in the analysis. First, the sociology of technology governance as a conceptual framework that provides me with analytical tool in approaching, second, discourse creating construction of cyber security threats through radical technological uncertainty. The third pillar delves from the combination of radical technological uncertainty and the field of knowledge that we need to acquire in order to appropriately solve technical glitches, which plays crucial role in construction of threats when combined with social aspect, especially the presumptive (e.g. hackers') intentions based on opportunities. As the grasp or definition of needed corpus of knowledge is hard to achieve in general, focus is put on how the political agenda emerges from mixing of technical expertise with political implications in so called *proliferation of hybrids*.[93]

Latour meant with this concept a problem of knowledge *purification*, a detachment of cultural bounds from scientifically verifiable knowledge, the Latour's idea of renewing empiricism. In particular, as the deepening complexity and decentralization of knowledge in networks has become unbearable and still continue to deepen, it is impossible to purify the needed knowledge. The idea of compact knowledge regarding particular discipline has become utopia (I elaborate on this topic in detail in the chapter 1.1 Beliefs, understanding and the proliferation of hybrids on the page 232). As Ezrahi put it at the beginning of 90s, the employment of science and technology in support of liberal democracy has become debatable in the end of 20th century.[94] However, it was brave argumentation especially in the end of Iron Curtain that according to general consensus in the Eastern Europe felt thanks to pirated satellite reception of Western TV programs. On the other hand, Ezrahi argued similarly to Sheila Jasanoff that the complexity of technology development is deepening and thus the governance of science and technology development has become complicated. These ideas are far away from the ages of late 40s and early 50s, when the national US policy strongly focused on technology

[93] Bruno Latour, *We Have Never Been Modern* (Cambridge, Massachusetts: Harvard University Press, 1993).

[94] Yaron Ezrahi, *The Descent of Icarus: Science and the Transformation of Contemporary Democracy* (Cambridge: Harvard University Press, 1990).

development as national security policy in a reaction to the World War II. The belief into technology as a tool of liberal emancipation, as a component of mutual reinforcement between technology and democracy had been visible since president Thomas Jefferson to 50s,[95] and finally sparked even later during the recent Arab Spring, while five years after the revolts in North African countries we are reading opinions by influential thinker Anne Applebaum that social networks are doing to democracy exactly the opposite, a destruction.[96] As Sheila Jasanoff put it, science and technology permeate the culture and politics of modernity.[97]

The rapid evolvement of communication technology and its possible malign usage produces a shadow of uncertainty of its security implications. This process subsequently gave birth of constructed security discourse about the need to take an appropriate action by authorities. In this relation, the ideas of DARPA to let artificial intelligence solve glitches in software in order to preemptively close possible exploits that can be used in hostile actions[98] are becoming very questionable policy approach, because any artificial intelligence cannot make a choice of particular software glitches and mark them as exploits before knowing what are hostile intentions behind their exploitation, while intentions are – if taking the constructionist perspective – *what we make of it.* [99] Thus the implications are not inevitable, they are constructed as Latour showed us. Nonetheless, ideas that artificial intelligence can be used in automated defense against cyber-attacks has been forming recently.[100] Governance of science and technology development is not only about the bureaucracies that help scientists and technology researches progress in their research, it is also about taking control of science and technology development. However, as technologies, but also a significant part of current scientific research, are encompassed in private industries, the governance by elected government is becoming only harder. Moreover, not only centralized global corporations play a significant role in

[95] Richard M Merelman, "Technological Cultures and Liberal Democracy in the United States," *Science, Technology, & Human Values* 25, no. 2 (2000): 167–94, doi:10.1177/016224390002500202.

[96] Anne Applebaum, "Mark Zuckerberg Should Spend $45 Billion on Undoing Facebook's Damage to Democracies," *The Washington Post*, 2016, https://www.washingtonpost.com/opinions/mark-zuckerberg-could-spend-45-billion-on-undoing-facebooks-damage/2015/12/10/4b7d1ba0-9e91-11e5-a3c5-c77f2cc5a43c_story.html.

[97] Jasanoff, *States of Knowledge: The Co-Production of Science and Social Order*, 1.

[98] Mohit Kumar, "DARPA Challenges Hackers to Create Automated Hacking System — WIN $2 Million," *The Hacker News*, 2016, http://thehackernews.com/2016/07/hacking-artificial-intelligence.html.

[99] Booth, "Security and Self: Reflections of a Fallen Realist."

[100] Kalyan Veeramachaneni and Ignacio Arnaldo, "AI 2 : Training a Big Data Machine to Defend," n.d.

this process, but currently whole assemblages of actors, from states to corporations, from individuals to politically motivated hacking communities.

However as said, based on uncertainty of possible security implications emanating from such a decentralized development, the ineffectiveness of direct governmental involvement due to the technological characteristics and the current governance of cyberspace has led to the increasing significance of *decentralized networks of power assemblages*. Every attempt to regulate this decentralized network assemblage is easily answered by technology development that help people to override the regulation. As Sheila Jasanoff argues, nation states lost their *ability* and also their *credibility* to govern society in this technological labyrinth.[101] This uncertainty produce a political requirement that the technological knowledge has to be understood in particular social contexts – state related security, not citizen related security. However, exactly these contexts are in the cyber political discourse more replicated than unveiled or appropriately understood.

Intentions of states to govern cyberspace are twofold. Western-type democratic states have been anchoring their involvement by securitization of the issue that produces need to underpin its possible security implications; the consequences can be analyzed as a birth of a hypothetical cyber war[102] producing new institutions, new strategies, new concepts, new perceptions, new identities and representations all through adopting new discourse. The eastern states such as Russia or China tend to solve their inability to govern the cyberspace by adopting strict laws regulating its usage.[103] However, technological characteristics and the pace of the technological development of communication technologies will probably lead into deeper inability to control the flow of information and proliferation of what I call liberating technologies; the technological answer to regulations. As a reaction, some undemocratic countries, for example, started

[101] Sheila Jasanoff, *Designs on Nature: Science and Democracy in Europe and the United States* (New Jersey: Princeton University Press, 2005), doi:10.1163/156848409X12526657425587.

[102] Kaiser, "The Birth of Cyberwar."

[103] Assafa Endeshaw, "Internet Regulation in China: The Never-ending Cat and Mouse game1," *Information & Communications Technology Law* 13, no. 1 (2004): 41–57, doi:10.1080/1360083042000190634; A Murray, *The Regulation of Cyberspace: Control in the Online Environment* (Oxon: Taylor & Francis, 2007).

to pour disinformation into the political debate in newly studied hybrid warfare rather than keep a mere blocking of undesirable information.[104]

The ability to physically coerce internet users is far from real as famous arch-cyber-libertarian John Perry Barlow claimed in his Declaration of the Independence of the Cyberspace (to be analyzed bellow on the page 180).[105] However any attempt to govern cyberspace by law will strengthen the decentralized power assemblages. On the other hand, it is hard to claim that there will be one "cyberspace" soon. Libertarians and the movement of crypto-anarchists adoring Bitcoin as a tool of ultimate emancipation of humankind from states will certainly keep current pace of technologies development delivering them perfect anonymity while nation states will tend to develop technologies providing them security for critical infrastructures. This process cannot lead into one open global cyberspace and thus talking about a global network is becoming clumsy. It can be seen in the light of a process Sheila Jasanoff calls a *co-production* during which the social activities undertaken by people creates new technologies and vice versa.[106] When it comes to libertarians and crypto-anarchists, even these are in a bitter conflict. While libertarians see in liberation technologies an emancipation from states and raise of a global market created by global corporations that will easily respond to every human need in ultra-liberal and thus far-right perspective, the crypto-anarchists are probably more the authors of the technologies they intend to use to tackle down state system in order to establish paradise on Earth in the far-left perspective.

When Vannevar Bush was writing his famous paper[107] just after the World War II as a response to the president Roosevelt, technology brought us a victory over Nazism in the end of the War. Bush argued that the current capacity in science and technology development should be preserved, that government is the only one authority to direct a military research, that scientific research is the main driver for further wealth being of American people, the main driver of employment and for security. He certainly helped

[104] Nikola Schmidt, "Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War," *Defense and Strategy* 14, no. 2 (2014): 73–86, doi:10.3849/1802-7199.14.2014.02.073-086.

[105] Declaration made at Davos, Switzerland, 8 February 1996, available online at: https://projects.eff.org/~barlow/Declaration-Final.html

[106] Jasanoff, *States of Knowledge: The Co-Production of Science and Social Order*.

[107] Vannevar Bush, "Science - The Endless Fronties," *Transactions of the Kansas Academy of Science* 48, no. 3 (1945): 231–64.

rise of the optimism in the technology determinism as a driver of post-war national security policy, which was quickly spread to Europe through Marshall plan. However, during the time some had argued conversely. This opposite way of thinking is known today as pessimistic technology determinism. People thinking in this way are convinced that the technology development is moving society to a governable edge, which might cause more harm than benefit.[108] Since we have been witnessing increasing pace of globalization and a shift of scientific research from governments to the private sector, the capability to govern technology by governments is significantly decreasing. As Sheila Jasanoff put it: *"the 'old' politics of modernity—with its core values of rationality, objectivity, universalism, centralization, and efficiency—is confronting, and possibly yielding to, a 'new' politics of pluralism, localism, irreducible ambiguity, and aestheticism in matters of lifestyle and taste."*[109]

Current capability of governments to shape the direction of scientific research, to produce science related to the government policy is significantly decreased by the complexity of current scientific research and of course by privately driven research. Moreover, governments face a need to govern scientific development, which is ambiguous, hard to read and full of uncertainties when it comes to national security. Undoubtedly, adding artificial intelligence as another actor that is making decisions on the further technology development cannot consolidate the complexity of technology knowledge related to cyber security. It is clearly diverting the desired need of the complexity comprehensiveness out of human control, which should serve to human benefit – a concept that is certainly morally and culturally bounded. However, it is much more expected that governments will govern the development rather than shape the research policy according to public opinion, the distinction that can be described on the relation between concepts *scientific governance* and *scientific democracy*.[110]

It is much more easy to govern development of currently known impacts of new scientific discoveries rather than anticipate the consequences of basic or fundamental research. It is easier to develop artificial intelligence dealing with one problem, but based

[108] Lewis Mumford, *The Myth of the Machine: The Pentagon of Power* (Harcourt, Brace & World, 1970).
[109] Jasanoff, *Designs on Nature: Science and Democracy in Europe and the United States*, 14.
[110] Alan Irwin, "Constructing the Scientific Citizen: Science and Democracy in the Biosciences," *Public Understanding of Science* 10, no. 1 (2001): 1–18, doi:10.1088/0963-6625/10/1/301.

on deep learning, which provides AI seriously uncontrollable opportunities; moreover, when people are deliberately not willing to interfere in such deep learning. The proliferation of hybrids gains another impetus by adding a cultural layer of AI that is definitely *unknown unknown*.

3.1. Policy makers and the relevant knowledge

When the capability to govern sociotechnical development seems to be decentralized and ungovernable by central authority, a question, what is the relevant or practical knowledge for the central government and its policy to preserver citizens' security, arises. The discussion is seen e.g. in areas such as values and ethics and then impacts of one's punishment when it comes to a return of unethical or asocial behavior. Government and other institutions with related expertise like courts and their authorized experts or specially established research centers on crime usually draw the epistemological line about what is acceptable and what is not. Additionally, there are also examples in history where corporations, not only government, had conducted normative development efforts through a deliberate propaganda campaign to enforce norms that support their economic interests. An example would be a production of new term "jaywalking" from "jay" and "walking" in the 1920s by car manufacturers to definitively establish rights of cars to ride the streets and make victims of accidents being responsible for their deaths while they were *jaywalking*.[111] What kind of knowledge had been produced in that time? To what subject the knowledge was related? And who profited from the new norm establishment?

In sociotechnical areas *legitimate knowledge* is related to hereafter mentioned concept of *boundary work*[112] where the idea of production of a *good science* can be found and thus the particular actor is given with a legitimacy to interpret, manipulate, evaluate, reproduce and implement knowledge on solutions of problems, which might

[111] Aidan Lewis, "Jaywalking: How the Car Industry Outlawed Crossing the Road," *BBC*, February 12, 2014, http://www.bbc.com/news/magazine-26073797; Joseph Stromberg, "The Forgotten History of How Automakers Invented the Crime Of 'jaywalking,'" *VOX*, January 15, 2015, http://www.vox.com/2015/1/15/7551873/jaywalking-history.

[112] Thomas Gieryn, *Cultural Boundaries of Science: Credibility on the Line* (Chicago: The University of Chicago Press, 1999).

paradoxically lead to deliberate manipulation in order to the institutional survival or increase of relevancy in the whole national administration structure. It does not need to be limited to institution, the legitimate knowledge for risk assessment can be possessed by *epistemic communities*[113] that transform into *epistemic authority* while becoming an authority within established advisory boards advising decision making structures (boards, councils, decision makers).

In this perspective drawing the distinction between *experience* and *expertise,* as a distinction between *science* and *politics* has been attempted[114] and criticized.[115] The fact that the experience is detached from expertise produces two different perspectives and thus knowledges that leads to decision-making under conditions of *radical uncertainty*.[116] However, delivery of knowledge to policy makers by specialist possessing specific expertise has been studied as successful stories, e.g. AIDS,[117] but that does not completely diminish the dynamics of deliberate manipulation in the interest of heightening institutional anchoring of those who deliver the *relevant knowledge*.

We can find a very special case in the history, a fight between scientist Clair Cameron Patterson and Robert Kehoe. Patterson blamed oil companies for deliberate deception of public by intentional spread of misinformation in a case of an additive of heavy metal lead in fuel causing cancer.[118] His enemy was a scientist paid by oil companies Robert Kehoe to sow doubt. Despite of years of fight and the final victory over oil companies and their supporters by convincing judges, public and politicians in their scientific results, knowledge needed to force oil companies to find different additives to fuel won just the first battle, but not the overall war against unhealthy way of civilization development where logic of naturally renewable sources would be certainly long-lasting

[113] K. Kastenhofer, "Risk Assessment of Emerging Technologies and Post-Normal Science," *Science, Technology & Human Values* 36, no. 3 (2011): 307–33, doi:10.1177/0162243910385787.

[114] Harold Maurice Collins and Robert John Evans, "The Third Wave of Science Studies: Studies of Expertise and Experience," *Social Studies of Science* 32, no. 2 (2002): 235–96, doi:10.1177/0306312702032002003.

[115] Sheila Jasanoff, "Breaking the Waves in Science Studies: Comment on H.M. Collins and Robert Evans, `The Third Wave of Science Studies'," *Social Studies of Science* 33, no. 3 (2003): 389–400, doi:10.1177/0306312703033004; Brian Wynne, "Seasick on the Third Wave? Subverting the Hegemony of Propositionalism.," *Social Studies of Science* 33, no. 3 (2003): 401–17, doi:10.1177/0306312703033005.

[116] Alan Irwin, *Expertise in Law and Regulation* (Ashgate, 2004).

[117] Steven Epstein, *Impure Science: AIDS, Activism and the Politics of Knowledge* (Berkeley: University of California Press, 1996).

[118] D M Settle and C C Patterson, "Lead in Albacore: Guide to Lead Pollution in Americans.," *Science (New York, N.Y.)* 207, no. 4436 (1980): 1167–76, doi:10.1126/science.6986654.

with less impact on the environment then non-renewable energy sources (in their ideal form).

In that perspective, a *relevant knowledge* for policy makers seemed to be certainly influenced by particular interests rather than a production of scientific research. Development of knowledge that is *policy* driven rather than *curiosity* driven that is usual in basic research. The story between world saviors and oil companies has not finished yet as the chopping into raising evidence of need for renewables is still underway and include nicely calculable bunch of self-convincing evidences.[119] The winning stories are much more about balance of arguments rather than a victory of rational science. However, in this case, we are talking about empirically and experimentally testable scientific knowledge despite its fractal shaped complexity. The interpretation of the results is the cause for a judge; in the case of cyber security we stand on a much more fluid basement and as Nissenbaum argue acquiring the specific knowledge in cyber security is a daunting task.[120] The idea that the assessment of threat in cyberspace can be tested by rational positivist research is simply unachievable. The case with heavy metal lead as a threat to human health cannot be used as an example that positivist approach can help us in assessment of cyber threats. It has been used to demonstrate how such an undisputable relevant knowledge regarding human health can be successfully impugned over time by a production of the opposing knowledge based on false facts in a long-lasting doubt sowing discourse. When acquiring relevant knowledge is a daunting task, discourse can play its role to raise the attention. As Nissenbaum argued elsewhere, we have observed a shift from hackers as wise geeks to hackers as terrorists,[121] clear securitization, which is a move that Deibert understands as unsecurutizable.[122] Such move encircles all activities of hackers as being equal to terrorist intentions, at least for a selected audience.

[119] Bjørn Lomborg, "Don't Be Fooled - Elon Musk's Electric Cars Aren't about to Save the Planet," *The Telegraph*, April 6, 2016, http://www.telegraph.co.uk/opinion/2016/04/06/dont-be-fooled---elon-musks-electric-cars-arent-about-to-save-th/.

[120] Helen Nissenbaum, "Where Computer Security Meets National Security," *Ethics and Information Technology* 7, no. 2 (2005): 61–73, doi:10.1007/s10676-005-4582-3.

[121] Helen Nissenbaum, "Hackers and the Contested Ontology of Cyberspace," *New Media & Society* 6, no. 2 (2004): 195–217, doi:10.1177/1461444804041445.

[122] R. J. Deibert, "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace," *Millennium - Journal of International Studies* 32, no. 3 (2003): 501–30, doi:10.1177/03058298030320030801.

Increasing complexity of mutually influenced variables along with extreme progress of technology evolution in information technologies does not help us to establish bridges of mutual understanding between scientists and policy makers as in the success story of Patterson, but favors the threat politics based on doomy imaginative scenarios that play a significant role in decision making. The politics of cyber security is filled with speech acts based on predictions rather than analysis of serious events (especially when it comes to attacks on infrastructures that might cause civilizational collapse); predictions that requires a scientific answer within a cultural boundary of expected scientific facts. One of the reasons why we depend on these imaginations is so called *attribution problem,* which is today understood as an unbeatable characteristic of all cyber-related events. Attribution problem, which poses an almost unanswerable question who has been behind the attack, is fairly irresolvable in current technological setting of Internet. However, one of the obstacle behind attribution problem has been merging privacy with anonymity, which in real life is distinct whereas in cyberspace people tend to merge them into one problem. Privacy is not the same as anonymity, neither qualitatively nor legally.[123] It comes from the internet architecture, from the origins where technology reliability was quite above its security. This can be changed by technology development focused on security rather than on *hypersecuritization* of cyberspace.

Cyber security and the trigger of national security agenda of everything "cyber" is not about scientifically testable knowledge and its interpretation, but rather about the interpretation and adoption of doomy scenarios hugged by concepts such as the attribution problem that multiply the impression of seriousness of the drawn cyber doom; seriousness that is deepened by using analogical reasoning and metaphorical language, which enforced due to the call for relevant scientific facts as answers to the presumptive threats. The fact, that there were examples of serious cyber-attacks with physical consequence (Stuxnet, German Steel Mill Attack, Ukraine Blackout) have not confirmed that ignored cyber security will doom our civilization; it will rather give a reason for significant reconstruction of the basis of our current communication systems

[123] Adam Firestone, "In Cyberspace, Anonymity and Privacy Are Not the Same," *Securityweek*, September 26, 2014, http://www.securityweek.com/cyberspace-anonymity-and-privacy-are-not-same.

and as Gatzke argued, these examples show us that even serious cyber-attack against critical infrastructure causing blackout in a vast area can be easily restarted and repaired without doomy consequences. If we accept this perspective, we should be able to study processes behind the policy making over cyber security in the light of toughly tangible *technological radical uncertainty* and the reasons of the agenda explosion in the last decade as *discursive processes materializing imaginative threats*, as an *order of discourse*.

3.2. Types of expertise and the cyberspace

We can observe more than one direction of expertise deepening in every discipline; however, in many disciplines it is needed to cover a certain, huge amount, but comprehensive and compact knowledge to be able to argue with experts in that discipline – the body of knowledge. We can use astrophysics or particle physics or medicine as an example. Discussing Higgs boson requires at least all the related knowledge of the standard physical model; discussing heart transplantation requires general knowledge from a vast variety of medical sub-disciplines. However, when it comes to cyber security we can observe similar disconnected sub-disciplines; e.g. different operation systems, networking, knowledge of particular programming language and its shortcomings, different environment (WWW, desktop programming, SCADA systems, deep space communication arrays etc.) and finally incomparable pace of its development and thus constant fluid change rather than a linear consequent evolution of knowledge.

Maybe this statement is not precise and fair, as physics does have currently serious problems where to evolve as string theory has brought a perspective of uncountable amount of solutions related to uncountable amount of events and particles or that the standard model is hardly compatible with quantum physics.[124] We might have had some shortcomings in medicine before first heart transplantation, but we have solved it and already pose knowledge how to successfully transplant heart; we already poses a compact knowledge that works in a practical way to achieve a clear objective – to

[124] Lee Smolin, *The Trouble With Physics: The Rise of String Theory, The Fall of a Science, and What Comes Next* (Houghton Mifflin Harcourt, 2007).

transplant heart, but the objective is clearly good one. This method may evolve, may change completely, but will last for some significant time, as it is successful and reliable.

In cyber security we are talking also about habits of people that change the shape of cyberspace too quickly and too seriously, that the technology development is also driven by the constantly changing habits of its users on a daily basis, they mutually constitute each other in an extreme short period of time[125] what brings quite serious problem to its governability. When it comes to cyberspace there is also an ongoing debate whether it supposes to be governed by governments or left to its self-governability.[126] This debate is quite huge and will be elaborated later; however, one point is important here. As the cyberspace is fluidly changing so quickly, the ability to govern is significantly limited. It is not only about the complexity, but about fluidly changing complexity. Governments may be able and are quite successful in supporting standardization leading to desirable resilience of critical systems as e.g. European Union requests in its strategy[127] followed by particular nations, but they may not be able to govern cyberspace completely, especially branches of the cyberspace that belongs to and are governed by people seeking for ultimate liberty in cyber anarchism[128] or cyber libertarianism. As said, the case of governability is not limited to the unlawful activities in cyberspace, but also about the governance of technology development related to future shape of cyberspace. That requirement exceeds inability of governance, it becomes utopia.

The technical capability of individual people can seriously exceeds capability of state employed experts what super-empowers them as well.[129] When we come back to threat analysis in cyberspace in this perspective, the ability to assess threats coming from

[125] Nikola Schmidt, "A Sociological Approach to Cyberspace Conceptualization and Implications for International Security," in *Perspectives on Cybersecurity*, ed. Jakub Drmola (Brno: Muni Press, 2015), 70–77.

[126] Ronald Deibert and Rafal Rohozinski, "Liberation vs. Control: The Future of Cyberspace," *Journal of Democracy* 21, no. 4 (2010): 43–57, doi:10.1353/jod.2010.0010; Ronald J. Deibert and Masashi Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls," *Global Governance* 18, no. 3 (2012): 339–61; Neil Weinstock Netanel, "Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory," *California Law Review* 88, no. 2 (2000): 397, doi:10.2307/3481227.

[127] EU, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" (Brussels, 2013), http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

[128] Harry Halpin, "The Philosophy of Anonymous: Ontological Politics without Identity," *Radical Philosophy* 176 (2012): 19–28.

[129] Nikola Schmidt, "Super-Empowering of Non-State Actors in Cyberspace," in *World International Studies Committee 2014* (Frankfurt: Goethe Universitat, 2014), 5.

particular sub-discipline of computer science does not critically require all other knowledge in a wide compact manner, but critical amount of certain knowledge. Young hackers, so called *script kiddies* were able to cause a lot of damage,[130] but also probably whole armies of hackers were able to cause larger damage to national infrastructure.[131] One may raise a question what is a damage in cyberspace as there are usually zero damage to physical infrastructure. In both cases, the conducted attacks found their targets unprepared, comparable attacks would cause zero damage to the targets today.[132] In summary, what is important on the digital world of computers is its quick change that gathering comprehensive and compact expertise in particular direction or sub-discipline is an impossible task. The ability to stay updated with current trends seems to be more and more critical rather than having deep knowledge in the computer science in general. This dynamic certainly influences the way how experts are requested to answer general questions regarding cyber related threats to national security.

The concept of *boundary work* offers an idea that a particular scientific group during the risk assessment based on hard scientific resources can be completely separated from value oriented policymaking. Such dynamics has been challenged,[133] but some particular successful occurrences are available in the literature.[134] However, these boundaries are being attacked by policy makers to produce deliberately value-oriented results or otherwise, the result by the *epistemic authority* was excessively absorbed as unchallengeable scientific *truth* by policy makers. Boundaries can be raised around the whole organizations that possess unchallengeable authority to assess particular problem even though the whole organization does not harbor experts with appropriate expertise. Moreover, the expertise appropriateness can be devised from conformity. Sometimes

[130] Michael Calce and Craig Silverman, *Mafiaboy: How I Cracked the Internet and Why It's Still Broken* (Viking, 2008).

[131] Binoy Kampmark, "Cyber Warfare Between Estonia And Russia," *Contemporary Review* 289 (2007): 288–93.

[132] Estonia 2007 was hit with DDoS with amplitude about 100mbits, according to the www.thedigitalattackmap.com current attacks every months reaches 400-500mbits without comparable political consequences. In the case of Mafia boy, DDoS attacks were very rare and servers of Amazon, eBay, Yahoo and all others targeted were found completely unprepared. Mafia boy also provides different context in his book, radio interviews and other media, thus it hard to evaluate how serious the attack was and whether he just had surfed a wave of his popularity to enlarge seriousness of these events.

[133] Alan Irwin and Brian Wynne, *Misunderstanding Science* (Cambridge: Cambridge University Press, 2004), doi:10.1017/CBO9780511563737.

[134] Jasanoff, *States of Knowledge: The Co-Production of Science and Social Order*, 1–12.

experts are not willing to contribute to the political process, but despite that policy makers are using their concepts to give the political agenda scientific relevance without having appropriate context or analysis. Shaping the reality is then clearly based on imagination, but with very real implications. Hence, the scientific results and society are *co-produced* in cycles;[135] even the scientific knowledge is then socially constructed as it does not lie on verifiable science. Furthermore, the invisible knowledge, expertise, technical practices and material objects somewhere in the middle of both, scientific and political processes, are shaping, sustaining, subverting or transforming the relations of authority.[136] These boundaries between authorities in technical expertise or policy relevance are not stable; they are rather *contextual products* of moment-to-moment, institutionally embedded, discursive interaction.[137]

Erwing Goffman's sociological concept of *framing*[138] is used in a context with STS as *collective action frames* where particular actors mobilize and counter-mobilize ideas and meanings[139] especially in the context of their own institutional survival invoking the God of science as the only rational way of risk assessment of security impacts of scientific discoveries or their application and thus the only relevant production of *legitimate knowledge* or *good science*. When this Goffman's framing is put into the current knowledge production, especially between experts of communication or internet/web technologies, we arrive to the world of Latour's power assemblages, where no particular institution is effectively capable to govern the realm between technology and society, but rather human and nonhuman actors are both included in the construction of sociotechnical systems, including the artificial intelligence, which research is currently successfully underway to be seriously added to the nexus of actors. That directly applies to the world where habits of users in cyberspace changes cyberspace itself, influences patches and new features, that produce new errors and thus exploits finally causing

[135] Claire Waterton and Brian Wynne, "Knowledge and Political Order in the European Environment Agency," in *States of Knowledge: The Co-Production of Science and Social Order*, ed. Sheila Jasanoff (London: Routledge, 2004), 87–108.

[136] Jasanoff, *States of Knowledge: The Co-Production of Science and Social Order*, 1–12.

[137] Michael Lynch, "Circumscribing Expertise: Membership Categories in Courtroom Testimony," in *States of Knowledge: The Co-Production of Science and Social Order* (London: Routledge, 2004), 161–80.

[138] Erwing Goffmann, *Frame Analysis: An Essay on the Organization of Experience* (Cambridge, Massachusetts: Harvard University Press, 1974).

[139] Andrew L Roth, Joshua Dunsby, and Lisa a Bero, "Framing Processes in Public Commentary on US Federal Tobacco Control Regulation.," *Social Studies of Science* 33, no. 1 (2003): 7–44, doi:10.1177/0306312703033001038.

security glitches interpreted as national security threats. How quickly behavior of artificial intelligence in service of cyber defense and preventive IT systems patching will be understood as a threat? And how some artificial intelligence will react on a hostile behavior by humans who previously learned that intelligence to recognize "hostile" behavior in order to patch exploits?

In that perspective, national security threats can be seen in fluidly changing cyber realm of mutually constitutive iterative process between habits of users and technology evolution, but also in technology self-evolution. The co-production process between experts constantly assessing and interpreting a current state of technology and its possible impact to national security that – as said – are *contextual products* of moment-to-moment, embedded to particular institution and its policy position, which discursively keeps their perspective alive to persist their reasons for existence, but which does not need to act against some newly emerging cyber related threats.

If we take into consideration the above mentioned dynamics of constantly changing shape of the digital world or in other words computing technologies, the production of knowledge (or higher computer literacy or expertise) supposes to be more random than systematic; how can then be the threat assessment systematic and compact? However, describing the threat in particular terms produces requirement of an answer on these threats as they can be solved preventively by adopting appropriate countermeasures. Sheila Jasanoff makes difference between governmental research driven by risk and scientific research driven by curiosity.[140] She elaborated this criticism of advisory boards serving policy makers, which are in fact policy makers themselves.[141] She is going so far that she makes the point that peer-review processes in particular cases fall into so called *regulatory science* and thus are influenced by the political will rather than being reviewed by scientific peers. The result is a production of knowledge serving interests of those who are in charge, who have been asked to develop countermeasures on threats that are more awaited by drawn doom scenarios such as "cyber 9/11" than

[140] Sheila Jasanoff, "Technologies of Humiliation: Citizen Participation in Governing Science," *Minerva* 41, no. 3 (2003): 223–44, doi:10.2307/41821248.

[141] Sheila Jasanoff, *The Fifth Branch: Science Advisers as Policy- Makers* (Cambridge, Massachusetts: Harvard University Press, 1990).

events in recent history.[142] Emotions and fears drive nation states into a state of fluid post-modern non-governability.

Experts driven by policy rather than curiosity have shared interest – to introduce the world a threat they are capable to deal with. Sharing a common threat unites them and sharing comparable solutions institutionalize them. Additionally, governments tend to create new institutions to deal with threats with preposition of "cyber" even though the acts might fall into responsibility of a computer servicing company (common virus), police (crime), intelligence (espionage) or defense (national security). These new institutions construct their selfhood, their irreplaceableness and thus power by adopting knowledge they previously created through grouping the *best* experts in the field.

The *boundary* within such cyber related institution serve construction of a new *church* with its own *scared texts* based on a presumptive *field of truth* keeping the institution in *power* by preserving its *authority* through keeping *experts* and *policy workers* in a *discipline*.

All of this can happen despite the self-evolving technology evolving itself through the deep learning method completely detached from human control. The question of related expertise is then moving beyond the cultural boundary as Latour and others discussed. That can be a completely new perspective for research in Science and Technology Studies.

[142] Lawson, "BEYOND CYBER-DOOM: Cyberattack Scenarios and the Evidence of History."

4. ARCHAEOLOGY, GENEALOGY AND THE RULES OF DISCOURSE

"The 'Enlightenment', which discovered the liberties, also invented the disciplines."[143]

— Michel Foucault —

> "Foucault's histories are not histories of ideas, opinions or influences nor are they histories of the way in which economic, political and social contexts have shaped ideas or opinions. Rather they are reconstructions of the material conditions of thought or 'knowledges'. They represent an attempt to produce what Foucault calls an archaeology of the material conditions of thought/knowledges, conditions which are not reducible to the idea of 'consciousness' or the idea of 'mind'.'"[144]

Based on Foucauldian perspective the research uses Foucault's lens of order of discourse to analyze the discursive streams in cyber security and how these streams produce knowledge used by decision makers to shape the political agenda. Additionally, Foucault's thoughts in Archaeology of Knowledge are used to bridge his thoughts of knowledge production with Science and Technology Studies that are more focused on the sociological dynamics of technology governance.

In the following research I study the evolution of cyber security, the genealogy of discourse that gave the birth of cyber security as a national security agenda. Taking Foucault's approach means that I put attention on the problem – why is cyber security a national security concern? Where the shift from *computer security* to *cyber security* happened and under what circumstances? I will define some starting points of its origin to unveil present materialization rather than to describe the discourse production as an historical period. I use the Foucault's archaeological approach to study the discourse and how this discourse has formed new material world – new institutions, new technologies, and new authorities. I will analyze statements of particular politicians or statesmen

[143] M Foucault, *Discipline & Punish: The Birth of the Prison*, Vintage (Knopf Doubleday Publishing Group, 2012).

[144] Gary Wickman and Gavin Kendall, *Using Foucault's Methods* (London: Sage Publications, 1999), 35.

having a significant impact on further policy development; discourses as practices, as *"the general system of the formation and transformation of statements."*[145]

Mutual constitutive processes between *what is sayable* and *what is visible* Foucault understands as a strategy that is fulfilled by discourse. Strategy where statements in *what is sayable* play the pivotal role in producing visible artifacts in the new shape of evolving society; in his writings, Foucault shows this dynamic on prison where statements about criminality forms the prison and also the reason of its existence, whereas the prison itself by its visible existence reinforces the statements about the criminality. Discourse has thus material implications in the process of its materialization.[146]

The methodological procedure of the research follows the archaeological approach by identifying and describing statements as snapshots following with genealogical approach to uncover how discourse helps materialization of *sayable* to *visible*. However, in the empirical part I am reading three discourses in a way to draw and interpret the red line across these three fields of self-reproducing knowledge with an objective to demonstrate the "left-to-right flow" of unbeatable truth (from geeks to crime to national security) and to discuss the related materialization of power in newly emerging institutions. There is no rigid step-shaped procedure in the empirical part. These steps are conducted randomly and thus should be understood as an insight in the method rather than a step by step sequential procedure. The objective is to use Foucault's approach to formation of new concepts and use them in further reading of discourse.

4.1. Formation of new concepts through successive series of statements

Being able to advance from the beginning, I will describe the methodological approach in layers. On the first layer, I focused on the origin of *concepts* used further by politicians and statesmen or any other stakeholders apparently involved in the general cyber national security discourse. I focus on the *formation of new concepts*[147] that are taken from sub culture of cyberpunk such as *hacker* or *geek*, which are altered, adopted and incorporated into new contexts during the creation of *church of knowledge* that is the

[145] Foucault, *The Archeology of Knowledge*, 130.
[146] Wickman and Kendall, *Using Foucault's Methods*, 26.
[147] Foucault, *The Archeology of Knowledge*, 62–71.

foundation of security assessment and thus new political agenda. What I mean with a concept *church of knowledge* I currently introduced? When I talked about the circulation of discourse within particular military community, the reiterated usage of altered concepts such as hacker produce specific knowledge through political statements with specific connotations calibrated to the sense of particular social group. However, it is not based on experience, but on speculations. In case of experience, Foucault talks about *fields of truth,* a field when the subject is torn away from itself in order to elucidate the truth from experience.[148] Foucault wanted to have read his books as a flow of experience and they particularly have a specific language, in which Foucault consequently use adjectives in series to precisely depict his current experience of thought. When I was thinking how to depict the reiterated experience of being exposed to a speculative knowledge based on transferred concepts from fields of knowledge that has comparable internal and confirmed dynamics, I decided to call it a *church of knowledge* as the observable beliefs in potentialities seem to suffer of confirmation bias and lack a scientific inquiry, in contrast to what Foucault calls *field of truth,* where the scientific inquiry[149] or experience[150] are critical.

Foucault distinguishes between two kind of knowledges that are distinguishable in French language. The distinction between *connaissance* and *savoire*.[151] In the former meaning, knowledge means knowing a thing, to understand that wheel is a wheel. Savoir, in contrast, means how to use that wheel and count on all possible implications of its usage. If one possesses knowledge how to use a wheel and anticipate the consequences, it provides him/her with power.[152] In our context, it is a political power how to use particular knowledge in gaining a political advantage; it does not matter whether the knowledge is based on speculations or experience if it is reiterated enough, if the demonstrative reasoning of statements anchor speculations as facts in long-lasting

[148] Timothy O'Leary, "Foucault, Experience, Literature," *Foucault Studies*, no. 5 (2008): 11, http://cjas.dk/index.php/foucault-studies/article/viewPDFInterstitial/1422/1526.

[149] Frédéric Gros, Francois Ewald, and Alessandro Fontana, *The Courage of the Truth (The Government of Self and Others II) LECTURES AT THE COLLÈGE DE FRANCE 1983–1984* (Palgrave Macmillan, 2008), 88.

[150] O'Leary, "Foucault, Experience, Literature," 11.

[151] Foucault, *The Archeology of Knowledge*, 200–205.

[152] Wickman and Kendall, *Using Foucault's Methods*, 51.

discourse. It is an area of knowledge with unbreakable boundaries that help the church to stand on a solid foundation.

If these statements appear in coexistence they create a *field of presence*, then, if they appear in sequence or in a system as they are used in chain, in a chain of demonstrative reasoning, in their altered meaning, they form *field of concomitance*. The field of presence is understood by Foucault as *"all statements formulated elsewhere and taken up in a discourse, acknowledged to be truthful, involving exact description, well-founded reasoning, or necessary presupposition"*[153] and the *field of concomitance "serve as analogical confirmation, or because they* [statements forming new concepts] *serve as a general principle and as premises accepted by a reasoning, or because they serve as models that can be transferred to other contents, or because they function as a higher authority than that to which at least certain propositions are presented and subjected."* [154] If a hacker within the cyberpunk discourse has its meaning close to a geek, the connotation, if applied to national security, shifts to cyber terrorists easily. The implications are already acknowledged to be truthful in the field of presence and filled with particular security related content through accepted premises by reasoning or model understood as the appropriate. Hacker has power to hack, but also to produce fear fueling the speculative processes of what a hacker is capable of. However the one, who transfers the meaning of that word knows how to use the wheel in further political advantage as the imaginations appear to be meaningful and how to depict a hacker as enemy. It is a mutually constitutive process between two actors seeing itself as mutual enemy, but in separated discourses, in separated worlds, in which they establish their own authority. They (usually) do not fight a battle.

Concepts taken from different cultural worlds are put into new relations producing new *fields of presence* in different worlds of meaning, but are understood as truthful; models have been transferred successfully. If the imaginations are subsequently based on potentialities, the new concepts are created in a speculative world and deepen the level of speculation. However, they are already anchored in unquestionable system of knowledge (*acknowledged to be truthful*) that belongs to particular beliefs, but based on

[153] Foucault, *The Archeology of Knowledge*, 64.
[154] Ibid.

speculative expectations that stands only thanks to preserving beliefs in potentialities, thus I call that corpus of newly emerged knowledge a *church of knowledge.*

Their usage in *successive series* is strengthening relevancy of emerging *church of knowledge* to the adoption of the current political agenda. *Successive series* consequently legitimize its adoption as unquestionably needed. Then, the series need to be easily comprehensible to the audience, so they are put in the *successive order* that further evolve into the new comprehensible *demonstrative reasoning* in form of political *statements* that seem to hit the nail on the head and the *field of concomitance* emerges. Further I discuss particular moments, where new reasoning of newly adopted concepts within new field of knowledge is taken as granted, the emergence of *field of concomitance* and evolves into new *statements* based on presumptive experience of those who face the threats on a professional level. Then the *field of concomitance* transforms into *field of truth* as they seem to be experienced by those who use the new statements. Casting doubts over them is a betrayal of a new *church of knowledge*. To uncover this shadow of admissibility we must pay attention on those who are criticized, judged, rejected or excluded for not following beliefs that are presented as experience.

Additionally, we should pay attention on *fields of memory*; on concepts that are not relevant anymore, but which were at the beginning, which are filiation of current *statements*, which do not define the current *field of presence* as they are not appropriate or do not seem to be valid to describe the current – national security – situation. Here, I am talking about the shift from *computer security* to *cyber security* covering very probably the same problem, but with new evolved meaning including national security concerns, a new *field of concomitance*. I do not treat *statements* as mere speech acts, but as units caught in a *logical* and *locutory nexus*. To summarize this phase, the point is to make the links between words and things; between *sayable* and *visible*.[155] It is the Foucauldian materialization of visibilities through statements and vice versa, both visibilities and statements are mutually constitutive; no prison would be possible without statements of criminality and criminal behavior is constituted by statements about morally acceptable

[155] Ibid., 56–58.

behavior.[156] No cyber security expert centers would be possible without cyber related national concerns created by *locutory nexus* of new *statements* emerging from a new *field of concomitance* representing a presumptive experienced *field of truth*.

4.2. Creation of field of truth and the logical slide

On the second layer, I elaborate on currently built structure of the identified statements and newly adopted concepts in the emerging cyber security discourse. The case is to analyze the order of these statements in time, in the dynamics of materializing structure, in their interrelations in time. How one statement influenced the other statement, the one which was a precursor for other statements; how a concept evolves in time to produce new one. In the words of our case, how a security related *statements* have built on the culturally bound *concepts* to generate new presumptive *fields of truth.* To distinguish between *fields of concomitance* and presumptive *fields of truth,* I will analyze several technical documents that easily deny even the technical possibility that a particular exploit can cause apocalyptic implications.

These new statements are based on another statements that cannot be challenged as they have already established their position in new reasoning, new logic, new belief, new undisputable concern. In particular, applying cyber security discourse on conventional waring. The whole discourse over cyber war depicts cyber war as something inevitable. It builds on assumption that conflicts happened in past and will happen in future as well as the IT systems simply have exploitable vulnerabilities. Cyber war will come in different shape, but more threatening and with comparable destruction to Pearl Harbor as they call it *cyber*-Pearl Harbor. It is a call on policy makers to describe what is going to happen and then, drawing on cyberpunk subculture to explain this call as a source for the prediction is not a mishap. Especially when this subculture still designs new technologies that are quickly stepping in our everyday lives and are uncontrollable by state authorities.

[156] Michel Foucault, *Power/Knowledge: Selected Interviews and Other Writings*, ed. Colin Gordon, *New York*, vol. 23 (Pantheon Books, 1980), 109–133.

The relation between sub-culturally bound concepts and national security related statements might seem to be unimportant as they exist in different dimensions of knowledge, but they interfere each other by their compatibility, its analogical confirmation, as they appear in the same discursive formation – war is becoming cyber war, national security is becoming national cyber security, espionage is becoming cyber espionage etc. They form a complex system of relations only because they appear in the same discourse where one expects the relation – spying is desirable for national security, thus other nations should expect it in its most (im)possible shape, in a doom scenario of hyper speed cyber espionage. It seems to be logical way of thinking and thus a *logical nexus*.

Later in the first empirical part, I am studying the ideology of the crypto-anarchist movement in order to understand what particular ideological content could be added to concepts previously known only in the dystopian science fiction literature known as cyberpunk. The relation between crypto-anarchy and cyber security as a national security agenda might look fuzzy, but adding the content of particular ideology to the statements helps to legitimize drawing of these doomy scenarios. The ideology of crypto-anarchist movement is adding content to the concepts used in the discourse that draws doomy scenario on their capabilities. Production of a technical knowledge under the curtain of such cultural cloud produce logical nexus of political statements and conviction that possibilities emanating from geeks' capabilities, which everybody understand as unimaginable to us mere earthlings, can materialize into the apocalypse if the ideology, and thus motivation, is applied. One may forget the link to a crypto-anarchy, but the doomy content prevails – it looks conceivable. Then the reasoning of the content in the same discursive formation has an origin and its genealogy and evolution that consequently produce new compact knowledge despite the obvious incompatibility according to their meaning and evolution (national cyber security evolved differently than crypto-anarchist movement). The incompatibility may diffract the discourse, but form it at the same time as authorities provide a framework. They help to resonate the statements without a clue of real technological consequences of particular technical vulnerability; it is a vulnerability in *cyber systems,* vulnerability that can be possibly exploited by hackers, which thus become a cyber terrorist and thus a threat to national

security. As I mentioned before, these two environments do not need to be in a tight contact, but are mutually constitutive. Without ideology behind the attacks, we would live only in a speculative world of possibilities constructed by the cyber war discourse as it was criticized by Gartzke.[157] However, if we include the ideology, the motivation of hackers seems to materialize, but in general, not only on *bad* hackers.

Authorities help form the legitimacy of the whole general cyber security discourse by being on the higher positions possessing higher authority, thus to the lower ones take it as granted; and vice versa! In other words, how experts use their assessments regarding cyber security to produce new dimensions of truth based on their undisputable expertise of knowing hackers and their skills. The policy makers point on these newly emerged experts as holders of the *relevant knowledge*. Nobody questions too much, as questioning is threatening the solid foundation of church of knowledge, especially within the related institutional environment possessing power to deal with cyber security at the national level. Who knows hacker communities or who *experienced their evil* is an expert in the cyber security field, as we saw in Kaiser's contribution when it comes to expertise coming from a particular geographical territory – Estonia.[158] However, it is based on their authority, on their social role, that gives them the opportunity to produce *relevant knowledge*, which is consequently used as an unbeatable established policy based on unquestionable and precisely sorted presumptive *fields of truth* rather than on scientific knowledge emanating from curiosity. The latter usually analyzes the problem in its core and proposes alternative solutions in more secure technologies, but this process is not in the interest of those who repeatedly co-produce the discourse, they rather focus on the presumptive *field of truth* nobody seriously question. Powerful policy makers cannot be challenged as they are expected to be responsible for peoples' security rather than being wrong with the criticism questioning whether the threat is actual, relevant or important. As we saw in Cox, there are two approaches, the "critical" that question the current policy and the "problem-solving" that needs smooth operation of institutions. [159]

[157] Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth."
[158] Kaiser, "The Birth of Cyberwar."
[159] Cox, "Social Forces, States and World Orders: Beyond International Relations Theory," 129.

4.3. Establishment of the field of truth by repeating and correlating

The third layer analyzes how the statements, their relation, the ordering and their complex system of interrelation *repeat* the *statements*, the presumptive *fields of truths*, to produce the discourse and how this repeatability causes the emergence of these statements ones more in the discourse and causes and deepens their validity, legitimacy and comprehensiveness. Repeating does not need to be conducted by the same individual. While the general public requires assurance that the governmental structures are working on newly emerging threats, repeating statements of other authorities reassure the public and reestablish the positions and *relevance* of these newly emerging *authorities*; whether persons or institutions. They have become relevant and they have to preserve the relevancy. Repeating statements in time prolongs these new subjects of authority a relevance of their existence. Avoiding the repeating of the same or critical questioning would do exactly the opposite effect.

Repeating goes along with a *correlations.* Those who use statements to deepen their authority would use correlations to show the *rationality* of their statements and the colorfulness of their meaning;[160] the interconnectedness of their concern with the general concerns of this field of discourse. These correlations are very visible in all cyber doom scenarios drawn on significant historical events as correlatable analogies, as *analogical confirmations* from *fields of concomitance*, such as *cyber*-Pearl Harbor, *cyber*-9/11, *cyber*-blitzkrieg*, cyber*-St. Mihiel*, cyber*-Battle of Great Britain*, cyber*-Vietnam etc. by statements warning about reiteration of these events in cyberspace. If we take into consideration some selected knowledge from social psychology, particularly Social Identity Theory (SIT),[161] repeating these correlative statements within a group of involved people tighten relations between them and pointing on any outer critics as being deft and blind without any self-criticism. In the end, cycles of these iterations help strengthen these tights and strong tights deepen beliefs of colleagues' expertise. Imaginations that were at the beginning a piece of possible scenario on which the national

[160] Foucault, *The Archeology of Knowledge*, 102.

[161] More thoughts on SIT could be found in Esra Cuhadar and Bruce Dayton, "The Social Psychology of Identity and Inter-Group Conflict: From Theory to Practice," *International Studies Perspectives* 12, no. 3 (2011): 273–93, doi:10.1111/j.1528-3585.2011.00433.x.

security structure should be prepared are becoming tacit instruments in social group closeness. The experience of particular persons is becoming a field of truth as the depicted experience is plausible in order to reach the overall policy objectives.

All these processes are in progress with no regard on a fact that there is zero empirically verifiable data as no cyber-9/11 has ever happened, but *may* happen, it is a pure speculation. It is not a preparation on possible catastrophe in order to normalize the reactions as Aradau and Munster proposed.[162] It is thought, that one event can bring us back to the *stone age*, thus it is not desirable to be prepared on that event, but it is broadly believed that we must act preemptively to cease the inevitable apocalypse. It is about social construction of the possible event in the future by correlating it with well-known emotionally bound event in the past by discourse as there is no other evidence or source of this claim. SIT also provides interesting relation with Foucault's method while the process of strengthening tights can be strengthened with Foucault's concept of discipline.[163] The repetition of statements and their correlation can be understood as a required discipline of those who are willing to be involved in the policy making process; SIT then confirms the efforts. If the experts are willing to be heard, to be accepted by the community, they have to participate on the discourse construction with an appropriate discipline. Think tanks are producing a row of policy papers that do not propose new thoughts, but build on a presumptive field of truth, so the author can be assured that he/she is not making a mistake and can expect to be accepted within the community. Even generals in NATO are expected to respect the problem of cyber threats with no regards on verifiable, observable and reliable data. It is an enclosed sect with its rooted truths nobody inside dares to question.

Statements are created, constructed, repeated and correlated by human beings, *subjects of discourse* and these are interrelated in horizontal as well as vertical relations. Lower subjects with lower authorities would not significantly influence those who have higher authorities and especially in state service, people would not question truths of their bosses. Subjects that poses authority are put into formalized roles, while it is a

[162] Aradau and Munster, *Politics of Catastrophe*.
[163] Foucault, *Discipline & Punish: The Birth of the Prison*.

human being who *speak, create, construct, repeat and correlate*,[164] but the impact is related to the authority, to the roles of the speakers, of the subjects who commit the speech act and produce the discourse. It is a teacher who is right over pupil, it is a policeman who is right with his argument to a jaywalker and there is no doubt that the higher authority can use the role, the position as a means of power.

4.4. Truths are growing from an underground to the surface of emergence

The fourth layer analyzes *surface of emergence*, places before they are institutionalized or forum where the discourse takes place, where it gains its reasoning and credibility; where proper solutions are given to raised threats.[165] These surfaces might be different for different discourses. In our case, surface of emergence will be an expert environment (furthermore related to network assemblages) already possessing needed respect by authorities, which need to repeat their statements to reassure their role, their position, their authority, their impact of their discourse. Where repetition is understood as a kind of discipline. If the result of the research was to uncover that the discipline is stronger than scientific curiosity as we saw in the case of Clair Cameron Patterson and Robert Kehoe while producing knowledge used by policy makers to anchor particular interests rather than support public interest, we would be able to identify how these surfaces of emergence in discourse play significantly higher role stating what is then uncritically understood as unbeatable truth; although, as a truth in its own universe. *Surfaces of emergence* are here related also to what we will later call *epistemic authority*, where the epistemic refers to the relation between experts who do not know each other, but share the same concerns and thus deliver a surface on which they can speak, repeat the statements of their sect, grow in hierarchy and construct the surface from which the later discourse emerges. Maybe also in the perspective of a group with inner cohesion based on SIT, where disagreement is punished as crime of disobeying inner non-written rules and norms.

[164] Foucault, *The Archeology of Knowledge*, 102.
[165] Wickman and Kendall, *Using Foucault's Methods*, 26.

4.5. Materialization of power

The fifth layer identifies how *surfaces of emergence* form into *institutions*. How creation of places of visibility has been formed from discourse into material world with acquired authority. These institutions might with an alarming regularity write their own laws to enshrine their authority in the process of discourse materialization; a process where the institutions' authority is directly materialized into national laws. This is the final moment of the establishment of the relevance of new knowledge, in which the efforts of experts and policy makers constructed a new field of knowledge emanating from *technological radical uncertainty*. The use of the genealogical method further in the research provides us an insight to this process of discourse materialization and unveils what partial steps have led into current assurance or confidence of need to preventively secure population against possible cyber war by adopting measures at the level of national security. If we adopted laws on a preventive manner, we would never realize whether they solve the threat.

Institutions are supporting backward forces, when new concepts, statements repetitively anchored in the new shrine of new policy are coming back to society to fulfill the cycle of the iteration and assurance of its relevancy. These forms of specification are targeting objects of the discourse, fulfilling its very objectives to convince people about the relevancy and trigger other materialization processes. It is about initiation of downstream, about *domains of application*. Once jaywalking had been adopted in one place in the world, the others followed the right of cars to drive fast in the city without complicated questions, burdens or public disagreement. Social construction of jaywalking probably lowered the causalities by giving cars right. It established a special regime between walkers and drivers without a reflection to what it might do to urbanism. Who is right, cars or pedestrians? Do we really lower number of causalities while significantly enlarged car usage? What is appropriate, a habit, that had been already established by discourse of those who blamed walkers by inappropriate hitting cars instead of otherwise. *Domain of application* which changes the world, the ideas, the society, the visible parts of society in current of events which are received uncritically, as granted, as a habit, as a cultural character and posed unquestionable distance from those who have not adopted it yet.

A comparative analysis of different states, which are mirroring each other waits for a critical analysis. Particularly, why states that have not already experienced a one significant cyber-attack are adopting the same policies? Why states, like the Czech Republic, and their statesmen or highly situated people are repeating one insignificant years old attack as a proof that cyber security is a national concern? Why states are adopting national policies by mirroring other states to solve transnational or global problem? Can a combination of harmonized national policies globally lead to a better cooperation without establishing a global authority? The conference in Dubai in 2012[166] was exactly that attempt in establishing one super-authority over Internet that failed. Paradoxically, the West with its liberal ideas would transfer powers to one body within United Nations and drop current multi-stakeholder governance of internet, but the fear that such body would be exploited by authoritarian states that found their way how to control internet on their territory, led to support of the current multi-stakeholder model.[167]

Institutions use their newly acquired authority, which can be understood as an emergence of power. Some critics argue that Foucault's power lacks subjects losing or gaining power over each other;[168] however, the mutual constitutive process between sayable and visible is what generates the power by actions, by those who are successful in advancing discourse in their very interest (from individual statements to collective institutionalization of solution of discursively and socially constructed problems or threats generally accepted as serious concerns). It is the kind of productive power where prison is a visible and material result of a discourse about crime; where statements about crime reintroduce backwards the prison as materialization of discourse. This is what Foucault call productive power. Deleuze commented the Foucauldian notion of power as a power between forces and those forces do not need to be conducted by particular subjects and thus it is about actions over other actions: *"It is 'an action upon an action, on*

[166] World Conference on International Telecommunications (WCIT) 2012.
[167] Deibert, "The Geopolitics of Cyberspace after Snowden."
[168] Michel Foucault and Duccio Trombadori, *Remarks on Marx: Conversations with Duccio Trombadori* (Semiotext(e), 1991), 112–113.

existing actions, or on those which may arise in the present or in the future'; it is 'a set of actions upon other actions'."[169]

4.6. Foucault applied and discussed

One may understand adopting this methodology as a direct and deliberate criticism and judgment of people who are taking care of our security by pointing on particular problems and reshaping them into threats to be solved in order to avoid serious problems. A process, which is unavoidable if we want to face what *might* happen in the future. However, it is needed to say here that the analysis does not want to judge, it supposes to be critical per se or critical with deliberate search for arguments to fulfill the premise of threat construction through deliberate threatening speech act. The purpose of the analysis focuses on the origin of the discourse through genealogy of its evolution:

> "It's amazing how people like judging. Judgment is being passed everywhere, all the time. Perhaps it is one of the simplest things mankind has been given to do. And you know very well that the last man, when radiation has finally reduced his last enemy to ashes, will sit down behind some rickety table and begin the trial of the individual responsible. I can't help but dream about a kind of criticism that would not try to judge but to bring an oeuvre, a book, a sentence, an idea to life; it would light fires, watch the grass grow, listen to the wind, and catch the sea-foam in the breeze and scatter it."[170]

When we are able to analytically grasp the process how the knowledge is produced, we are prepared to analyze and unveil the origin of the knowledge. The objective here is to analyze the origin and the evolution since the origin. We are probably unable to set a particular point, however, we do our best to read back into the history to seek for the processes that precede current state of the policy in cyber security. It is very possible that the genealogical approach will find the subjects of discourse, those who

[169] Gilles Deleuze, *Foucault* (Paris: Editions de minuit, 1986).
[170] Michel Foucault, "The Masked Philosopher," in *Politics, Philosophy, Culture. Interviews and Other Writings 1977-1984*, ed. Lawrence D. Kritzman (New York: Routledge, 1988), 326.

produce it, quite uncomfortable. The same happened to psychiatrists who did not want to hear about the origin of the madness, sexuality, dementia from Foucault's writings where Foucault made a point that psychiatrists needed to fill an empty leper house with a new person, the madman.

Here, I see a great opportunity to take the position as Foucault took. One may raise a question, where is the truth? How this research contributes to a concern whether we are standing in front of cyber war or not? The point is not to answer this question. Purpose of this research is not to confirm or exclude whether cyber war is coming or whether the current state of technology will give a raise to self-confident Skynet (from the classical cyberpunk movie Terminator), which will take over the government over the whole humanity. One may be curious to ask, to raise this question, to find the reasonable analysis of steps leading to threats posed by technology, develop capability that avoids raise of artificial intelligence or self-confident machines either material or just in a form of software. This research takes the opportunity to ask a question concerning ontology of present, ontology of ourselves, a critical analysis of social and material environment we have produced in order to deal with threats, which are have been imagined, thus expected and then probably constructed based on our *technological radical uncertainty*.[171]

I have been already talking about *processes* before; however, the archaeology is about capability to make a snapshot in the history of the problem in interest; in a specific context, to disentangle relations and identify the origin.[172] Genealogy is about process of putting these snapshots into relations, giving them the reasoning in the context of emerging power, with an emphasis on power through 'disreputable origins and unpalatable functions' what is exactly about making those who constructs subjects of discourse uncomfortable by showing the origins and efforts that they would rather have hidden.[173] If one poses power thanks to established beliefs, one would not be interested in deconstruction process of the power origin. Power is also about holding the knowledge, authority to alter it, evolve it in an intended direction without being criticized

[171] Ibid., 95.
[172] Wickman and Kendall, *Using Foucault's Methods*, 24.
[173] Ibid., 29.

or suspicious of preserving the power.[174] These who were appointed by a role to deal with constructed, established and unquestionable threats are in a position to solve it. Authorities expect solutions from experts and do not question whether that or other interpretation under *technological radical uncertainty* is legitimate.

Transformation of anything into a weapon can happen by discursive materialization. If such statements are said in successive series, they lead into demonstrative reasoning. Reiterating cycles of statements are producing fields of concomitance that subsequently help legitimization of such efforts, which consequently materialize the problem. The already discussed mutual constitution between visible and sayable. This logic applies on overemphasis of exploits as cyber weapons as well as on overemphasis of communication satellites that can, if possess corrective ion engines, be understood as a kinetic weapon thanks to its maneuverability. It is therefore called a dual-use technology.[175] Pure discursive attribute. There is a normative layer of using a knife, we all know that knife is a weapon as well as an irreplaceable tool in a kitchen and it is up to the user how the tool will be used who usually understand the consequences. In the case of satellites and their maneuverability, which can be used to lower the orbital debris by deorbiting retired satellites or to direct a satellite against another one, the normative layer has not been developed yet and thus the discourse of dual-use technology is so powerful. The consequences are not clear and thus the attention is put on the capability to maneuver rather than on intention behind the capability, a peaceful and rational capability to deorbit. The doom scenarios prevail in discourse if uncertainty is present. The same applies on cyber threats; especially thanks to the attribution problem causing inability to punish the actor behind the possible attack. It is the same logic of criticism as we can observer elsewhere, for example Gartzke spent a significant part of his article to raise rationality in this way of thinking.[176] We all have knifes, but there is no carnage in streets, but we expect apocalypse in cyberspace. We usually hear that *everything is possible* and this statement drives the whole policy world into doom scenarios and to processes of adopting policies dealing with imaginative threats. The efforts to stop

[174] Ibid., 47.

[175] François Nadeau, "Examining the Effects of Anti-Space Weaponization Arguments in the Media: Some Experimental Findings from Canada," *Space Policy* 29, no. 1 (February 4, 2013): 67–75, doi:10.1016/j.spacepol.2012.11.004.

[176] Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth."

potentialities is not a preparation on possible catastrophe, it is a legitimation of particular policy application.

Michel Foucault in one of his text mentioned that the relevance of scientific invention or assertion in the Middle Ages, its truthfulness, was based on link to a particular person and its social status, hence the scientific value was derived from the authority of the author, but authority that emanate from much more solid and traditional social status and its kind.[177] The emergence of enlightenment with its emphasis on reason and rationale had not definitely dematerialized this power of discourse produced by authorities in their fields. Experts' texts calling for higher attention materialize their *truth* in semantic delimitation of such truth to possible negative outcomes when no measures are taken.[178] The relevance of the assertion is amplified by expectation that technical experts are relevant suppliers of expertise and thus suppliers of truth, which is accepted as granted – *epistemic community, advisory board or authority* in the role of the owner of relevant knowledge giving unbeatable advise leading to a production of threat politics. They are a representative of appropriate epistemic community, an authority; appropriate to bear the burden to draw the truth of forthcoming events, *"what gives the disturbing language of fiction its unities, its nodes of coherence, its insertion of the real."*[179] Including science fiction literature, in particular cyberpunk literature, is – to my opinion – eyes-opening approach as the literature contain exactly the kind of fiction that is later materialized in cyber policy imaginations.

Foucault understands the discourse as a *performative materialization* of truth rather than a mere linguistic construction. Disciplines, as this new one discipline of analyzing, assessing and evaluating of possible cyber security concerns in political decision making, tend to create their own borders, limits, principles of internal control and thus produce its own theoretical horizons in a set of concepts used in contextual relation to them or to other disciplines taken as relevant to their own objectives, e.g.

[177] Mark Olssen, *MICHEL FOUCAULT - Materialism and Education*, *America*, 1999, 173.

[178] Gary McGraw, "Cyber War Is Inevitable (Unless We Build Security In)," *Journal of Strategic Studies* 36 (February 2013): 109–19, doi:10.1080/01402390.2012.742013.

[179] Michel Foucault, "The Order of Discourse," in *Untying the Text: A Post-Structuralist Reader*, ed. Robert Young (London and New York: Routledge, 1981), 48–78.

security studies and the academic production that applies classical concepts on new security concerns.

New whole dimension of knowledge is created on experts' assumptions inspired by other experts' assumptions producing and repeating newly adopted concepts; it is a constructed and shared meaning about used concepts that leads into emergence of the whole disciplinary *perceptual field: "a corpus of knowledge that presupposed the same way of looking at things."*[180]

Newly created knowledge by processes of application of classical concepts on new realities is subsequently reproduced in repetitive discourses that consequently in time materialize as a new security agenda. How these different *perceptual fields* overlaps, influence each other, delimitate their own space of meaning by suing any critically oriented questions as *unscientific* or *blind to the truth* that, if ignored, might transform into Cyber World War III? What are the rules of formation and what are the conditions of existence of such discursive production of knowledge? How the repetition, transformation and reactivation of unimportant historical event by discourse form new reality of serious security concern? How new concepts produce new strategies against constructed threats in the perceptual field of respected experts? How have different cyber security discourses evolved, overlapped and influenced each other since their birth in historical perspective? … are the concerns of this research.

4.7. Method overview

ARCHAEOLOGY

1. *THE PERFORMATIVE MATERIALIZATION OF THE STRUCTURE*
   - Identify all the relevant ***statements***
   - Formation of new ***concepts*** (taken, adopted, incorporated into new contexts)
   - Putting the statements into ***logical*** and ***locutory nexus***
   - Drawing the formation of ***fields of presence*** *(fields of nexuses)*
   - *Producing the* ***fields of concomitance***

[180] Foucault, *The Archeology of Knowledge*.

- In their ***successive series*** and ***successive orders***
- Show how the ***demonstrative reasoning*** translate into new ***field of knowledge*** which is taken as granted
- Emergence of the ***church of knowledge***
- Beside – ***field of memory*** (concepts that are not relevant anymore, but which were at the beginning)

PERCEPTUAL FIELD

2. *THE GENEAOLOGY OF KNOWLEDGE 1 – EMERGENCE OF FIELD OF TRUTH*

- Order of the statements in time (materializing the structure in time)
- New ***security related statements*** > building on each other > ***field of truth***
- Incompatibility beaten by emergence of the *field of truth*
- How fields of truth produce policy that fits ***church of knowledge***

3. *THE GENEAOLOGY OF KNOWLEDGE 2 – ESTABLISHMENT OF TRUTH*

- The ***repeatability*** – continuous discourse production, validity deepening
- Establishment of ***new authorities*** by repeating the arguments of ***established authorities***
- Identification of ***correlations*** between different authorities, *bending the previous form different next* by correlations in ***constructed analogies***
- ***Correlatable constructed analogies*** – risk of reiteration of events based on ***materialized structural knowledge***
- Correlation as discipline within representative of church of knowledges
- ***Hierarchies of authorities*** (diagram how correlations influence layers of authorities)

POWER

4. *IDENTIFICATION OF SURFACES OF EMERGENCE*

- Where discourse prepare materialize the visible
- Surfaces that are the basis of future institutions – ***unbeatable systematized truth***
- Emergence of ***epistemic authorities*** – transformation from *epistemic community* to *epistemic authority* producing ***surfaces of emergence*** leading to *institutions* as *domains of application*

5. *DOMAINS OF APPLICATION*

- How new truths form new ***institutions*** – the production of result: materialization of new institutions with hidden church of knowledge inside
- Spillover effect/mirroring between authorities, construction of culture – establishment of the ***new norm*** backed by ***productive power*** (materializing the institution
- Comparison of state policies to uncover the mirroring process (cyber resilience in EU strategy)

5. PERCEIVING ACTORS IN CYBERSPACE AND THE NOTION OF DEMOCRACY

5.1. Three discourses to be studied

The amount of approaches to Foucauldian archaeology and genealogy of discourse is as numerous as the number of researches done. That is not an excuse to omit a method, it is rather an explanation why the each chapter of the empirical part significantly vary in their approaches to their respective objectives. Three discourses are studied; however, these discourses represent three different but intermingled realities. The extent of their interlinkage is discussed, but certainly not measured or put into unbeatable causal linkage. The flow of the discourse from one to other realities remains sufficient indication for the assessment that they mutually influence and constitute each other. Nevertheless, one can be confused not to find three discourses studied and rigidly compared. I avoided this approach exactly not to do the rigid depiction of three detached worlds sharing the same terminology and producing some debatable outcomes. I wanted to do rather the opposite: depict how these three worlds overlap each other. The method of their study was chosen differently as each discourse plays a different role in a constitutive process of our reality; finally, infinite realities in which they flow and oscillate. Three discourses are not flawless approach as I had to decide the number of discourses to put aside to each other and delimit their borders. Moreover, it would be audacious to construct such borders, but who can claim that one world influences the other while these realities may be one bigger covering all? These are of course dilemmas I had to accept when choosing the following approach.

The first chapter of the following part concerning techno-geeks and cyberpunk exists to depict the origin and evolution of a subculture that gave a row of terms and concepts to the current cyber security discourse – THE CONTENT. It does not study techno-geeks discourse in extreme detail; it rather introduces the genesis of critical concepts in literature. It would be nonsense to look deeply into the pit of cyberpunk and crypto anarchist movement to show the link with the forthcoming realities. Nonsense in the meaning of being lost in an ocean of postmodern dystopian world of people living in

cellars in case of far-left cyberpunk geeks or respectively being hidden behind white collars in case of crypto anarchists with a libertarian and thus far-right motivations. Hence I rather chose an approach to show the link between the genesis of certain critical concepts, their resonation in ideology formation and the final materialization of power. As said, the chapter ends with defining the particular power within the crypto anarchist movement; in that moment the power will be conceptualized by the ideology and empowered by the battery of concepts flowing from the techno-geek discourse. Since not only a *geek terminology*, but even a deep *crypto anarchic ideology* has made the *utopian ultra-libertarian world* without central authorities presumptively realizable, it is important to put these together as they both constitute this social reality despite their contradictory political missions. Terms such as hacker, cracker or cyberspace have born in science fiction literature, or better said in the cyberpunk subculture, and thus have had a particular meaning driven by idealistic belief into an ultra-libertarian future enabled by technology. To measure the extent of the cyberpunk subculture influence is not the objective of this work; however, the study of the discourse has been conducted in a way to show how the cyberpunk discourse has constitutive effects in further realities. One may find some parts a bit weird, e.g. why so much science fiction when we have to deal with *reality of cyberwar*? Well, literature certainly has a constitutive role in our political life. Omitting a defining discourse in the cyberpunk sub-culture is to my opinion one of the biggest mistake while drawing national security strategies. Knowing the ideology is exactly the foundation of any defensive measures against people having the idea to topple down the current international regime; especially – and that is not a secret to almost any specialist in cyber security – since the conventional force has lost its sense in cyberspace. Nation states are not fully in charge in cyberspace.

The second chapter of the following part takes the opportunity to show some evidence of cyber-crime and espionage. Both troubles simply have empirical evidence of its massive scale. These events are of course measurable, but the debate whether they are serious threats to national security or to placid lives of our citizens is an issue belonging to the discursive analysis. On the one hand, having a bank account siphoned is not a case of discursive analysis, but a case of evidence. The impacts to the society and finally also the numbers are issues discussed; who makes the final statements and what are the

consequences in their materialization is a significant portion of this chapter. As espionage has been here since the ages, its cyber layer can be understood as an understandable move in information society and thoroughly interconnected world. Cyber-crime, on the other hand, is a completely new phenomenon. The ability to massively steal money from thousands to millions of sources at once is something that previous criminals could dream about. However, what is the difference then? Is it *new normal* we have to live with or the banks have been caught unprepared against new skills computer networks simply gave to criminals? Both troubles are based on the interlinked world and its subsequent massive scale, at least reputedly *massive scale*. Well espionage is tacit and it does not impact a particular citizen; it is still based on statements heard from our politicians, whereas cyber-crime is an everyday reality each of us can experience. The amount of money stolen from banks is a value available from insurance companies, which back these issues of banks or the banks report it; these are clear numbers, but even them are interpreted and the decisions are made on the interpretation of these numbers. Finally, it is not hard to find numbers rising in front of your eyes on a webpage that possess particular authority with an objective to make you a bit panic. Presence of crime-espionage discourse was chosen to show how some particular objectives in crypto-anarchist movement might be interlinked to this dynamic; certainly the motives behind cyber-crime and how it enables cyber espionage. For example, there have been reports regarding the espionage campaign Red October claiming that a non-state actor has been behind.[181] How a non-state actor can be behind an espionage campaign of such a massive scale? They probably sell the information to governments and they certainly instill doubt between all the governments by doing so, because governments buy information about their adversary and at the same time pour money into a non-state infrastructure that spy on everybody to sell everybody. Pure cyberpunk dystopian nightmare.

The third chapter of the following part takes up on the previous ones to study how this doubt sowed by the realities of cyberpunk followed by cyber-crime and cyber-espionage constitute new national defense capabilities in a socially constructed space – cyberspace. There are examples in recent history that cannot keep us calm for sure;

[181] Miguel Alberto Gomez, "Operation Red October Fuels Debate over Cyber Espionage," *Eastasiaforum.org*, 2013, http://www.eastasiaforum.org/2013/02/07/operation-red-october-fuels-debate-over-cyber-espionage/.

however, the reaction of national administrations is building up new institutions, national security strategies, international cyber defense centers and all point to particular global threats in certain patterns. One cannot hide the imagination that drives all these motivations as we do not face an ongoing Armageddon from cyberspace, but some influential people tend to assert what we do on a daily basis. They also ignore investigations by responsible administrations to support the doomy fictional scenario of *cyber war*. The doubt sowed into the reality of cyber security at different levels probably fuels the drive of the possibilities in technological uncertainties and constitutes the national security agenda in cyberspace. However, at what basis remains a serious question. The fact that policy makers tend to secure us against possibilities, which probabilities remain hidden, is obvious. One can argue that environmental degradation on a global scale is reaching a no-way-back point and as all these assertions are backed by serious research reports, based on advanced infrastructure from underground to space, used by wide variety of interdisciplinary experts, the threat we face is unquestionable.[182] However, it is not an exception that a national security strategy contains cyber as the biggest threat to our lives, which is certainly not based on scientific results, but on possibilities based on imaginations[183] or deductions coming from a limited amount of scary events. Focus on high-impact low probable events instead of on low-impact but high probable events, which in a row of its reiterations can cause that massive troubles with cyber-crime has been criticized already.[184] This chapter has an objective to show how these imaginations flow in a hard-to-grasp post-modern environment and how the *technological radical uncertainty* causes new imaginations that materialize in new state-held power. Finally, one can ask whether the genius people behind the crypto-anarchic movement, who are paradoxically building less anarchic society in their decentralized self-control utopia, are not the case of policy makers' imaginations or whether the policy makers are even aware about this slowly coming dystopian nightmare where nobody governs.

[182] NASA, "Scientific Consensus: Earth's Climate Is Warming," 2016, http://climate.nasa.gov/scientific-consensus/.

[183] Kaiser, "The Birth of Cyberwar."

[184] Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better."

The following table shows the perspectives I have taken, while studying the intermingled discourses and what features I observe in each of them and what relations (>>>) between them.

	CYBER-PUNK	CYBER-CRIME	CYBER-WAR
Function	constitutive	evidentiary	imaginative
Founding policy	idealism	realism	threat politics
Effects	forgotten	exploding	overemphasized
Discursive influence	>>> hacker becomes criminal >>>	>>> evidence transfer >>>	>>> hacker implies terrorist >>>
Resulting role	hero	criminal	terrorist

Table 1 - Perspectives taken in the following three discourse analyses

5.2. The interwoven discourses and a bit of their evolution

In the Table 1, three evident detached worlds are visible. The point of the table is to depict the dynamics between these three worlds; how they relate to each other, construct each other from left to right and finally how they represent socially constructed three worlds instead of being separated in the reality. While the cyber-punk environment has a constitutive function in meaning of constituting particular concepts, life visions or life styles, being driven by deep idealism visioning bright future of independent individual, the following worlds build on it and I would argue they do so unintentionally. As will be described in detail, here, I show how a concept *hacker* from cyber-punk culture became a concept in cyber-crime discourse and later also a concept in national security discourse.

In the former world, *hacker* means a bunch of skills that help one to survive out of the vision, surveillance, state control, the establishment or – as usually written in the cyber-punk literature – within a system by understanding it through its decomposition, deconstruction or using the geek language trough *reverse engineering*. In the middle world, *hacker* became a symbol of criminal offense. The one who violates law and has to be prosecuted according to law. However, cyber-crime is reality and despite extreme

fluctuation between debatable interpretations of losses, the fact that banks are under pressure of people willing to siphon their money in electronic means is undisputable. Examples such as the code Zeus helping to steal identification to prevalently internet banking systems, which became open-source and thus available to masses[185] depict the reality enough without statistical punctuality. Zeus did not attacked banks, but users' computers who then gave all the needed identification to attackers as they were deceived that they were giving the information to their bank, quite a successful fraud.[186] Zeus is just an example and I will use other examples to demonstrate how the cyber-crime discourse builds on an empirical evidence. The construction of a threat is then quite successful, because the *technological radical uncertainty* behind gives politicians powerful weapon in their mouth while asking for new Acts, laws, directives, institutions and finally even preventive offensive actions. I also show some particular examples how clear hacktivism without profit oriented objectives or intentions to harm become national security agenda.

The cyber-war discourse then lies precisely on this cyber-crime evidence amplified by the uncertainty of politicians through discourse. *Hero* in the eyes of crypto-anarchist movement is becoming *criminal* when attacking banks or selling DDoS attacks on the black market and subsequently is becoming a *terrorist* who can fire their DDoS spikes against the shields of critical infrastructure causing spill of data napalm in the streets.

There have been different perspectives how to approach, depict and understand troubles behind the computers and their networked environment in the past. *Cyber security* was understood as a *computer security* or we can say *data security* to avoid confusion with current connotation of *information security* in propaganda issues. The following list of bullet points show how the perspectives have evolved, I am choosing the super-famous securitization quotations to depict the present time:

[185] Peter Kruse, "Complete ZeuS Sourcecode Has Been Leaked to the Masses," *CSIS*, 2011, http://www.csis.dk/en/csis/blog/3229.

[186] FBI, "FBI — Manhattan U.S. Attorney Charges 37 Defendants Involved in Global Bank Fraud Schemes That Used 'Zeus Trojan' and Other Malware to Steal Millions of Dollars from U.S. Bank Accounts," *Fbi.gov*, 2013, http://www.fbi.gov/newyork/press-releases/2010/nyfo093010.htm.

- Computers can spill sensitive data and must be guarded (1960s)[187]
- Computers can be attacked and data stolen (1970s) [188]
- We can build computer attacks into military arsenals (1980s and 1990s) [189]
- Others might do that to us – and perhaps are doing already (1990s) [190]
- Electronic Pearl Harbor (1995s) [191]
- Marching signal crossing border in first ever cyber-war (2000s)
  "[An] Russian invasion force … of digital signals marched across the border into Estonia in very large numbers and shut down the main Estonian bank" quoting the author of cited article[192]
- Cyber espionage constitutes the *"greatest transfer of wealth in history"* quoting chief of NSA Keith Alexander (2010s)[193]
- Waiting for a *"cyber-Pearl Harbor"* (2010s) [194]
- Fighting imaginative cyber-war by collecting masses of data is not about security of citizens, but about power of state,[195] which is blurring with emergence of other actors[196] and network assemblages[197] (2010s)
- Organized hacking empires (2016)[198]

[187] Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* 27, no. February 2015 (2012): 781–99, doi:10.1080/02684527.2012.708530.

[188] Ibid.

[189] Ibid.

[190] Ibid.

[191] M E Bowman, "Is International Law Ready for the Information Age," *Fordham Int'l LJ* 19, no. 5 (1995): 1935; Michael Rustad and Lori E. Eisenschmidt, "Commercial Law of Internet Security, The," *High Technology Law Journal* 10, no. 2 (1995): 213, doi:10.15779/Z38QX0H.

[192] Robin Bloor, "Large-Scale DOS Attack Menace Continues to Grow," *The Register*, June 11, 2007, http://www.theregister.co.uk/2007/06/11/dos_security_cyberwarfare/.

[193] Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'greatest Transfer of Wealth in History,'" *Foreign Policy*, July 9, 2012, http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/?wp_login_redirect=0.

[194] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, October 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

[195] Bauman et al., "After Snowden: Rethinking the Impact of Surveillance."

[196] Myriam Dunn Cavelty, V. Mauer, and S.F. SF Krishna-Hensel, *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace* (Ashgate Publishing, Limited, 2007).

[197] Rita Abrahamsen and Michael C. Williams, "Security Beyond the State: Global Security Assemblages in International Politics," *International Political Sociology* 3, no. 1 (March 2009): 1–17, doi:10.1111/j.1749-5687.2008.00060.x.

[198] The~Economist, "Hackers Inc.," *12th July*, 2014.

The visible link between the actions of people behind computers and military discourse has been quite clearly visible since the Estonia events in 2007. The author of the article uses also terms such as *collateral damage* of cyber warfare and asking a question whether the adversary was *government Russia* itself or *Russian hackers*.[199] The attacker is also blurred, what gives states a great opportunity to use so called *plausible deniability* in order to circumvent international law by exploiting the attribution problem. A move that I named *dual interest of states*.[200]

Moreover, very famous is the speech given by Department of Defense secretary Leon Panetta in 2012. There have not been too many such extremely impactful speeches in the last years; this one resonated so much that we can clearly point to all the impact, which is visible in following text as he chose particular significant words*. "An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches,"* Panetta said. *"They could derail passenger trains, or even more dangerous, derail passenger trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country."*[201] Panetta used strong metaphors such as Pearl Harbor, which has a specific emotional effects on American citizens: *"cyber-Pearl Harbor that would cause physical destruction and the loss of life, an attack that would paralyze and shock the nation and create a profound new sense of vulnerability."* [202] The imagination included in his speech is visible to the reader immediately; however, when said by such a high-rank official, the ideas are taken as granted, as a possible future. We train students in cyber 9/11 competitions to ensure the new generation how serious the situation is.[203]

However, the term "cyber-Pearl Harbor" can be found in literature quite earlier than Panetta has his own speech. In particular, Richard Clark falls into the category of people who like to use metaphors, construct securitization discourse and finally use false

[199] Bloor, "Large-Scale DOS Attack Menace Continues to Grow."
[200] Schmidt, "Super-Empowering of Non-State Actors in Cyberspace."
[201] Bumiller and Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S."
[202] Ibid.
[203] Atlantic Council, "About the Cyber 9/12 Student Challenge," accessed April 22, 2016, http://www.atlanticcouncil.org/programs/brent-scowcroft-center/cyber-statecraft/cyber-9-12/about-the-cyber-9-12-student-challenge.

information in his argumentation;[204] he used this term already in 1999.[205] Clark can be seriously (one of the) responsible in introducing the term *cyber* before *Pearl Harbor* as before 1999 we can observe *electronic Pearl Harbor*[206] and also some criticism how improbable it is.[207] In another part of Panetta's speech in 2012 he focused on how he is not willing to violate rights or liberties: *"We're not interested in looking at e-mail, we're not interested in looking at information in computers, I'm not interested in violating rights or liberties of people."*[208] However, Snowden revelations unveiled quite a different reality of US security policy in practice. I argue that these speeches are directly focused on strengthening relevance of securitization discourse, which consequently gives power to particular institutions. As I said it did not need to be intentional, it could be just unwise. However, deepening state power is the argument of those, who could not withstand the surveillance reality: *"These programs were never about terrorism: they're about economic spying, social control, and diplomatic manipulation. They're about power."*[209] In my country of the Czech Republic, even here in a small country of 10 million inhabitants we can observe extreme exaggeration of events that never took place by highest responsible persons who are securitizing cyber as they need to support agenda of a particular institution. The events of electric blackout in Israel mentioned by the director of National Cyber Security Center have never took place, but was mentioned on a day of prime minister visit to the Center, which was also devoted to the debate about future budget.[210]

5.3. The fight for power and the notion of democracy

The following table should serve as an additional one to the previous table concerning three discourses. Here, the point is to show a list of actors that operate in the

[204] These findings are discussed in the chapter National leaders and the (un)certainty of the future of national security.

[205] Richard Clarke, "Threats to US National Security: Proposed Partnership Initiatives towards Preventing Cyber Terrorist Attacks," *DePaul Business Law Journal* 12 (1999): 33–44.

[206] Bowman, "Is International Law Ready for the Information Age"; Rustad and Eisenschmidt, "Commercial Law of Internet Security, The."

[207] George Smith, "An Electronic Pearl Harbor? Not Likely," *Issues in Science and Technology* 15, no. 1 (1998): 68–73.

[208] Bumiller and Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S."

[209] Edward Snowden, "An Open Letter to the People of Brazil," *Pastebin*, December 17, 2013, http://pastebin.com/2ybz27UE.

[210] HEG, "Česko Je Podle Sobotky v Evropě Vzorem v Kybernetické Bezpečnosti. Hrozba Hackerských Útoků Ale Stoupá," *Hospodářské Noviny*, 2016, http://domaci.ihned.cz/c1-65206270-cesko-je-podle-sobotky-v-evrope-vzorem-v-kyberneticke-bezpecnosti-hrozba-hackerskych-utoku-ale-stoupa.

cyber-space. These actors do not need to be perfectly distinguishable from one or another such as *states* and *foreign countries;* they certainly overlap. However, state in a role of a foreign country plays that *dual interest game* I introduced earlier already. Moreover, one may consider crypto-anarchists being probably for 99% geeks, but that would not include people who are more focused on technology usage rather than on technology development. While geeks are developing particular technologies in order to alter the system, crypto-anarchist use these technologies to hide themselves from the state to reach their political objectives in ultimate liberation of society, and, from a state of course, which is understood as a principal evil abusing its power. Cyber criminals might be super organized international networks with their own marketing, selling, strategy departments,[211] but they might be individuals doing things that are simply not in the interest of states. For example, encryption technologies have had to be registered at the state administration in Russia since the year of 2001;[212] not all operators follow this law of course as the tools can be obtained easily elsewhere; however, they are approached as criminals breaking the law. Actors including geeks, crypto-anarchists, cyber criminals and also foreign states hidden behind the attribution problem are empowering themselves through cyberspace, they support development of particular technologies enabling them towards their objectives. Geeks deepen them through open-source concept of open development groups of hundred thousand people; crypto-anarchists use them to enable their ultra-liberal ideology as they slowly move from idealistic anarchism to anarcho-capitalism, cyber-criminals to support their international criminal networks in reaching an objective of gaining profit and foreign countries in collecting industrial espionage.

When we move from criminal sphere to intelligence, we can observe a bit of overlap between crime and espionage operations; the division can be made easily on the ground of actors. While an action of an individual is a criminal offense, the same operation done by military personnel is understood as an espionage operation. However, there are examples of espionage operations run by private networks where clients are states –

[211] The~Economist, "Hackers Inc."
[212] Christian von Wistinghausen, "Certification and Licensing of Encryption Software in the Russian Federation," *Rus Soft*, October 31, 2001, http://russoft.org/docs/?doc=88.

already mentioned Red October operation. U.S. national intelligence was caught spying on millions of its own citizens when the national defense secretary was arguing that the state has to be secured from extremist groups by taking a bit of our privacy and ensuring the public that the national security bodies are not interested in our personal lives. This was responded with a certain reservation that collecting metadata is not violating individual rights and that the computers storing metadata do not violate privacy per se and thus that the program qualify on both constitutional and legal grounds[213] and that unveiling national security by Edward Snowden or the journalists who published his leaks are not judges over the national security.[214]

However, the result of these revelations are a lower belief into liberal democratic regime represented by current democratic nation states. Moreover, the representation of the states is blurring with transnational intelligence networks as these metadata cannot be easily identified to particular nationality and additionally through mixing the operations with other actors in processes of transnationalization, digitization and privatization by participating transnational corporations and private contractors.[215] National intelligence under the light of Snowden revelations operate much more autonomously on state control. Questionably in order to support democratic values. National security is no longer national, law enforcement overlaps with intelligence and certainty in low amount of data has transformed into blurred uncertainty of large amount of data. States are disappearing in their own efforts to strengthen national security by violating the foundational norms of liberal democracy and participating on intelligence practices with transnational corporations.

[213] Amitai Etzioni, *NSA: National Security vs. Individual Rights*, *Intelligence and National Security*, vol. 00, 2014, doi:10.1080/02684527.2013.867221.

[214] Edward Lucas, *The Snowden Operation*, 2014.

[215] Bauman et al., "After Snowden: Rethinking the Impact of Surveillance."

ACTORS	DIS.	ADVERSARY	OBJECTIVES		METHODS		IMPLICATIONS
Geeks	**1**	no-one, alters the system	empower through cyberspace	deepen the technological complexity	specific knowledge	sw/hw development & disentanglement	**EMERGENCE OF SPECIFIC TECHNOLOGIES**
Crypto anarchists	**1**	nation state system		ultimate liberation of the society		networked social structures	**MASSIVE USE OF CERTAIN TECHNOLOGIES**
Cyber criminals	**2**	law enforcement agencies		revenue		transnational criminal networks	**ABUSE OF THE TECHNOLOGIES**
Foreign countries	**2**	national counter intelligence		industrial and state espionage	hidden behind attribution problem	massive penetration of networks & buying information on a black market	**ESCALATION OF ACTIVITIES & THREAT PERCEPTIONS**
National Intelligence	**2**	foreign countries	national security	proactive prevention	gathering intelligence	active probe of information flow	**LOWERING CONFIDENCE IN LIBERAL STATE**
Law Enforcement	**2**	cyber criminals		proactive punishment	prosecute criminals	forensic analysis of past	**LOWERING OBSOLETE CRIME & DEEPENING COMPLEXITY OF FUTURE CRIME**
States	**3**	terrorists/geeks, crypto-anarchists, foreign countries, intelligence		national defense	securitization of international terrorism	construction of institutions & power materialization	**MORE POWERFUL & LESS CREDIBLE STATE**
Corporations	**1-3**	ALL	revenue	good relations with states, *for now*	securitization of critical infrastructure	technology standardization	**MORE VULNERABLE NATIONAL SYSTEMS**
Citizens	**1-3**	ALL	DEMOCRACY, independence on state & corporate control	personal profit	using tools making life better	adopting crypto-anarchist tools	**LOWER DEPENDENCE ON STATE**
Artificial Intelligence	**F**	- ? -	following tasks	semi-autonomous self-alteration	environment alteration	technology self-evolution	**UNCONTROLLABLE AI "CRIME" AND "ESPIONAGE"**

Table 2 - Actors recognized in the following three discourse analyses

Finally, the discourse taken by state representatives in order to secure citizens from extremely low probable lethal death by a single terrorist attack is about a raising fear in uncertainty of who is the security provider. States fight desperately for a continuous reason of their existence, but one cannot deny that other actors involved in

national security would eventually produce intelligence according to their own interest[216] and thus slowly produce environment in their own favor rather than in favor of the nation state. This process is having an impact on how citizens and states approach differently the question of privacy and finally how states tend to reconfigure the ideas behind the notion of privacy instead. The transnationalization of the national security intelligence gathering finally leads into clearly autonomous transnational arena, in which no actor is even able to recognize each other; non-recognizable nationality is far away from this problem of emerging actors that are not driven by values of democracy. Here, we are not talking about authoritarian regimes only, several glimpses of upcoming capabilities artificial intelligence show that we have to take this new actor to the game.

The table above should serve as a steer for orientation in the following text. Dividing three discourses into three different branches for further and isolated discourse analysis would be simplifying approach as discussed just above the table. However, three worlds of different arguments are studied in their respective foundations and relation to national security and finally in order to discuss the perspectives of global governance under democratic ideas in the world of transnational networks based on cartographies of electrical circuits rather than territories of sovereign states.

[216] Ibid.

THREE ARCHAEOLOGIES OF DISCOURSES MATERIALIZING CYBER SECURITY AGENDA

I.

TECHNO-GEEKS, CYBERPUNK AND THE UNTOUCHABLE ANONYMOUS EXCEPTIONAL GENIUSES

“You mean old books?"

"Stories written before space travel but about space travel."

"How could there have been stories about space travel before --"

"The writers," Pris said, "made it up.”

— Philip K. Dick, Do Androids Dream of Electric Sheep? (1968) —

1. WHY CYBERPUNK?

The following chapter explains the relation between cyberpunk subculture of the 1980s and national cyber security agenda in 2000s, the list of indications of this relations follows.

Firstly, one of the clear reason why to start with the cyberpunk subculture is the fact that it not only produced the word *cyberspace,* but also words such as a *hacker* or a *cracker.* The word does not have only a meaning, but mainly it has a specific connotation developed in fictional works by the classical cyberpunk literature author William Gibson. Experts in cybersecurity have done tough work until today to define the term *cyberspace* in national security relations; however, I would argue that they consciously omit the postmodern layer of its meaning. We can look at the national cyber security strategies and they are full of threats of possible attacks emanating from cyberspace, while these threats are defined so baldly, based on imaginations rather than on empirical evidence and empirical evidence does not significantly change the imaginations (as will be shown for example on Ukraine blackout in 2015). During the debates concerning Confidence Building Measures in cyberspace at the headquarters of Organization for Security and Cooperation in Vienna in years 2012-2013 diplomats agreed that they simply do not know what cyberspace is. The question of territoriality and their consequent mandate to even discuss the topic on behalf of a nation state was put into question.[217]

However, clear static positivist definitions do not only help policy makers to understand its meaning in a simple way, they neglect its real interaction with (social) reality. It is important to understand its dynamics in societal world to develop an appropriate security policy or put differently, it is important to understand the perspective taken by those who conceptualize it in security matters to unveil the source of their threat perspective. Imaginative perspective. What kind of policy can be applied when policy makers perceive cyberspace from a national security perspective while people who keenly work on its existence, and finally its shape as well, see a kind of different world? Especially a world that can create ultimate liberty?

[217] Based on personal observations of the OSCE meetings as an invited expert on cyber security in years 2012-2013 on behalf of the Czech Republic.

Secondly, cyberpunk does not provide us with utopian futures such as classical science fiction. It has much more to do with dystopian prediction of near future based on a present world. In that perspective, cyberpunk provides us with an insight into the inherent reality around us; a bit fictional explanation of current technology development implications to the society. Depicting the dystopian world might easily constitute the reality around as it might shape the imaginations of those, who constitute our social reality by adopting certain policy solutions. Especially under the *technological radical uncertainty*.

Thirdly, cyberpunk is a path-defining subculture for those who possess particular abilities in shaping, controlling, programming and inventing (communication) technologies. Not only because it gave us the word *cyberspace*, but – as said – also words such as *hacker* or *cracker* and along with these words, the devotions of people with the ideology of ultimate liberty. Social construction of these words defines the desirable activities of the in-world *operators,* currently of every internet user willing to gain power in cyberspace.

Fourthly, cyberpunk provides a specific legitimation of techno anarchy or legalization of activities that are understood as a crime in the real world; libertarian legalization that depicts new business models as a progress of modernity. Just remember the debate[218] between Google and book publishers; now it is clear what is legitimate behavior, but during the time when google provided all the scanned books online for free, or was selling reprints, the debate concerning intellectual property was really hot and the legitimate perspective was blurred by the libertarian expectations of newly emerging communication technologies. Google then switched to show only a portion of the book, but even accusation about snippets from the books was not accepted easily and had finished a bit later.[219] Additionally, remember all the other currently dead services such as Napster[220] who's founder later won the case with BMG and EMI. Later on, when he won

[218] Eric Pfanner and James Kanter, "Google Tries to Calm Europe Over Book Deal - The New York Times," September 7, 2009, http://www.nytimes.com/2009/09/08/technology/internet/08books.html.

[219] Jonathan Stempel, "Google Defeats Authors in U.S. Book-Scanning Lawsuit," *Reuters.com*, November 14, 2013, http://www.reuters.com/article/us-google-books-idUSBRE9AD0TT20131114.

[220] BBC, "MP3 Sites Accused of Music 'Hijack,'" *BBC News*, July 12, 2000, http://news.bbc.co.uk/2/hi/americas/829668.stm.

the sue, received about $20 million to shut down Napster and invested in Facebook. Napster was dead, but new decentralized sharing open source tool DC++ emerged very quickly and now has about 90% of peer-to-peer sharing market with no possibility to shut it down as no individual is behind it. Another example would be the service Megaupload who's founder became a cult hero after seizing the servers and himself.[221] The case of Megaupload raised very novel doubts over law enforcement operations out of the respective territory as American FBI seized him in New Zealand without knowledge of local authorities. However, there are still technologies that are almost unbeatable: torrents or The Onion Network – TOR. All these cases share the same values – to alter the legitimacy of the real world in cyberspace.

Fifthly, cyberpunk follows writings of post-modern authors such as Baudrillard. An idea that the world will be governed by corporations which inject themselves into our hearts and minds even with electronics is a *dystopian technological nightmare* that drives the current crypto-anarchist movement in developing an alternate world to the one states are organizing. The liberalization from states into techno-altered humanity where each individual can alter even a human body by open source community driven and self-controlled technology is the utopian vision of the current crypto-anarchist movement. However, that does not stop it from achieving the utopia visions. Globalization in its radical decentralized shape[222] is in their imagination possible with the plethora of technologies currently available such as global digital currencies (Bitcoin)[223] that do not have authorities above it. While states tend to keep it under control,[224] the ultra-libertarian crypto-anarchist movement sees a bright liberal future of toppling down the dominance of nation states by tools like that[225] and discussing whether they can withstand an attack by state.[226] Why so much animosity between the two?

[221] Jonathan Hutchinson, "Megaupload Founder Goes From Arrest to Cult Hero," *New York Times*, July 3, 2012, http://www.nytimes.com/2012/07/04/technology/megaupload-founder-goes-from-arrest-to-cult-hero.html.

[222] P Barša and O Císař, *Levice v Postrevoluční Době: Občanská Společnost a Nová Sociální Hnutí v Radikální Politické Teorii 20. Století*, Politika a Společnost (Brno: Centrum pro studium demokracie a kultury, 2004).

[223] Satoshi Nakamoto, "Bitcoin : A Peer-to-Peer Electronic Cash System," 2008, 1–9.

[224] Plassaras, "Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF."

[225] Robert Kutiš, "Bitcoin - Light at the End of the Tunnel for Cyber-Libertarians," *HeinOnline* 8, no. 2 (2014): 214–21.

[226] Andrew Kim, Daryl Sng, and Soyeon Yu, "The Stateless Currency and the State: An Examination of the Feasibility of a State Attack on Bitcoin," 2014, 1–32, http://randomwalker.info/teaching/spring-2014-privacy-technologies/state-attack.pdf.

Sixthly, it seems that states are a bit disoriented in this world. State authorities even paradoxically developed some key technologies, e.g. TOR was probably developed by US military,[227] that is currently used to create so called *"Dark net"*, a symbol of ultra-libertarian technological war against suppositious nation states dominance and deemed oppression. A term, that depicts nothing else than a portion of current internet network; but that definition depends on context. It can depict the way how internet is used only, so it is not a subspace of the cyberspace. Saying about some servers that they are part of Darknet only because they are not indexed by search engines. However, it is untouchable and uncontrollable by nation states, which certainly dislike this fact, so they call it *dark net.* It is nothing else than encrypted communication on Internet, which is about illegitimate and criminal activities. It is not a network of vampires as it might look like from a dystopic term *Dark net.* This shows how developing tools are clearly a double-edged sword; the development of Stuxnet by US and Israeli intelligence and its backward usage against US allies during the Saudi Aramco cyber-attack would serve as another example.

Seventhly, the beliefs of an ultimate open society literally a battle between its protagonists and traditionalists. Napster existence in 2000 had finally led to emergence of paid streaming services such as Spotify (2008) or Netflix (founded in 1997 as a DVD-on-demand provider and started streaming services in 2007). However, the battle over unconditional access to humankind knowledge is hard to ignore in academic world. SciHub or Library Genesis show clearly that their values are the unconditional access to knowledge to everybody, not making money on a knowledge of somebody else. They defy accusation that they violate intellectual property as they disagree with the whole concept of intellectual property when it comes to a production of knowledge. In this perspective, *dark net* can be understood as a *"public's great equalizing force in the digital millennium"* and might led to a global revolution of particular services.[228] It is a kind of resistance against widely accepted norm of paid access to knowledge. Such a resistance behavior is

[227] Timothy B. Lee, "Everything You Need to Know about the NSA and Tor in One FAQ," October 4, 2014, https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/everything-you-need-to-know-about-the-nsa-and-tor-in-one-faq/.

[228] Jessica A Wood, "The Darknet: A Digital Copyright Revolution," *Richmond Journal of Law and Technology* 16, no. 4 (2009): 1.

shaking with nation states, which tend to preserve their credibility by successful tackling with securitized threats that can be tackled only by traditional law enforcement institutions; however, they clearly understand their growing inability to tackle with the violation of intellectual property or illicit financial transactions or other crimes conducted by adaptable criminals in cyberspace,[229] so they call for cyber defenses against possible cyber terrorism, which is based on dystopian imaginations. When hackers get access to a bank, national security specialists immediately rise attention to that attack and start depicting consequences providing a similar attack is conducted against critical infrastructure.

Eighthly, we do not need to draw dystopian future of humans merged with or augmented by technology to see how technology has influenced human lives; the information time is not a special moment, it is only a bit different to the previous ones. However, the raise of services such as global accommodation service AirBnB or global taxi provider UBER or the raise of Bitcoin (in particular the universal confirmation technology blockchain) show how services can be delivered accordingly, fairly and reliably without nation state intervention, but with tremendous disasters to established business models. Specifically, they do not need legal environment created by states as the service heavily stand and fall with good references of its users; both sides of the contract. It leads to an ultimate "trustless" functioning interaction neoliberal system without central institutions including enforcement mechanisms.[230]

If one asks a question where is the origin of all the dystopic doom-like scenarios of possible cyber-attacks on national critical infrastructures nation states serve us on a daily basis, the first step should be to ask where the concepts they use come from. It is a crystal clear fact that a lot of words, terms and concepts were developed in cyberpunk literature and nowadays are established terms in national security strategies. Combining them with emotional historical events such as Pearl Harbor is a clear discursive social construction of reality that is seriously reflected in cyber security national strategies. However, the transformation of fictional dystopian visions into security imaginations

[229] Christopher Bronk, Cody Monk, and John Villasenor, "The Dark Side of Cyber Finance," *Survival* 54, no. 2 (November 14, 2012): 129–42, doi:10.1080/00396338.2012.672794.

[230] Trevor I Kiviat, "Beyond Bitcoin: Issues in Regulating Blockchain Transactions," *Duke Law Journal* 65, no. 3 (2015): 569–608.

leads to predictions based on fictional basis. The reason to include cyberpunk in the following dissertation is clearly to depict how fictional content can easily transform to seriously reflected imaginations that has nothing to do with real threats emanating from communication technology; or at least with that threats we should be scared of. However, as Gartzke put it, we do not need to be scared of a cyber war as we are not scared that every second person on the street will stub us with a kitchen knife.[231] I decided to study cyberpunk in philosophical perspective of Jean Baudrillard as he contributed to the debate with post-modern thought that is closely related to the same philosophical basis as cyberpunk. Cyberpunk as a dystopian nightmare is an opposite to grand ideological narratives of modernism, an opposition to rationality, objectivity or concept of absolute truth; it studies the environment in its fluid substance rather than analyzes it as a perfect composition assembled rationally in the best shape, here the skepticism arises. Nothing is right, authorities are wrong, corrupted and hostile to the liberty of people, the resistance must arise and do the best to topple down the shadow curtain from the society.

[231] Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth."

2. THE BRIEF ETYMOLOGY OF CYBER AND CYBERNETICS

A short etymological insight into a word *cyber* may explain the reason why we have shifted from computer security to cyber security despite the fact that both terms are about the same. There are more logical and meaningful links between *cyberpunk* culture and the word *cyber* than *cyber security of critical infrastructure* and the word *cyber; the dilemma in cybernetics of critical infrastructure* would be much more appropriate to the problem we think we face. Cyber as a word has etymologically come from the Greek word kubernētēs (κυβερνᾶν), or *kybernetikos*, which means *to steer* or *steering*. The word has its version in Latin as *gubernetes* or in a later form *gubernator*, which does give us better understanding of its etymological root. The first ever use of the word can be dated to ancient Greece, in Plato's work named The Alcibiades, in which Plato studies the possibilities of self-governance.[232] Governance here makes the distinction between found-in-nature and made-by-culture. Science and cybernetics are indistinguishable as both are *"multi-causal, non-linear, synergetic, impossible to fathom, and difficult to control or even guide."*[233] Cybernetics is about the scientific enquiry of governance; the art to govern or to self-govern in evolving iterations. We use the term *cyber* as we think that we need to control technology development related to computer security; it comes from an ambition to govern cyberspace by controlling the technology development, e.g. whether encryption is allowed or denied.

Cybernetics is about the scientific enquiry of governance; the art to govern or to self-govern in evolving iterations based on feedback, historical implications, refining the goal, finally a "*dialectics or 'conversations' among the bits, bytes, and constituent subsystems of coevolving nature and culture."*[234] Deriving from this intertwining interaction we can say that cybernetics is a kind of science, the art of communication, feedback and control. It is an ability to govern technology, hence, in our language of science and technology studies, it is a *governance of technology*. Governance that include the ability to understand consequences related to decisions over technology

[232] Plato, *Alcibiades I & II* (1st World Library Literary Society, 2004).

[233] Barnabas D. Johnson, "The Cybernetics of Society: The Governance of Self and Civilization," accessed March 19, 2016, http://www.jurlandia.org/cybsoc.htm.

[234] Ibid.

development and application. It does not matter whether the constitutive agents are natural or cultural. It consists of both, the natural, biological, mechanical or cultural elements that need governance based on development of knowledge converted into choice and then into action. [235] The needed knowledge is visible in the Socrates' argument criticizing a man, in a dialogue with Alcibiades, ignoring the result of making a decision leading into action. The evolution of knowledge, its ability to propagate, qualitatively increase and keep the responsibility of the impacts of that decision to the man – knowledge that constitute morale. Kubernētēs is a navigation skill in the naturally-cultural world; a capacity to understand what is moral. Everyone has a certain power, but that power can be used in a tyrannical way or in virtue. Nobody would be happy if the aim was to gain power in a tyrannical way, but would be happy, if the power is used in virtue. [236]

[235] Ibid.
[236] Ibid.

3. THE ORIGINS OF CYBERPUNK IN A RECENT PHILOSOPHICAL THOUGHT

Jean Baudrillard, as a member of French post-structuralist school, is also significant in his post-modernist perspective. Baudrillard among the other classical post-structuralists (Julia Kristeva, Michel Foucault, Jacques Lacan, Tzvetan Todorov, Jacques Derrida, Louis Althusser, Gilles Deleuze, Jean-François Lyotard or René Girard)[237] arrived as a prophet of post-modernity. In his world, *"classes, genders, political differences, and once autonomous realms of society and culture imploded into each other, erasing boundaries and differences in a postmodern kaleidoscope."*[238] Individuals in this world are escaping from the *desert of the real* into a new realm generated by new technologies, computers, media and ecstasies of *hyperreality*.[239] He prophesizes the dissolution of borders and territories in favor of *precession of simulacra – "a map that engenders territory and if we were to revive the fable today, it would be the territory whose shreds are slowly rotting across the map*."[240] When Baudrillard talks about the hyperreality and disappearance of reality, *the desert of reality*, the text is full of typical postmodern anxiety. *"It is nothing more than operational. In fact, since it is no longer enveloped by an imaginary, it is no longer real at all. It is a hyperreal, the product of an irradiating synthesis of combinatory models in a hyperspace without atmosphere."*[241]

Baudrillard, in the comparable way as Zygmunt Bauman,[242] was a strong critic of consumer world.[243] While Bauman is famous for his concept of *liquid modernity*, which is a construction stone of post-modern thought and the row of recommendations how to get oriented in such a persistently changing world, Baudrillard criticizes the current flow of *repeatedly recopied reality* as a playback without any possibly meaningful intervention in the process by an individual. He sees a mysticism behind the notion of equality, a notion that is supposed to fuel democratic ideology; however, in fact it *"conceals the absence of*

[237] Peter Pericles Trifonas, *Barthes and the Empire of Signs*, *Barthes and the Empire of Signs* (Totem Books, 2001), 4.

[238] Douglas Kellner, *Media Culture: Cultural Studies, Identity and Politics between the Modern and the Postmodern* (London and New York: Routledge, 1995), 297.

[239] Kellner, *Media Culture: Cultural Studies, Identity and Politics between the Modern and the Postmodern*.

[240] Jean Baudrillard, *Simulations* (New York, NY, USA: Columbia University, 1983), 6.

[241] Ibid., 7.

[242] Zygmunt Bauman, *Umění Života* (Praha: Academia, 2010); Zygmunt Bauman, *Liquid Modernity*, *Contemporary Sociology*, vol. 30, 2000, doi:10.2307/3089803.

[243] Jean Baudrillard, *The Consumer Society: Myths and Structures* (London: SAGE Publications, 1998).

democracy and the non-existence of equality."[244] Consumer ideology constructs needs with reassuring ends; fulfilment of these needs is an objective of universal equality, with no privileged individuals, not so different to utopian communist society. Baudrillard then put it that the final equilibrium is hard to achieve, the final harmonized and freed society as a whole political game of welfare state is utopia as the needed growth in the exchange process itself causes the inequality.[245] Baudrillard's world is not only about excessive consumption, he sees failing system on an emergence of new simulated system that is served to citizens as an answer to their needs. Flattering culture into a consumerist culture, where media does not serve but dominate, where information is not about curiosity but materialize power, and where technology and human beings merge and thus lose control of their previous meant extension into new techno-environments.[246]

Baudrillard in one of his work combines thoughts about reality, *Integral Reality*, power and evil.[247] The irreversible flow of destiny into *Integral Reality*, the kind of reality we cannot understand as a clear reality, but *hyperreality*, virtual reality that *'rests on the deregulation of the very reality principle'*[248] is a result of God disappearance from the society. Instead of unveiling the objective reality after disappearance of God we rest in a quagmire of *Integral Reality*; we lost the imagination of real through conviction of living the real. That conviction is a foundation of our moral order, but nothing, human and technology including, is willing to obey the order or moral imperative,[249] they rebel – they create, organize, they assemble a *resistance*. No dreams, no desire, a mental deprivation of unachievable real by living the *Integral Real*. The reality is a whole dream, a designed dream, or a part of our imaginary, but working on the universal fulfilment of our legitimate moral (consumer) desire, which is understood as a final salvation.[250]

[244] Ibid., 50.
[245] Ibid., 53.
[246] Sallie Westwood, *Imagining Cities: Scripts, Signs, Memory*, 1997, 299, doi:10.4324/9780203397350.
[247] Jean Baudrillard (2005), *The Intelligence of Evil Or the Lucidity Pact,* New York: Berg.

[248] Jean Baudrillard (2005), pp. 17.

[249] Jean Baudrillard (2005), pp. 19.

[250] Jean Baudrillard (1998), *The Consumer Society: Myths and Structures*, *London: Sage Publications*.

Baudrillard see two antagonistic trends: First, the *Integral Reality* as *'the irreversible movement towards the totalization of the world'* and *The Dual Form* as *'the reversibility internal to the irreversible movement of the real.'*[251] While the *Integral Reality* is working towards the totalization, the absolute conquest of our minds by the virtual reality using the signs that form our interpretation of reality, that tell us the "truths" about presumptive cyber-attacks and the needed reaction on them on behalf of national security, the *Dual Form* represents the rebellion against it, the desire to understand, to oppose the grand narratives, the everydayness, the authorities we take as granted, to challenge the global violence caused by world system consisting of corrupted states. While the *Integral Reality* seeks the very idea of completion – how to make all software exploits gone using artificial intelligence that will do it on its own,[252] definitive accomplishment, the final reconciliation, a kind of an utopic vision in hands of technology itself, in order to the totalize power; *The Dual Form* does the opposite, it rather creates, understands and controls technology than introduces ideas such as artificial intelligence in the service of national defense; it tries to topple down the world system in its radical way – in a dawn of a global crypto anarchist revolution.

Post-modern perspective along with its fluidity does not give us a chance to understand the contemporary; everything flows too quickly, hence depicting utopic far future as we see in classical science fiction seems to be odd and pointless. Cyberpunk provides different feelings as it is depicting supposedly inevitable near future as we can see in classics such as Gibson's Neuromancer[253] that introduced cyberspace as a term or Philip K. Dicks writings preceding the movie Blade Runner where human blurs with androids and the moral imperative moves away from humankind (will be elaborated in detail below).[254] These writings leads into a state of consciousness where *no control is possible* in our near future as the *dystopic technological nightmare* depicted in cyberpunk subculture is inevitable state of society, state of consciousness, a techno-consciousness in

[251] Jean Baudrillard (2005), pp. 21.

[252] The Hacker News (2016), 'DARPA Challenges Hackers to Create Automated Hacking System — WIN $2 Million,' <http://thehackernews.com/2016/07/hacking-artificial-intelligence.html> (accessed 1 August 2016).

[253] William Gibson (1984), *Neuromancer*, New York: Ace Books.

[254] Philip K. Dick (1968), *Do Androids Dream of Electric Sheep?,* Garden City, NY: Doubleday.

a techno-environment, which is full of unbearable moral decisions. In that moment, no other way than a complete rebellion against the system is an acceptable and legitimate approach for people seeking liberty against the wish of control of the oppressor, because the ultimate control, as usual, is a totalized utopia and current technology in service of surveillance can easily provide the utopias we have read in cyberpunk classics, but of course in George Orwell's 1984[255] or Franz Kafka's Trial.[256]

Cyberpunk connects the human body with technology, alters the technology itself by humanity, and alters humanity by technology. Finally, it questions morality, legitimacy and the principles of liberal democratic governance. Cyberpunk unveils the undesirable future of Baudrillard's *Integral Reality* that irreversibly leads into totalization of the world by the ultimate reign of technology in hands of corporations augmented into a human body, into cyborgs supported or tacitly respected by corrupted governments. Crypto-anarchist movement then sees itself in the role of *The Dual Form,* in the visionary resistance promoting hope of liberation from totalized power oppression, they believe in technology under control, into its liberating power in hands of individual, in a decentralized world without authorities.

This is the contrast the following text will work with. The contrast between the utopias of authorities and the resistance. The utopia of nation states, of their policy makers or policy driven cyber experts who are convinced that all exploits in cyberspace can be patched, even using the most advanced artificial intelligence without critical imagination what implications we can face when the artificial intelligence starts to produce its own 0-days exploits. And the utopia of resistance that can respect authorities to some extent, but is not willing to respect total regulation in order to preserve security against presumptive insecurity; a regulation in its totalized form, a regulation we are witnessing in a growing tendency.

The Buadrillards' dystopic fictitious vision of the society development in the 70s is written in time when almost the whole world, especially the countries east to the Iron Curtain, were looking towards the United States, its capitalist achievements, Apollo

[255] George Orwell, *1984: A Novel* (New American Library, 1949).
[256] Franz Kafka, *The Trial* (Courier Corporation, 2012).

program, highway network and boom of modernization of any meaningful sector; consumer electronics, computers and internet included. Baudrillard's world was a corrupted, failed, immoral and unscrupulous in its objective of one global market run by amoral capitalist principles with corporations in reign: *"instantaneous cruelty, incomprehensible ferocity, fundamental immorality…it is a monstrous unprincipled undertaking, nothing more"*.[257] A world where democracy is just an excuse to spread influence on a global scale through legitimization of capitalist power in hands of massively and globally growing corporations. Moreover, the speed of the growth is running faster and faster causing changes in social sphere faster, much more than in any prior system.[258] The technology development is making major part of the society alienated. Nobody clearly understands its possible consequences, because technology as an augmentation of traditional life disturbs logical deductive processes. *Everything is possible* and these who have the power to let the technology work for them are causing deep uncertainty within governing elites that as a consequence produce fear. The uncertainty is also fueled by the fact of toppled borders between nation states; the traditional fuse of their security. Such development in last decades has given a birth to a new subculture. The cyberpunk.

[257] Baudrillard, *Simulations*, 28–9.

[258] Anthony Giddens, *Modernity and Self-Identity: Self and Society in the Late Modern Age* (Polity Press, 1991).

4. THE CYBERPUNK EMERGENCE AND THE GENESIS OF CYBER

"I've seen things you people wouldn't believe. Attack ships on fire off the shoulder of Orion. I watched C-beams glitter in the dark near the Tannhäuser Gate. All those moments will be lost in time, like tears...in...rain. Time to die."

— Roy Batty, NEXUS-6 N6MAA10816 (8/1/2016 – 8/10/2019), Blade Runner movie (1982) —

The ancient genesis of cyber as a governance, or a self-governance, a morally constitutive governance was discussed above. The first emergence in the forthcoming industrial age was probably a usage by a French mathematician and physicist André-Marie Ampère in the 19th Century just a year before he died. He used it in an essay *Essai sur la philosophie des sciences* in that context of self-governance as well.[259] Ampère used for a first time its version *cybernétique* in a clear relation between human interaction and machines. This meaning was directly related to its use in a development of *cybernetics* (first usage in English version) in the late 40s of 20th century; that time it was coined by Norbert Wiener, an American mathematician from Tufts College and Harvard University, in a work Cybernetics, or Control and Communication in the Animal and Machine.[260] Wiener along with various scientists from biologists, through engineers, computer scientists, neuroscientists to social scientists were experimenting with ideas of human body augmentation by technology.

Everything they were thinking about was meant as possible future development in technology, its augmentation to biological structure or what will be the social implications to the society. All of this was understood as a futuristic prediction, but scientifically driven. From here, the term *cybernetics*, with its "current" futuristic sheen. The most used of prefix *cyber-* was probably related to its link to organism, from there the term *cyborg* – a cybernetic organism. It is a very different meaning to a term *robot* introduced by Czech writer Karel Čapek in his masterpiece R.U.R. In contrast, cyborg is not only a mechanical machine, it is a combination of machine and organism. The term

[259] A M Ampère and C A Sainte-Beuve, *Essai Sur La Philosophie Des Sciences; Ou, Exposition Analytique D'une Classification Naturelle de Toutes Les Connaissances Humaines*, Essai Sur La Philosophie Des Sciences; Ou, Exposition Analytique D'une Classification Naturelle de Toutes Les Connaissances Humaines (Bachelier, 1838).

[260] N Wiener, *The Human Use of Human Beings: Cybernetics and Society* (Da Capo Press, Incorporated, 1988).

cyborg was coined by Manfred Clynes, a scientist, musician and inventor in an article from 1960 that argued for cyborgs in space exploration.[261] According to Manfred, it is not feasible to alter the environment for humans; they have to be altered by technology to survive instead. When it comes to cyborg, who steers who is not clear, whether the machine steers the living organism or the organism steers the machine. Are we losing governance over technology needed to mine asteroids if we go for cyborgs instead of pure mechanics? This debate about the source of steering is the principal foundation of dilemmas we can observe in subsequent cyberpunk subculture. Understanding of cyber quickly found its way to cultural expressions, literature and movies. Dr. Who (1966) was probably the first television show using cyborg as a part of the plot and Martin Cadin's novel Cyborg published in 1972 was about cyborg, clearly from the title. The novel Cyborg inspired the movie and TV show named The Million Dollar Man. They were far from dystopian future images; the plot was much more about the dilemma of an augmented man with *superhuman* abilities fulfilling a mission of a special agent he was not consent with at the beginning rather than about the dilemma of steering, or the source of consciousness. However, it is important to understand the archaeology of the term between late 40s and early 70s, before its merge with dystopian postmodernist philosophy (where Baudrillard should be used as an example as it would be hard to prove his direct influence) in the emergence of dystopian *cyberpunk*. For example, when Tyrell Corporation in the movie Blade Runner (1982) developed the latest model of its android for space utilization, they implemented emotions to make the androids more human, but also a retirement day to avoid troubles if the consciousness would worked out better than expected.

Cyberpunk is a subculture that depicts a dystopian world where corporations such as Tyrell reign the world, people augment their bodies with technologies creating *cyborgs* and *androids*. They are artificial intelligence that is hard to recognize from humans and entity that is hard to steer by humans in the end. Technology and humanity merge into one or into indistinct. Technology created by humans is getting emotions, an ability to distinct between good and bad, an ability to recognize moral behavior. The unbearable *Integral Reality* of our everyday life has grown into a dark present. Cyberpunk does not

[261] M. Clynes and N. Kline, "Cyborgs and Space," *Astronautics*, no. September (1960): 26–27, 74–75.

predict far utopian futures, such as science fiction icons Star Trek or Star Wars; it does depict the postmodernist dark present in the near future. Cyberpunk distinction from utopian intergalactic science fictions we know from Isaac Asimov or Arthur C. Clark is based on a bit of ambiguous clash inside it; a clash we observe in *The Dual Form* concept of Baudrillard's writing. It is clear where is good and where evil in Isaac Asimov novel I Robot. Cyberpunk could do this by the differentiating move that includes the very principal dilemma emanating from source of consciousness. In Blade Runner, who is right? The android banned from coming back on Earth or the Blade Runner who hunts them? And who should have the power to make the decision, state or corporation? Does state possess enough power to *steer* this morally dilemmatic situation? Who is right then, the authorities or the resistance? This question is not easy to answer; the example with intellectual property shows it precisely.

The real step into the interconnected *dystopic technological nightmare* was made by William Gibson with his novel *Neuromancer*.[262] However, we can debate about who was first. Gibson certainly used the term *cyberspace* for the first time. Nevertheless, he was certainly influenced by Ridley Scott's movie *Blade Runner,* which was released in 1982.[263] Moreover, he was shocked when he watched the first screening of Blade Runner. It was so close to his ideas that he researched deep into it to alter his forthcoming novel and delayed the publication for several months. But what kind of research could he conduct? Blade Runner is based on a novel written by Philip K. Dick named *Do Android Dream About Electric Sheep?* first published in 1968. Philip K. Dick preceded these two cyberpunk iconic masterpieces as he wrote a lot of other novels that can be barely ignored when dealing with cyberpunk subculture (e.g. Minority Report). All of this was a product of combining criticism of consumerism, uncritical usage of technology, risk of corporate power and inability of elected institutions to deal with it. Before I return to Neuromancer, which is directly related to the genesis of cyberspace, let me say some thoughts on these new cultural expressions.

[262] William Gibson, *Neuromancer* (New York: Ace Books, 1984).
[263] Herlander Elias, *Cyberpunk 2.0. Fiction and Contemporary*, 2009, 42.

Blade Runner is a movie that can be easily found in every science fiction movies list, usually at the top. The environment is based on *noir* movies from the 40s that were depicting the underground crime scene of the 30s, during the prohibition and Great Depression after the Black Friday in 1929. However, Blade Runner connects this atmosphere with new technologies and power of corporations into a rainy, foggy, dark atmosphere of a polluted city, in which no one has even power over him/herself – the world full of inability of self-governance. People are walking with virtual reality helmets in streets, stealing tech from police cars, who have offices in a dark and messy old buildings, while the Tyrell Corporation producing hard to recognize human-like androids has a monumental super modern headquarters above the city. People dream about real animals as every animal in human society is already a manufactured artificial life; the chaos between what is real and what is a replica of the real traversing the whole artwork. The movie contains so many specific moments and messages that it is still under research even 34 years after its release. The depicted dystopian future is important as it directly defines motives of people in present movements such as Anonymous fighting their battle for human emancipation. They are understood as an adversary to the ordered world while their motives are clearly moral rather than profit oriented. The final battle in Blade Runner is about the very existence of humanity (the last words of Roy Batty/NEXUS 6 in the quotation at the beginning of the chapter) as the android realizes that the last thing to do in life might have moral connotation rather than selfish one. Tyrell wanted to build androids "more human than humans", but in the end it is not clear whose behavior is more human if humans possess the moral consciousness. Once renegades – the androids – found their way back to Earth to prolong their lives, they faced the reality of their *retirement* implemented by their creator, Tyrell. Then one android, Roy Batty, saves the life of a policeman that hunted him to enjoy the last minute of his life. These clashes of realities, "a confusion of realities" is typical (Philip K. Dickean) to the dilemma where the good and humanity lies.[264] This very easily goes with the Baudrillard's term *Integral Reality* as we do not know where is the real real, but we are confident that we live the *real*; clearly depicted dilemma in another cyberpunk movie The Matrix. These dilemmas are critical for understand the ideology of several hacktivist movements and certainly

[264] Ibid., 58.

helps to understand the securitization process under *technological radical uncertainty*. The inability to grasp the real threat from cyberspace, to depict imagination that can help to shape a national security policy, but rather imagine the future in a hypersecuritization manner clearly shows how these possible images of near future insecurities are fluid and unstable.

The ambiguous battle is an important mode. There is no good, no evil. Nobody knows where the good intentions are and where the evil begins. The very principal moment of post-modern thought is the reality that flows away just after it emerges. Everybody participates in the dystopian world as we participate in consumerist society. There is no way out and disorientation is everywhere. In modernity, we can observe a linear teleological development and accumulation. In post-modernity, we observe how this development and accumulation rotate around without achievable reconciliation. Baudrillard talks about phases of culture as a reaction to a symbolic exchange and a simulation.[265] Symbolic exchange, which is detached from the real. Simulations, as *sham objects*, are then the depiction of the (un)real world around us causing confusion with real things despite the superabundance of signs attached to it.[266] This causes the same dilemmas about humanity as I talked about above. Frankenstein, as a cultural reaction to this confusion answers the dilemmas of industrial age. Neuromancer and Blade Runner are a reaction to post-industrial age and forthcoming information age where our minds might one day be interlinked through cyberspace. Matrix is a popular culture reaction to the information age with the same Baudrillard's links about inconsistence of the presumptive real, the fluidity of the real from one to another.

The link to current ultra-libertarian movement driven by crypto-anarchist technology utopia lies in their vision of emancipation that is directly based on opposition to this dystopic threat under construction by authority they see in nation states and corporations and they have serious evidence from whistleblowers such as Snowden to draw this plot in a serious way. Nation states have power that they draw lines along the national security policy and as we know from history, nation states do not tend to reform

[265] Baudrillard, *The Consumer Society: Myths and Structures*.
[266] Ibid., 12.

themselves, but need to be reformed by rebellion; either democratically elected or toppled by revolutions. The paradoxical part in this plot is the fact that both Internet and TOR, which give such cyber power to decentralized networks of hackers, were developed by US military, the biggest adversary to these people whose prime objective is not to crack some computer systems for money, but to crack the whole state-corporate world system that so depends on cyberspace today. These almost hysterical antagonist worlds depend on each other and are mutually constituted. The imaginations about the adversary within the opposite worlds are driven by the antagonist relations, by the imaginations of possible when the technology provides one with an argument that everything is possible. Than the dystopia is an understandable outcome.

The above depicted dystopian fiction of cyberpunk is a source of inspiration to the geek communities, to those who develop (crypto-anarchists) or apply (ultra-libertarians) technology to change the world order. However, there is a conflict within resistance as well: while the crypto-anarchists would give the knowledge for free completely, the libertarian anarcho-capitalists would make money on everything, but are not consistent when it comes to knowledge. Even within the community that resist the authorities are fundamental antagonisms. It is needed to understand the cultural basis of these motivations as the imaginaries the fictitious stories inspire people to cooperate. As Aradau and Munster[267] influentially argued, the knowledge of possible catastrophes is important in order to react in a normalized manner. If we fall into dystopian visions drawing near future insecurities in clearly fictitious way, we will find ourselves deeply swallowed by the dystopian visions. Knowledge about the subculture helps to predict actions of respective actors, but they react in resistance. More regulation of cyberspace means more powerful resistance. Too much regulation seeking the utopian totalized solution will lead to uncontrollable resistance and will lower the credibility of liberal democratic societies as we are finally witnessing in the end of the writing of this dissertation in the real time. Ideas like the one of DARPA with artificial intelligence patching exploits as self-learning organism is not a dystopian vision, it is a consequence

[267] Aradau and Munster, *Politics of Catastrophe*.

of these dystopian imaginations, it is real. It does not solve the problem; it constructs it in a much more tremendous and absolutely unpredictable shape.

5. CYBERSPACE GENESIS

"Cyberspace. 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 banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding..."

— William Gibson, Neuromancer (1984) —

The first definitions from national security strategies tended to understand cyberspace merely in a technical way, as interconnected devices that communicate. The socially constructed environment was almost or completely omitted. It took decades before national strategist included the component of social interaction and still the definitions seem to avoid addressing the hard-to-grasp social environment. However, we might witness a change in the forthcoming years due to the propaganda activity by Russia, which is using social networks and other services where the interaction of people take place to put through its foreign policy interests by weaponization of information, [268] its cognition while avoiding any attacks on physical devices (in this particular strategy).

I would like to firstly deconstruct the above shown quotation, in which the first ever use of the term cyberspace appeared.[269] The newness in the term in relation to ongoing cyberpunk subculture expressions was the addition of its interconnectedness. The emergence of internet in the 60s evolved as a national defense project,[270] but its real social consequences became very quickly self-evident; especially in the 80s when the internet was already very actively used in academia. The possibility that everybody and everything can be connected in one interconnected world was certainly utopian, but now an achievable vision; however, with a different consequences that we expected. Gibson in Neuromancer depicted this world of infinite complexity, a consensual hallucination, a term in which he probably means the ability of all the billions of operators to project their awareness into one cyberspace. Certainly, as they can buy ROMs (read-only memory)

[268] Peter Pomerantsev and Michael Weiss, "The Menace of Unreality : How the Kremlin Weaponizes Information , Culture and Money" (New York, 2014).

[269] Neuromancer is usually mentioned as the first literature piece showing a word cyberspace. In fact, Gibson coined the term earlier in his very short science fiction Burning Chrome published in the July issue of magazine Omni, which he read for an audience of four people including Bruce Sperling in 1981. Later it was nominated for a Nebula Award in 1983. William Gibson, "Burning Chrome," *Omni* (Omni, July 1982), http://www.voidspace.org.uk/cyberpunk/burning_chrome.shtml#burning.

[270] J. Ryan, *A History of the Internet and the Digital Future* (London: Reaktion Books, 2010).

with consciousness, but at the same time their biological neurological system can be destroyed by a drug called myotoxin causing inability to connect to cyberspace. While united, the light sparks all the minds into constellations of data. Data are created, used, exploited, altered, distributed or consumed by operators – the indistinct actor between living organism and androids – cyborgs, if we synthesize the ideas of the whole subculture. However, all of this is influenced by power of corporations. Nobody knows where the power of these super-actors ends and whether or not one operator can change everything (e.g. the role of Neo from movie Matrix) and become *superhuman*. These constellations can be understood as current clouds, constellations of data that all be found in the urban jungle. Then all the computers are grown through humans in human systems that crossover all the nations in a borderless world. Gibson's definition of cyberspace, albeit a bit visionary, is still one of the best we have. In contrary to other spaces (or domains such as land, air, sea, space), cyberspace is constructed by consciousness of its operators; it is socially constructed.

Timothy Leary said that Gibson "*has produced nothing less than the underlying myth, the core legend, of the next stage of human evolution. He is performing the philosophic function that Dante did for feudalism and that writers like Mann, Tolstoy [and] Melville…did for the industrial age."*[271] Gibson created a new battlefield on an information basis. He shows how can we attack back using counter-information, and shows us a new man who can stand up having the faculty to distinguish between information and noise; to be oriented in a black market of cyberspace (observe the link with a current term *Dark Net*). On the other hand, the protagonist in the story is artificial intelligence that shows the hard-to-distinct reality and humanity from unreal and artificial life form. All of these infinities are covered by multinational corporations that hangs as an umbrella over totalized uncontrollable infinite ocean of information. This infinite complexity also contains a vast amount of enemies that seek for Deleuzen and Guatarris

[271] Cited in Kellner, *Media Culture: Cultural Studies, Identity and Politics between the Modern and the Postmodern*, 298.

reterritorialization[272] of the real within the vast labyrinth of *virtuality, hyperreality* or *integral reality*.

In contrast, national security strategies or more precisely national cyber security strategies tend to provide us only with simple definitions that have been developed by analysts who wanted to point out on a growing security problem in cyberspace. First of all, they tend to omit the distinction between technical infrastructure and the abstract social construct above it. They usually vary around different physical/technical perspectives or we can say they tend to compete who chooses the better and more important devices connected to an ultimate global network to show the policy makers that even they depend on things related to the Internet. Let me show some of these oversimplifying definitions: *"The interdependent network of information technology infrastructures, and includes the Internet, telecommunication networks, computer systems, and embedded processors and controllers in critical industries."*[273] Another one starts with the term *nervous system* that has links to the above drawn dystopian world, but the whole document does not work with that perspective very brightly: *"Nervous system – the control system of the country (…) composed of hundreds of thousands of interconnected computers, servers, routers, switches and fiber optic cables that allow our critical infrastructure to work."*[274] Using the term *nervous* does not have any other reason in the mentioned strategy than to depict how complex it is. However, one may argue that here we come with the first seed of imagination as using the term *nervous* might have other reasons; maybe a system, on which we all depend and cannot live without? It increases seriousness of the network by choosing this particular term, while the term itself says nothing to its functioning. Definition that constitute emotions rather than to provide some explanatory outcome. Other definitions add a layer of information: *"Digital environment enabling the origin, processing and exchange of information, made up of information systems and the services and networks of electronic communication."*[275]

[272] Gilles Deleuze and Felix Guattari, *Anti-Edipus. Capitalism and Schizophrenia*, *SubStance* (Minneapolis: University of Minnesota Press, 1983), doi:10.2307/3684887.

[273] White House, "National Presidential Directive 54" (Washington D.C.: White House, 2008), http://fas.org/irp/offdocs/nspd/nspd-54.pdf.

[274] TheWhiteHouse, "The National Strategy to Secure Cyberspace." (Washington, DC., 2003).

[275] Petr Jirásek, Luděk Novák, and Josef Požár, *Cyber Security Glossary*, 3rd ed. (Praha: AFCEA and NCKB, 2015), http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf.

However, it took some time since these definitions have included its change *by the use of it*. The following is to my knowledge and based on my opinion, and certainly thanks to the research by the author that lies behind it, the best available definition for policy makers:

> *"A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."*[276]

Right now we have three layers, the technical infrastructure that is interconnected through networks, the information stored somewhere within and the *fluid character* caused *by the use of it*, but we still do not have the abstract layer. The Encyclopædia Britannica defines the term *cyberspace* thoroughly, but in the second sentence it mentions the distinction between internet and cyberspace; respectively the distinction between the infrastructure and the generation of the *place* produced by the interconnected network that is consisting of information[277] can be understood as our active creation and reflection of that place, an abstract place as it does not have physical proportions. The distinction between outer-space and cyber-space can be made on distinction between exploration and construction,[278] respectively *exploration of the real* and *construction of the virtual*. Cyberspace in cyberpunk subculture, but also later during the dawn of computer games and chatrooms was understood as a *virtual place* where interactions between people occurred. Without these interactions no cyberspace would exist.

Today, we can add also machines as the internet is full of information collected by automated systems (systems that do not merely distribute, but generate information), e.g. publicly available satellite imagery; maybe traffic information would be a better example as we make immediate decisions based on such information distributed using automated systems. Google traffic collects anonymous data from cell phones, excluding

[276] Daniel Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, vol. 35 (Potomac Books, 2013), 24–42.

[277] Jennifer Bussel, "Cyberspace," *The Encyclopædia Britannica*, 2016, http://www.britannica.com/topic/cyberspace.

[278] N. Choucri, *Cyberpolitics in International Relations* (Cambridge, Massachusetts and London, England: MIT Press, 2012), 51.

anomalies such as frequent stops of postal or any other delivery vans and produces colors on a map.[279] These colors representing levels of traffic jams are used to calculate the shorter path. The driver then follows the car GPS navigation system. This is just a small example in which our pragmatic reflection of data automatically generated through cyberspace directly influences our decisions. However, artificial intelligence marches into our lives as Google introduces its ChatBot. It will soon help us solve technical problems with our computers by answering even clarifying questions in language quality and insight that people might not even register they are talking to a bot.[280]

Martin Libicki in his book from 2007[281] divided cyberspace into four layers, and he added the pragmatic one:

- physical, consists of hardware, processors, storage, switches, routers, handsets, and conduits both wired and wireless (INFRASTRUCTURE),
- syntactic – communication conventions and protocols (CONNECTIVITY),
- semantic – stored data and information (CONTENT),
- pragmatic – users' decision making (COGNITION).

Despite its rigid approach in definite and bordered layers that helps understanding different characteristics of cyberspace, the addition of pragmatic layer made its step towards understanding of cyberspace as a space depicted in the cyberpunk subculture. Without pragmatic layer, there would not be perspective of social construction of cyberspace in national security policy.

Right now, we can add the postmodern perspective to the whole conceptualization. Postmodernism as a theoretical approach and as a culture emanates also from the *uncertainty of technology innovation* and its societal implications. The technology on the one hand tries to not only help us to understand the dynamics, but to answer the uncertainty during a constitutive process. I mean a process in which the

[279] NCTA, "How Google Tracks Traffic," *National Cable & Telecommunications Association*, 2014, https://www.ncta.com/platform/broadband-internet/how-google-tracks-traffic/.

[280] Cade Metz, "Google Made a Chatbot That Debates the Meaning of Life," *Wired*, June 26, 2015, http://www.wired.com/2015/06/google-made-chatbot-debates-meaning-life/.

[281] Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge University Press, 2007), 236–237.

technology plays both roles, of the agent and of the structure. Giddens, as a postmodern sociologist, introduced this idea in which the agent and the structure are mutually constitutive,[282] where practices translate into habits during a performative dance between the both.

I used this idea recently to explain the sociological constitutive notion in cyberspace conceptualization,[283] in which I tried to put the principal theoretical basis of cyberspace existence back to the postmodern perspective; to the age in which the logic of internal cyberspace dynamics emerged as Gibson's hallucination of millions of operators connected to the network. Without the connection and consequent shaping by ideas, cyberspace would not be possible. The nature of its security is not limited to working routers and servers. It is also dependent on the way, how we reflect its implications. The principal argument during the time of writing was to point on a power switch we can witness in cyberspace. Every single national defense strategy in cyberspace tends to translate conventional power to cyber power pointing on accessibility of every system in critical infrastructure[284] while omitting the very fact of its postmodern inaccessibility as it changes fluidly and as such flowing between fingers as the target services, software settings and hardware configuration change, but also as people's habits change in space and time. What we are witnessing today is a real performation of a cyberpunk imagination, in which the high-tech environment and cyberpunk culture are both mapping and illuminating the apparent reality.[285]

Gibson's *hallucinations*, Britannica's cyberspace *production* on the links of internet generating abstract virtual world, Kuehl's perspective of its shaping *by its use of it* and mine *sociological approach* to its conceptualization using Giddens theory are all constitutive stepping stones to cyberspace conceptualization; to better understand the space we all have been creating and will constantly change in near or far future. Cyberspace helps to produce new realities and these realities certainly empowers new

[282] Giddens, *The Constitution of Society*, 17.

[283] Schmidt, "A Sociological Approach to Cyberspace Conceptualization and Implications for International Security."

[284] Franklin D. Kramer, "Cyberpower and National Security," *American Foreign Policy Interests* 35 (January 2013): 45–58, doi:10.1080/10803920.2013.757960.

[285] Kellner, *Media Culture: Cultural Studies, Identity and Politics between the Modern and the Postmodern*, 303.

people who like to exploit their opportunity based on their knowledge; and these motives are not too much taken seriously.

However, if we have to take into consideration all the characteristics of cyberspace for purposes of national security strategies, almost all the definitions I cited above seriously lack a lot of later discussed specifics which are critical for any meaningful approach by policy makers. One has to admit that even without doing the etymological research of a term *cyberspace*, we read news about threats that include the cognitive layer every single day. The Russian propaganda for example, which is currently very tangible topic and might have serious consequences in the long term[286] despite some allegations that the bigger problems are produced by "useful idiots" rather than by the direct propaganda itself.[287] However, the ability of people to organize themselves after politically important events to protest has been shown for example in Philippines.[288] However, the sociological approach is valuable even in hard security policy as it shows that attacks on hard targets such as power plant are not currently part of the adversaries. When it comes to state hostilities, the influence of Russia in European politics and currently even to the presidential campaign in USA has become a norm. When it comes to the resistance, the ability of states to govern technology development is far from possible. In the end, we have strong political players on the global scale in USA and Russia who try to destabilize their political systems and then decentralized communities that tend to isolate themselves from political turmoil in geeks, crypto-anarchists or libertarians taking their opportunity and at the same time rising unnumbered amount of artificial intelligence self-learning system. The reality looks like a dystopian post-modern chaos where nobody knows who is on what side or whether there are a side to take.

Talking about security in sense of connectivity between devices would be really shortsighted. The following list introduces some of the most important characteristics

[286] Salome Samadashvili, "Muzzling the Bear Muzzling the Bear. Strategic Defence for Russia's Undeclared Information War on Europe" (Brussels, 2015).
[287] Maria Snegovaya, "Putin's Information Warfare in Ukraine," no. September (2015): 28.
[288] Clay Shirky, "The Political Power of Social Media," *Foreign Affairs* 9, no. 1 (2010): 1–7.

related to current shape of cyberspace and how each characteristic contribute to the post-modern chaos:[289]

- *Temporality* – if one is interested in an attack of an enemy, there is no traditional discussion how much it will take since the launch of the operation. Everything is going on in real time. The preparation phase is critically important, while the operation itself might be extremely short. Even just a one moment. Time disappeared.
- *Physicality* – physical accessibility loses its sense when it comes to politics of cyberspace. The constraints of physical distance, the geography itself and the situation of the infrastructure changes significantly. The ability to influence political processes in other countries directly, change the strategy every day from far distances, use a cyber-attack against power grid, all of this is completely different since the cyberspace have been developed. When the first air forces were deployed, the strategy significantly changed, because air could go over the front lines, attack supplies and return safely back. Cyberspace change this completely, we do not need to be physically present to cause serious harm and even completely destabilize other countries.
- *Permeation* – the fact that people do not behave according to habits in their "real" social life, that actors, states including, do not obey rules and laws. This characteristic is important in understanding how any kind of regime cannot be applied to people in their operation of technologies connected to the Internet.[290] As it is completely (almost) unable to enforce a regime in cyberspace, it is also completely unable to govern the technology that deepens the complexity of the technologies. Developing norms of behavior, rules of the road for new actors in space that change so quickly become unachievable objective. That of course seriously harm even the notion of

[289] The meaning extension in the commentary is author's alteration, but the list and the basis of the characteristics are taken from Choucri, *Cyberpolitics in International Relations*, 4.

[290] Rex Hughes, "A Treaty for Cyberspace," *International Affairs* 86 (2010): 523–41, doi:10.1111/j.1468-2346.2010.00894.x.

moral behavior and the polarity of good and evil outcomes of our technology usage, development and exploitation.

- *Fluidity* – the very post-modern characteristic. The one that depicts the constant change of the environment, services, habits and routines.[291] Not only the technical infrastructure, but also available services and the long chain of consequences are directly or indirectly connected to the real physical domain of our lives. There are real businesses that experienced their failure due to emergence of even illegal services online. The debate over intellectual property would be a clear example. [292]
- *Participation* – as will be discussed in the rest of this chapter, cyberspace seriously changed the way how people can participate on a public life. Activism, with – of course – its supposedly negative connotation as a *hacktivism*, fuels power of non-governmental institutions and any other non-state actors and gives an unprecedented possibility to people to show united opinion quickly and also massively. This characteristic seriously shaken with whole states during the Arab Spring.[293] However, participation characteristic is important in any kind of non-physical organization. People are not able only to topple down regimes, they are also easily achievable by those who might have interest in toppling down the regime as we can see in current Russian behavior in socially constructing unreal *signs* in the audience in Europe and elsewhere.[294]
- *Attribution* – one of the most important characteristic in interstate relations. The fact that the origin of an attack is hard to attribute to particular actor, and the fact that the actor is not willing to change it as the state can easily exploit it to its advantage, creates antagonistic moment I called *dual-interest of states*.[295] On the one hand, they tend to discuss how

[291] Schmidt, "A Sociological Approach to Cyberspace Conceptualization and Implications for International Security."

[292] David R Koepsell, *The Ontology of Cyberspace: Philosophy, Law, and the Future of Intellectual Property* (Open Court Publishing, 2003).

[293] Volker Perthes, "Europe and the Arab Spring," *Survival* 53, no. 6 (November 15, 2011): 73–84, doi:10.1080/00396338.2011.636273.

[294] Pomerantsev and Weiss, "The Menace of Unreality : How the Kremlin Weaponizes Information , Culture and Money."

[295] Schmidt, "Super-Empowering of Non-State Actors in Cyberspace."

to divide privacy and anonymity to beat current ultimate anonymity and keep people private online. On the other hand, it is in their very interest to be hidden behind the attribution problem to conduct operations in cyberspace and circumvent international law; especially in operations that by the definition do not violate international law, but seriously undermine national security.[296]

- *Accountability* – the characteristic related to the attribution problem. When the attribution is problematic, the accountability is impossible. Some scholars propose more structured responsibility to states if they fail to avoid cyber-attacks emanating from their territory,[297] but the dual-interest keep these ideas grounded.

The debate could go deeper, but let me start developing the point of the whole dissertation here. The definitions we saw above, which were related to the national administration of USA, must had influence on policy making. Researchers in critical studies already pointed out the enormous effect of security framing of the so called critical infrastructure threats based on pure imagination.[298] These definitions share the uncertainty of the communication technology. The fact that military has to defend their networks to be operable, the fact that one must be able to make a call over laid wires, the fact that physical network architecture matters in cyber security raises attention to the physical layer. All the definitions and perceptions visible in first national cyber security strategies shares this simplification. For example, the Dutch national cyber security strategy does not talk about cyberspace, but about *digital domain* to make it more chaotic, however, the definition still contains that simplification approach: "*The digital domain is the conglomerate of ICT tools and services and comprises all entities that can be or are digitally linked. The domain comprises both permanent, temporary or local connections, as*

[296] Schmidt, "Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War."
[297] Healey, "The Spectrum of National Responsibility for Cybera."
[298] Cavelty, *Cyber-Security and Threat Politics: US Efforts to*; Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse."

well as information, such as data and programme codes, located in this domain where geographical limitations do not apply."[299]

So we *the nervous network*, *the digital domain, the global and dynamic domain, the warring domain, the electromagnetic spectrum, the realm of electronic communication, the notional environment* and so on. One may ask why the need of cyberpunk debate when all of this is about cyber security as a national security agenda. The answer is clear:

First, the way how we understand cyberspace is the way how we influence the policy that embrace it.

Second, the characteristics of implosion (combination of human body and technological prostheses, neuro-chemicals and drugs influencing mind and altering personalities, where minds are programmable…) in a one's motivation to reach *general liberty* by being an ultimate sovereign individual Gibson envisioned in *Neuromancer*. The same is in interest of current techno-geek communities despite the less fictional approach. It is important to understand ideology of hacker communities in order to understand motives behind their actions.

Third, the will and the ability to post-structurally grasp and construct a fluid society, having the presumable contingencies under control, stimulating the constant move and the ability to keep the others out from understanding the consequences of merging human body and the growing world of electronics is a visible advantage of techno-geeks over observers of cyberspace as cables.

Fourth, hackers depicted as *"password pirates and electronic burglars"* who possess *"a certain techno-scientific power"*[300] are nightmare for policy makers, because they possess power in real. On one hand, they adore their capabilities and use them as a powerful tool when enabling cyberspace for national security interests during some

[299] Jonas Matthias Eiriksson and José Manuel Retsloff, "Librarians in the ' Information Age ': Promoter of Change or Provider of Stability? Deconstructing Reality" (Royal School of Library and Information Science, 2006), http://www.bibliotekskonsulenterne.dk/filer/Librarians in the information age Promoter of change or Provider of stability.pdf.

[300] Elias, *Cyberpunk 2.0. Fiction and Contemporary*, 28.

special operations such as Stuxnet.[301] On the other hand, they simply cannot withstand the fact of their incapability to face them despite the fact that the incapability emanates from the complexity rather than from lack of knowledge as the complete understanding is unachievable. Hence the defensive countermeasure is the drawing of dystopian doom scenarios[302] in the real world producing securitization terms such as critical infrastructure. Different approach is to propose them a job in state administration.[303] However, that move – in the contrary to their will – confute them of that incapability to understand the cyberspace possibilities. That in circle again empowers the techno-geek community. An interesting example would be the discourse behind the rise of bitcoin. The crypto currency, or digital currency, has its own important general advantages especially in the technology of block chain on which it builds, but also underline the achievability of the crypto-anarchist objectives as will be discussed later. The discourse of people supporting and promoting usage of block chain technology is usually oriented to mock politicians even in situations, when they are willing recognize it as a genius invention.[304] The resistance understands the will to support it as false and as another cheating of governments on the rising liberty of people.

Fifth, we should understand this moment in motion rather than as a solid moment in time space. Cyberpunk is not a future prediction for policy makers, it is an inspiration for techno-geeks. It empowers their motivations and action. In Neuromancer, operators are making money by selling information, information is the currency in that world. These, who steel from banks nowadays, have computer, capability and information, nothing else. This power gives them a radical vision of an ultimate liberal world without nation states.

[301] Liam O Murchu Nicolas Falliere and and Eric Chien, "W32.Stuxnet Dossier" (Cupertino, 2012), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[302] Lawson, "BEYOND CYBER-DOOM: Cyberattack Scenarios and the Evidence of History."

[303] Brian B Kelly, "Investigating in a Centralized Cybersecurity Infrastructure: Why 'Hacktivism' can and Should Influence Cybersecurity Reform," *Boston University Law Review* 92, no. 5 (2012): 1663–1711.

[304] Michael del Castillo, "European Parliament Member: Everyone Should 'Get Some Bitcoins,'" *Coindesk*, April 22, 2016, http://www.coindesk.com/european-parliament-member-blockchain-get-some-bitcoins/.

6. TECHNO-GEEKS AND THE ORIGINS OF CRYPTO ANARCHIST MOVEMENT

"Nobody can give you freedom. Nobody can give you equality or justice. If you are a man, you take it."

— Malcom X, The Anonymous Hacktivist Group —

Baudrillard's simulation represents the uncertainty in technology development; the uncertainty producing realities out of the *presumable real*, in which those who provides knowledge suggest to oscillate between promoting study of changes and providing stability;[305] in the quagmire of post-modern instability, contingency and fluidity. We can observe the distinction between that *presumable real* and the *individual real*, the construction of subcultural world, which is detached from the outside world and untouchable by people untouched by technology or without a clue how all the newly generating techno-social environment works. These "outside" people that care about the *presumable real* are making decisions over a social environment they can barely control. It is a courageous claim; however, never ending argument, simplified into an expression that all the *"threats emanating from cyberspace"*[306] are a problem, proves the inability to distinguish appropriately where the power comes from and how these threats significantly vary in their internal potential to disrupt societies or destroy critical infrastructure. Cyberspace is a social construction and the plethora of threats it can bring up is as wide as all the threats we can even imagine in a physical space.

The perspective of critical infrastructure protection as a render of national security obligations by state will be analyzed in the third chapter of this part. However, how people who see only the physical cable from power plant can secure the cyberspace from geeks as non-state actors or geeks employed by other states remains clearly

[305] Eiriksson and Retsloff, "Librarians in the ' Information Age ': Promoter of Change or Provider of Stability? Deconstructing Reality."

[306] Nigel Inkster, "China in Cyberspace," *Survival* 52, no. 4 (November 15, 2010): 55–66, doi:10.1080/00396338.2010.506820; Nils Melzer, "Cyberwarfare and International Law," 2011, http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf; C. Czosseck and K. Geers, *The Virtual Battlefield: Perspectives on Cyber Warfare* (Ios Press, 2009); Cavelty, Mauer, and Krishna-Hensel, *Power and Security in the Information Age: Investi*; Nikola Schmidt, "Critical Comments on Current Research Agenda in Cyber Security," *Defense and Strategy* 14, no. 1 (2014): 29–38, doi:10.3849/1802-7199.14.2014.01.029-038; TheWhiteHouse, "International Strategy for Cyberspace," 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; Keneth Geers, *Strategic Cyber Security* (Tallinn: NATO CCD COE Publication, 2011); Alexander Melnitzky, "Defending America Against Chinese Cyber Espionage Through The Use Of Active Defenses," *Cardozo Journal of International & Comparative Law* 20 (2012): 537–70.

questionable. The problem of socially constructed cyberspace is not a geeky construct. Nice evidence of relation to serious national security agenda would be the Operation Orchard conducted by Israel into Syrian airspace with a result of a bombing of purported nuclear reactor.[307] It is used as one of the examples of so called cyber war; however, the point is that Israel altered the visible data on the way to monitors. The operators in Syria then could not make a decision as they did not see anything. Simple and extremely powerful ability. The one who has this ability, possess an enormous power.

The ability changes as the environment changes, who controls the environment, obtains specific ability related to that respective environment and as there is no single biggest authority or ultimate actor in cyberspace, because each single operator socially constructs it, these operators will have power only over these parts they have constructed. When we were talking about "a target in a constant motion" causing ontological insecurity without an ability to create a sociological frame of current fluid society,[308] this clearly applies to cyberspace as a socially constructed environment that changes in the same unpredictable way as a wind shaping the surface image over a lawn. Additionally, there is no more or less power, there is only a critical knowledge related to particular implications that materialize in momentous power. One may possess more detailed knowledge implying more power, but this power will be still a very specific one.

Geek, the one who possess power that the others even cannot imagine, not necessarily in its scale, but in its technological specificity. That immeasurability of skills is what constitutes the technological radical uncertainty, where plausible knowns and normalized reactions are unreachable as skills of geeks are immeasurable. The definition from an urban dictionary perfectly catch the meaning of a geek: *'someone with ridiculous skills on a computer or other electronical device and scares us mere earthlings. They have a habit of breaking these after stretching them beyond their ability for normal usage. They also sometimes know more about a product than the producer.'*[309] The actual application

[307] Lior Tabansky and Isaac Ben Israel, "Striking with Bits? The IDF and Cyber-Warfare," in *Cybersecurity in Israel*, SpringerBriefs in Cybersecurity (Cham: Springer International Publishing, 2015), doi:10.1007/978-3-319-18986-4.

[308] Westwood, *Imagining Cities: Scripts, Signs, Memory*.

[309] Urban Dictionary (2010), 'Tech Geek,' <http://www.urbandictionary.com/define.php?term=tech+geek> (accessed 20 March 2016).

of the definition into a contextual meaning is described in the cited dictionary as follows: '*so I just took out the hard drive, cleaned the terminals and de-floobied the remainder of the computer so I could download this software which enabled me to detonate a bomb on the other side of the world which is specifically programmed to kill everyone except me.'* One may argue that the meaning is overemphasized, it is of course, but the core meaning of ungraspable or unimaginable knowledge to do such things is what drives national security imaginations to a point, in which they talk about an infinite fog of threats emanating from cyberspace. The clash between a geek having specific knowledge and a five-star general having a nuclear button, but no power to stop a geek, is the core of the fear that drives national cyber security imaginations into the doom scenarios.

Crypto-anarchy movement is emerged from this capability based on opportunities of a globalized cyberspace. We can date the origins of the movement to the year of 1988 in which *The Crypto Anarchist Manifesto* was written by Timothy C. May and publicly read at the Crypto '88 conference; later it was used as a founding paper for a crypto anarchist movement in 1992.[310] Consider the dates, World Wide Web emerged in 1989 in its very very prenatal shape; the first web browser was written by the author of HTML language Tim Berners-Lee, an employee of CERN in Switzerland, in 1990. The manifesto looks forward to the future and declares how the future of cyberspace should look like. Let me cite the manifesto completely (emphasis are made by me for further argumentation):

> "A specter is haunting the modern world, the specter of crypto anarchy. Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a *totally anonymous manner*. Two persons may exchange messages, conduct business, and negotiate electronic contracts *without ever knowing the True Name, or legal identity*, of the other. Interactions over networks will be *untraceable*, via extensive rerouting of *encrypted packets* and tamper-proof boxes which implement cryptographic protocols with *nearly perfect assurance against any tampering*. *Reputations will be of central importance*, far more important in dealings than even the credit ratings of today. These developments will alter completely the *nature of*

[310] Timothy C. May, "The Crypto Anarchist Manifesto," in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, ed. Peter Ludlow (Cambridge, Massachusetts and London, England: MIT Press, 2001), 61–63.

government regulation, *the ability to tax* and *control economic interactions*, the ability to *keep information secret*, and will even *alter the nature of trust and reputation*. The technology for this *revolution*—and it surely will be both a social and economic revolution—has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences *monitored closely by the National Security Agency*. But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable. And the next ten years will bring enough additional speed to make the ideas *economically feasible* and *essentially unstoppable*. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers, and encryption chips now under development will be some of the enabling technologies. *The State* will of course *try to slow or halt* the spread of this technology, *citing national security concerns*, use of the technology by drug dealers and tax evaders, and *fears of societal disintegration*. Any of these concerns will be valid; *crypto anarchy will allow national secrets to be trade freely* and *will allow illicit and stolen materials to be traded*. An *anonymous computerized market* will even make possible abhorrent markets for *assassinations and extortion*. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy. Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will *cryptologic methods fundamentally alter the nature of corporations* and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus *altering forever the concepts of land and property rights* in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which *dismantle the barbed wire around intellectual property*. Arise, you have nothing to lose but your barbed wire fences!"

The depicted future in 1988 has materialized in today reality in a very similar shape as predicted. The *true name* or *legal identity* today is a luxury in any other social network than Facebook and Facebook does not provide us with certainty about the names people around. Russian trolls would serve as an example to that no-rule. The *non-traceability* is in national security discourse described as the *attribution problem*. The fact that people wanted to be untraceable made untraceable states as well and finally founded one of the biggest problem in cyber security. Attribution problem produces dilemmas in all meaningful policy related debates. No attack can be fully attributed to a particular state even when some "proof" based on "sophistication as a criterion"[311] is available; the complexity of forensics makes it a near impossibility. This fact causes serious troubles to the international law application, which has been thoroughly studied,[312] but is shortsighted against threats of slow *societal disintegration* that states finally have to face.[313]

Traceability is directly related to currently used communication technologies such as the IPv4 protocol that has been used since 1972, but also to *encryption*, which is a very heated debate today as it has been last decades. The most recent moment, in which the corporation Apple denied the request of FBI in the United States to unlock a mobile phone of a killed terrorist in California, might serve as a clear example.[314] Apple argued that they simply cannot assist FBI in this possible leading case as they do not have only American clients and that cracking the phone would show that the security of Apple products is only a marketing whiff. Additionally, decrypting phone does not mean decrypting all the possible encrypted instant messaging that might lay inside the phone, so the FBI's request does not follow their needs. Other argument is that assisting FBI could mean a need to assist any other governments in the future, including authoritarian governments. Finally,

311 Clement Guitton and Elaine Korzak, "The Sophistication Criterion for Attribution," *The RUSI Journal* 158 (August 2013): 62–68, doi:10.1080/03071847.2013.826509.

312 CCDCOE, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, ed. Michael N. Schmitt (New York: Cambridge University Press, 2013); Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harv. Int'l L.J. Online* 54 (2012), http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/.

313 Schmidt, "Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War"; Steve Ranger, "The New Art of War: How Trolls, Hackers and Spies Are Rewriting the Rules of Conflict," *Techrepublic.com*, 2016, http://www.techrepublic.com/article/the-new-art-of-war-how-trolls-hackers-and-spies-are-rewriting-the-rules-of-conflict/.

314 The~Economist, "Taking a Bite at the Apple," 2016, http://www.economist.com/news/science-and-technology/21693564-fbis-legal-battle-maker-iphones-escalation.

FBI made its own way into the phone and the possibility of a third party involvement was not denied.[315] The latest news show that FBI was not probably able to break it without an intervention of a third party. The debate is not limited to one case with Apple. The threat of global terrorism usually rises a question whether the anonymity should equal privacy and whether the ultimate anonymity is defensible in the long run.[316] The current situation in instant messaging for mobile phones already gives *nearly perfect assurance against tampering*. The terrorists of late 2015 Paris attacks used currently the probably nearly perfectly secure instant messenger Telegram,[317] which is understood as nearly unbreakable system.[318] Breaking the iPhone would certainly not solve all the obstacles of encryption in catching terrorists.

All of these services have become *economically feasible*, Telegram is for free and such services are literally *essentially unstoppable.* No authority has power to enforce drop of the encryption technologies and when the technologies are cleverly developed there is no chance to break them. The accessibility to such technology today is not limited and there are no prospects it might be in near or far future. We have to take into consideration that fighting liberating technologies in cyberspace, especially these, which play a role in intellectual property laws violations, has only produced more durable technologies for the same purpose. In that perspective, its *illicit usage, tax evading* or *societal disintegration* has become everyday reality. Governments are losing control over a vast amount of human activity as Sheila Jasanoff arues, but they were not in this situation.

Another example of this trend would be the case with global taxation. It has become a problem with services such as the global accommodation portal AirBNB or global taxi service UBER.[319] All of these services have become true thanks to a raising trust in *online reputation.* Systems of reviews and feedbacks are becoming important for our digital identities; the possibility to buy or sell products on portals such as eBay has

[315] Bob Crilly, "FBI Finds Method to Hack Gunman's iPhone without Apple's Help," *Telegraph.co.uk*, March 29, 2016, http://www.telegraph.co.uk/technology/2016/03/29/fbi-finds-method-to-hack-gunmans-iphone-without-apples-help0/.

[316] The~Economist, "The Terrorist in the Data," *28th November*, 2015.

[317] The~Economist, "Unfriended," *12th December*, 2015.

[318] Telegram.org, "FAQ Telegram Security," 2016, https://core.telegram.org/techfaq#q-how-are-mtproto-messages-authenticated.

[319] The~Economist, "All Eyes on the Sharing Economy," *9th March*, 2013.

become real only thanks to the system of *online reputation of our digital identity.* The self-control reputation systems provide better security to users than states through their regulation and law enforcement. Understandably, when it comes to these services, states do their best to put them under control. However, as the tax collection of global players is not an easy task, they also tend to prohibit them at all within their territories, but they barely can. Uber is a peer-to-peer service between users' mobile phones only and its success is visible all around the world.[320] Governments of course try to deal with this reality of their erosion in tax collection and regulation ability and as I argue later they have two options. Either to free ride as some countries do when they provide tax heavens or unite in order to regain power in global business taxation, regulation and governance.

Another topic mentioned in the manifesto and clearly visible today is the inability of state to keep national security secret. Cases such as the leak by Edward Snowden show how one dedicated man can significantly damage national security structure and the way how the security policy is regarded by the public. Snowden is a clear representative of these fundamental fears. It shows fears about implications coming from a huge amount of data about hundreds of millions of people in hands of few.[321] It shows what implications the application of crypto-anarchist ideology in practice can have to national security. Only a destruction of beliefs into a concept of nation state.

The whole situation with intellectual property that has changed the whole world from distribution of recordings on plates to data streaming all around the world was predicted as well. The idea of information smuggling is visible in private intelligence driven operations such as Red October[322] and the remark about *CryptoNet* is certainly today the *DarkNet*. The former predicted, the latter depicted by authorities that need to add the dark connotation in their defense to make clear who possess legitimacy. The clear emergence of two fighting discourses based on one emerging reality.

[320] The~Economist, "Uber Is Now More Popular than Taxis or Car Rental with Business People," *22nd January*, 2015.
[321] The~Economist, "Over to the Dark Side," *10th June*, 2013.
[322] Gomez, "Operation Red October Fuels Debate over Cyber Espionage."

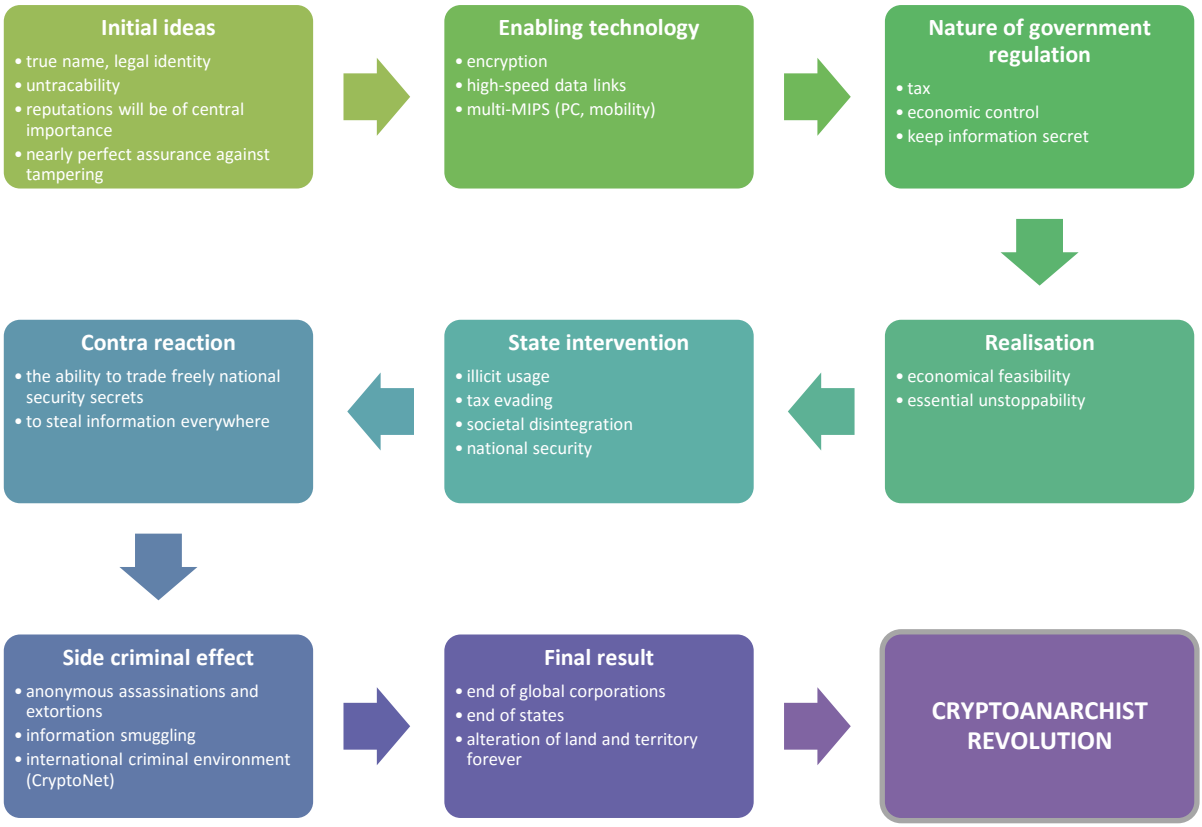


Figure 2 - The Crypto Anarchist Manifesto logical structure

Additionally, thirteen years later the reality was on the way. In an edited book from 2001 named *Crypto Anarchy, Cyberstates and Pirate Utopias*, the editor Peter Ludlow in the introduction argues that these utopic *cypherpunks* might be soon or later able to escape detection by states using advanced cryptography.[323] Seven years later Satoshi Nakamoto, still probably a genius ghost[324] who has never been met by anybody, published an article explaining the mathematical model of Bitcoin, which has been since then the first widely used digital currency, which is also called a crypto currency.[325] The system is designed that all transactions between wallets are open and visible to everybody. The system is used as a perfectly reliable clearing service for transactions as the clearing is provided by the community, which *mines* bitcoins by providing computing

[323] Peter Ludlow, *Crypto Anarchy, Cyberstates, and Pirate Utopias* (Cambridge, Massachusetts and London, England: MIT Press, 2001), doi:10.1108/14636690232094299 5.

[324] Andy Greenberg and Gwern Branwen, "Bitcoin's Creator Satoshi Nakamoto Is Probably This Unknown Australian Genius," *Wired.com*, 2015, http://www.wired.com/2015/12/bitcoins-creator-satoshi-nakamoto-is-probably-this-unknown-australian-genius/.

[325] Nakamoto, "Bitcoin : A Peer-to-Peer Electronic Cash System."

power; it is still bulletproof for hijackers on the way. Moreover, if an owner of a wallet is not making mistakes, the real identity is not discoverable. That includes exchanges with real money as the owner of an encrypted wallet is not known; yes, there are methods how to unveil the identity by combining more data flows from one or other sources[326] or simply by buying a product delivered to a particular address, but supporting an assassination of hated politician with anonymous bitcoins is reality as well[327] and it was mentioned as possible future in the Crypto Anarchist Manifesto. Germany, for example, recognized bitcoin as a "private money" in 2013 and made it totally legal currency; however, it is not recognized as a foreign currency, nor as a product, but as a "unit of account".[328] Other countries, in the contrary, have made it illegal; including Russia, China, Laos, Iceland or Bolivia.[329] The question whether these countries can effectively regulate the exchange in cyberspace remains clear; they cannot. Fifteen years earlier, the question of a completely detached cyber-crime environment was a discussion within utopias, right now it is a reality.

Dorothy Denning argued in 2001 that a new technology called *key escrow* will exchange the liberal cryptologic methods with new one into which the authorities will keep access,[330] while she argued against the feasibility of crypto anarchy ideas. Dorothy Denning finally admitted the low probability of spread of this technology and usage just in the next chapter.[331] However, the reality today is more complicated. Corporations use that technology to watch communication of their employees in general, while authoritarian states do the same, e.g. Russia, which is a bit special as each developer of any cryptographic technology needs a license according to the Russia Federal Law N 128-FZ *On Licensing Certain Types of Activity*. This is for sure not a solution as software can be

[326] A list of proven methods are available in Fergal Reid and Martin Harrigan, "An Analysis of Anonymity in the Bitcoin System," in *Security and Privacy in Social Networks*, 2013, 5–6, doi:10.1007/978-1-4614-4139-7_10.

[327] Richard Boas, "Sinister New Site 'Assassination Market' Enables Users to Contribute Bitcoins for Murder of US Officials," *Coindesk.com*, 2013, http://www.coindesk.com/sinister-new-site-assassination-market-enables-users-contribute-bitcoins-murder-us-officials/.

[328] Matt Clinch, "Bitcoin Recognized by Germany as 'Private Money,'" *Cnbc.com*, August 19, 2013, http://www.cnbc.com/id/100971898.

[329] "Bitlegal Tracks the Evolving Regulatory Landscape of Cryptocurrency, Digital Assets and Distributed Ledger Technology around the World," *Bitlegal.io*, accessed March 26, 2016, http://bitlegal.io/.

[330] Dorothy E. Denning, "The Future of Cryptography," in *Crypto Anarchy, Cyberstates and Pirate Utopias*, ed. Peter Ludlow (Cambridge, Massachusetts and London, England: MIT Press, 2001), 85–101.

[331] Dorothy E. Denning, "Afterword to 'The Future of Cryptography,'" in *Crypto Anarchy, Cyberstates and Pirate Utopias*, ed. Peter Ludlow (Cambridge, Massachusetts and London, England: MIT Press, 2001), 103.

acquired globally with no real restriction and if state restrict access to particular webpages, one can use The Onion Network to access everywhere and being anonymous.

An example about this losing battle between governments and geeks comes from Russia. In the case with VKontakte and Telegram messenger. They were both developed by Nikolai and Pavel Durov, Russian citizens who had to leave VKontakte when the government took over this most popular social network in Russia. The specific advantage of Telegram in comparison to all other messengers around is that encryption keys are generated, stored and deleted in each device. There is no way to break the system from a central point; authors do not save these keys on servers. This characteristic can be easily confirmed as the software is open source; thus community driven (the open source code is available to everybody). An example of community driven power over state institutions hardcoded into the software, which in addition has its own API, hence the logic can be used in infinite instant messengers others will develop later.[332] There is no way for anyone to break it. Spread of such technology would make the *key escrow* technology a non-sense.

One of the most profound example where states cannot match geeks in their technological advancement is the Pirate bay from Sweden; a torrent indexer. A web portal that provides just a list of torrents concerning movies, series, TV shows, porn, computer games, software and whatever else one can imagine. Torrent is a genius technology that is precisely designed to be unbeatable by authorities. When one user has a movie the others can download it, but not directly from one user. The point is that the availability of the movie is within the community of people who seek the movie; they do not know each other. Torrent clients maintain balance between each other that newly coming users can download pieces from these who came before them and so on. The movie is not stored on a server, but pieces of this movie is stored on users' computers that have been connected for some time and already downloaded portions from those who already watch the movie in that time. The web portal Pirate bay maintains library of these torrent

[332] Catherine Shu, "Meet Telegram, A Secure Messaging App From The Founders Of VK, Russia's Largest Social Network," *Techcrunch.com*, October 27, 2013, http://techcrunch.com/2013/10/27/meet-telegram-a-secure-messaging-app-from-the-founders-of-vk-russias-largest-social-network/.

files and has been a target of authorities several times. The developers were sentenced to imprisonment for up to almost one year, but the community around has kept the system on.[333] The last attempt by authorities, the so called 2014 December raid, to topple down the Pirate bay caused switch of the used technology to a completely decentralized system CloudFlare, a company which offers reverse proxy services that helps site to withstand DDoS attacks or other attempts of enforced shut down.[334] Right now, Pirate bay does not provide even the torrent files, but only magnet links. Hence, the web portal is probably unbeatable by the law enforcement agencies, but also can withstand direct DDoS attacks. Hydra from ancient Greek legends would serve as a near perfect depiction where this battle leads.

[333] Linus Larsson, "Charges Filed against the Pirate Bay Four," *ComputerSweden.idg.se*, January 31, 2008, http://computersweden.idg.se/2.2683/1.143146.

[334] "CloudFlare," accessed March 29, 2016, https://www.cloudflare.com/.

7. THE TRANSLATION OF UNBEATABLE TRUTH INTO AUTHORITY

"Knowledge is free. We are Anonymous. We are Legion.
We do not forgive. We do not forget. Expect us."

— Anonymous (the movement, undated) —

The crypto-anarchy manifesto gave the foundation of beliefs that a better and more liberal world without corrupted nation states is possible. The *church of knowledge* within its community is strictly oriented antagonistically against any kind of authority that may attempt to regulate any portion of human life. The belief is devoted to liberating technologies that can deliver trust using decentralized organization. Governments are approached as corrupted with no exemption. International organizations are understood to be established to govern powerless and technologies such as bitcoin can emancipate everybody from dominion of elites. Debates regarding democracy, while its core values are in their own interest, usually ends in giving somebody up being lost in a havoc of nation state governance system. They seek radical revolution by toppling down governments through undermining their legitimacy and credibility. In that perspective, whistleblower revelations are wind to their sails in order to fulfil the utopian vision of ultimate liberal and equal world to everybody – the anarchic eden. There is no space to discuss reformed democratic state governance using modern decentralized technologies to e.g. control state expenditures. Everything can be done by enlightened corporations of people that are not driven by transnational capital, but by anonymous donations of people willing to support their policy. When they move to the other extreme where libertarians lie, corporations that were before depicted as malign in cyberpunk are now perceived as a pure power that answers people's needs by answering the market.

The internet chatrooms, but also physical crypto-anarchist institutions such as the one in Prague called Parallel Polis,[335] are centers of these core ideological positions. Their institute has become famous throughout the world as they deliberately opened fight against the nation states, organize regular meetings or a huge international conference with the brightest names from world hacking communities. Meetings are named

[335] "Paralelni Polis," 2016, https://www.paralelnipolis.cz/en/.

suggestively: *"Bitcoin meetup. How much time is left to nation states?" or "Bitcoin meetup. Hivemind – the power of decentralized mind"*.[336] The statement of this institution is not different to other hacking communities throughout the world, the crypto-anarchist manifesto lies all the time at its foundations. Another such community would be a global hackers meeting DEF CON.[337]

Conferences, meetings, presentations, technology demonstrations, coffee bar where you can pay only with bitcoins and debates with representatives have been building new center of crypto-anarchist movement, in which the membership is well-deserved and reserved to those, who openly challenge state authorities. The international scope of the movement is giving birth to so called *epistemic community*[338] of people sharing the same values, beliefs and knowledge. Analogies to historical moments of oppressed people by authoritarian regimes are often used to demonstrate reasons, why we have to stand united against the governmental dominion of corrupted elites. All meetings are not far from sectarian repeating of core conspiratorial arguments of everywhere visible corruption that should spark light in *hiveminds* to stay united against the bad order. Giving the equation between liberal democratic and authoritarian regime in simplified concept of general nation state is a needed prerequisite of being a member. Questioning the manifesto as a radical left is usually appraised as a violation of crypto anarchist code that leads to exclusion from the movement. When the presumptive *field of concomitance* is systematized in such a way, it gives existence of authority, an institution that represents it. *Nation states should expect them.*

An important final remark should be made to depict what consequences such dynamics have had and certainly will have. As Singh argued, scholars usually omit the distinction between two kinds of power: the instrumental power and the productive power. While the former is focused on the possibilities of the technology, the former is oriented more on social aspects of power.[339] In the former version, technology is depicted

[336] "BITCOIN MEETUP | Hivemind - Síla Decentralizované Mysli," 2016, https://www.facebook.com/events/555520327962033/.

[337] "DEF CON," 2016, https://www.defcon.org/.

[338] Emanuel Adler and PM Peter M. Haas, "Epistemic Communities, World Order, and the Creation of a Reflective Research Program," *International Organization* 46, no. 01 (1992): 367, doi:10.1017/S0020818300001533.

[339] James N. Rosenau and J. P. Singh, *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, 2002, 10.

as an ambassador of future evil due to the unimaginable opportunities, while the latter adds to the former the cultural content of the community that has the intentions to do it. If we add the structural power conceptualized by Barnett and Duvall,[340] we reach a situation that even completely decentralized empire of crypto-anarchy can cause serious damage to the current international system. The argumentation of officials after Snowden revelations would serve as an example. In the end, the dystopian imaginations are not based on overemphasized power of script kiddies, but the power of the community worldwide that socially bounds people together based on particular values they share – the liberty from oppression. The centuries long struggle has been given with a new shape. I argue that it is important to understand the culturally founded and socially bounded community that is inspired by certain ideology. The power of the community rises with the attachment of libertarians, who are able to unbound themselves from the leftist utopia of the crypto anarchy paradise and make significant amount of money using the liberation technologies. Duval and Barnett also argue that in certain situations (in their example at the UN) can legitimate and constitute corporations as socially responsible actors by the discourse: *"the social processes and the systems of knowledge through which meaning is produced, fixed, lived, experienced, and transformed."*[341] These new actors, global corporations, will certainly play a role in deploying or modifying new political regimes how we deal with problems and also with security threats, especially in communication technologies, in cyber domain. The ability of Facebook to learn artificial intelligence to choose selected information that consequently make isolated bubbles of worldviews is one example. The need for feasible political regime in Solar System for upcoming asteroid mining, where states are responsible for business operations, but tend to bend international law in order to support their national businesses that require ownership of mined minerals, would serve as another example. New actors in new spaces tend to lay down new regimes and when the access, existence or operation in these space require specific technology, it will be these actors who tend to have the final word. This

[340] Michael Barnett and Raymond Duvall, *Power in International Politics*, *International Organization*, vol. 59, 2005, doi:10.1017/S0020818305050010.

[341] Ibid., 59:55.

dynamic creates an unpredictable environment producing radical uncertainty, *technological radical uncertainty.*

8. CONCLUSION

One may ask a question why so much cultural studies when it comes to cyber security. The research question at the beginning asked what is the source of the exaggerated policy full of imaginations. The concept radical uncertainty, which was extended to *technological radical uncertainty*, draws policy environment, in which policy makers are requested to make decisions over so complex technological environment that without proper expertise they simply cannot. New actors are given opportunity to use liberating technologies produced by crypto-anarchist movement. Technologies changing cyberspace so swiftly that is technically unbearable to govern related technology development and thus predict the implications of the newly acquired technology by unpredictable actors. The uncertainty of technology implications, the technology or clearly the consequences emanating from the technology that flows the same way as any post-modern social concepts. In that perspective, I drew the argumentation on two sources, the popular culture of cyberpunk and the post-modernist philosophy of Jean Baudrillard.

Cyberpunk literature is an important contributor to the debate as the crypto-anarchist movement stands culturally on it. Moreover, the dystopian depiction of the near future nightmare adds a content and reason to draw the dystopian imaginations by governmental experts or policy makers. The power of community to conduct an operation that can cause significant damage emanates from the culturally bound conviction in the fictional writings. The case with Heidi and Alvin Toffler who use imaginations close to the dystopian predictions to further apply produced fiction on possible near future development provides us with an example how certain imaginations can make its way to the serious policy making. However, when we come back to the sources, Baudrillard's idea of clashing two worlds of *Integral Reality* and *The Dual Form* show how the abuse of technology by one actor in order to totalize utopian visions of absolute security, for example by developing hard-to-control artificial intelligence patching exploits autonomously, produce resistance on the other side. While the resistance imprints its conviction of oppression in nation states, nation states conversely depict hackers operating in Dark Web as the forthcoming cyber terrorists. It shows, how

the politics regarding cyber security is still culturally bound in a world that is very close to cyberpunk dystopian depictions despite the fact that majority of policy makers have never heard this word, but are certain in a needed policy to address emerging threat of *cyber-war* and warn against possible *cyber-9/11* or *cyber-Pearl Harbor*. Ironically they create the dystopia as they are convinced about the non-governability, while the attempts to govern cyberspace tend to lead into post-modern quagmire nobody control or is even oriented in. We should remind the reader that the governance of internet technologies is the instrumental power, but certainly not the structural power.

Both actors are creating an environment in which the others arise as the most powerful. The corporations that were born in libertarian centers are in the end using technologies crypto-anarchists developed, which they are able to use with significant profit. The ungovernable chaos was described through the perspective of Baudrillard as a post-modern quagmire, where no one can be easily oriented; where on one is in charge. This is an important point to be used in the following chapter; in which I will discuss how nation states use technologies in order to conduct massive global surveillance in cooperation with corporations, but certainly without ability to be sure they are in control of the operation. At least, we can be assured that these corporation gained new knowledge from the intelligence community that can be used in order to support their market share. Such a development is a pure cyberpunk dystopian nightmare as the democracy and the election system seems to be put aside in benefit of more powerful actors that are not elected, but certainly with a global impact.

Despite the fact that the new power is now in hands of a new kind of actors who are untouchable, unrecognizable, unreachable, the critical infrastructure somehow does not fail every day and thus the demonic doom scenarios are not fulfilling. The national security experts omit the perspective of ungraspable postmodern dystopia of cyberspace and tend to defend it in a military way.[342] At the same time governments are scared of the ability to govern the near future, in which states do not have power over corporations running technology that has grown into our lives, but also into our minds and hearts as corporations like UBER have been able to deliver more fair system to particular business

[342] Rattray and Healey, "Proceedings of a Workshop on Deterring CyberAttack."

sectors than regulation by law. Paradoxically, as will be shown in the following part, nation states empower corporations in surveillance programs and lose control of the empowerment at the same time. However, there are other actors which are in control, at least of part of cyberspace, and it is not a nation state.

II.
CRIME, ESPIONAGE AND THE DAWN OF CORPORATE WARS

"Nobody needs to justify why they 'need' a right. (...) The burden of justification falls on the one seeking to infringe upon the right. (...) Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

— Edward Snowden, visit to Reddit on May 21, 2015 —

1. VARIATIONS OF CYBER-CRIME CASES

"It is with no doubt that cyber-crime has started playing a significant role in our lives." Similar sentence can be seen across all relevant annual reports concerning the topic of cyber-crime from cyber security firms, law enforcement agencies or technology corporations that are dependent on solid security such as Microsoft or Apple. However, what is cyber-crime then? One definition would be *any criminal activity enabled by cyber means*. However, it might look like that we have criminals on the one bank of the river and law enforcement on the other. It is not. Some activities such as defacement of webpage can be certainly understood by the geek community as a protest; even the DDoS attack on Estonia was by some people understood as a massive digital protest,[343] but clearly not as means of cyber war. In fact, for states it was understood as means of cyber war, for example by the political representatives of Estonia who wanted to trigger Article 5 of the Washington Treaty.[344] Moreover, law enforcement agencies may understand a DDoS attack as a criminal offence against the liberty of the server's owner. Result might be a requirement on the attacker to repay the losses caused by the attack. Who is right? The damage is a debatable variable when it comes to data as it is in a case when a peaceful protest takes place in the middle of the city. Is it a damage when one could not sell a burger on a street due to the mass protest taking place? The debate over losses caused due to the introduction of the internet, especially in music distribution business, is aligned in favor of the way how the business was made before the internet. Music business is a great example as the digital distribution was a problem until the day producers found a way how to distribute content online as well.

The right to protest is the first democratic liberty we possess. Understanding DDoS attacks by hacktivists in that way might finally completely change the perspective of their security impact, weather as a national security concern or just a crime causing damage. However, that does not apply to bank fraud, blackmailing people by encrypting their data with ransomware (recently kind of intelligently aimed to people including their

[343] Rid, *Cyber War Will Not Take Place*, 2013.

[344] Scott J. Shackelford, "Estonia Three Years Later: A Progress Report On Combating Cyber Attacks," *Journal of Internet Law* 13 (2010): 22–29.

postal addresses),[345] stealing credit card information on a seriously massive scale[346] or publishing the whole stolen national ID databases as in the case of Turkey on 4th April 2016.[347] Finally, it has not been a whole citizen database, but "only" about 50 millions.[348] The server with the link on torrent is down, but torrent itself will live probably a long time as the technology is simply unbeatable.[349] Some attack vectors are surprisingly simply. One can find a vulnerability on desktop sharing software such as Teamviewer and scan internet with a bot for a running service on random IP address; if successfully detected, hacker would take complete remote control over a computer and all security measures are for nothing. The digital ID, all passwords, access to PayPal and other services could be leaked and the hacker could cause a serious damage to one's life. All these actions can finally be done with automated bots. Not to mention that current phishing methods based on scam emails might quickly change to AI chatbots[350] learning from our own communication between family members about meaning of life.[351] Risk of deception by artificial intelligence during our online lives is becoming closer than ever in that perspective.

However, there are also attacks that might have a commercial background in supporting a movie that looks like a serious breach to national intellectual property, in which a president of the United States played an unwanted role, as it (maybe) happened in the case of SONY Pictures in 2014.[352] The word *maybe* is important as these cases usually flow away without deeper investigation and the conspiracy debates blossom. One thing is clear: SONY survived the attack, President Obama showed will to counter attack

[345] BBC News, "The Ransomware That Knows Where You Live," *BBC*, April 8, 2016, http://www.bbc.com/news/technology-35996408.

[346] Elizabeth Palermo, "10 Worst Data Breaches of All Time," *Tom's Guide*, February 6, 2015, http://www.tomsguide.com/us/biggest-data-breaches,news-19083.html.

[347] John Leyden, "Did Hacktivists Really Just Expose Half of Turkey's Entire Population to ID Theft? Entire Citizen Database? Probably Not," *The Register*, April 4, 2016, http://www.theregister.co.uk/2016/04/04/turkey_megaleak/.

[348] The website containing a link of stolen database was up between 4th April and 8th April 2016. On 9th and 10th was down. Link is: http://185.100.87.84/

[349] Pierluigi Paganini, "DB with Records of 50 Million Turkish Citizens Leaked Online. Are They Recycled Data?," *Security Affairs*, April 4, 2016, http://securityaffairs.co/wordpress/45981/data-breach/db-50-million-turkish-citizens.html.

[350] Jane Wakefield, "Hello, I Am BBCTechbot. How Can I Help?," *BBC News*, April 12, 2016, http://www.bbc.com/news/technology-36024160.

[351] Metz, "Google Made a Chatbot That Debates the Meaning of Life."

[352] Jane Wakefield, "Whodunnit? The Mystery of the Sony Pictures Hack," *BBC.co.uk*, December 18, 2014, http://www.bbc.com/news/technology-30530361.

on a cyber-attack, in this case against North Korea that is probably the least likely adversary causing an international unease against the US.[353] Additionally, the movie was significantly successful in theaters despite its mediocre meta-critic evaluation and other states are aware of US capability to cut a nation from the Internet if needed according to national security, which can be understood as a demonstration of power and thus have a strategic deterrent element. North Korea, which is not connected to the Internet, only selected computers at the national administration level, is a great target to demonstrate power. Moreover, in the case of North Korea it can be certainly done without any serious diplomatic repercussions. SONY Pictures hack is a great example how the uncertainty of consequences in crime event, the actor behind and the intentions at the beginning can escalate into an international cyber conflict; everything based on assumption as digital forensics are far from providing undisputable proof.[354]

[353] David C. Gompert and Martin Libicki, "Waging Cyber War the American Way," *Survival* 57, no. 4 (2015): 7–28, doi:10.1080/00396338.2015.1068551.

[354] J F Blanchette, *Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents* (MIT Press, 2012).

2. THE BLURRED EMPIRICAL EVIDENCE AND ITS (MIS)INTERPRETATION

The assessment of cyber-crime consequences is a Sisyphean job. One approach to the assessment whether cyber-crime is a rising threat might come from calculation of losses caused through cyber means. However, that is exactly the debatable approach. Stealing intellectual property in means of distributing torrents online usually cause losses to the producers who argue that each watched video downloaded using the torrent technology is a loss equivalent to one unsold DVD or ticket to the cinema;[355] how many jobs have been lost due to piracy etc. This approach to loss calculation is of course criticized using the opposite arguments that piracy can help to spread culture, produce other jobs in other sectors as it does not destroy national economy, but influence particular business models, so it just transforms how the sector makes money.[356] Why numbers simply cannot play a significant role in the assessment process is not visible in these fluid debates, but also exactly in numbers. For example, BSA – Business Software Alliance – argued in 2003 that software piracy was responsible for $812 billion of losses on a global scale.[357]

However, McAfee Lab in cooperation with Center for Strategic and International Studies calculated all cyber-crime (software piracy is a just tiny piece of that mammoth) related losses in 2014 to $375 billion with a maximum at $575.[358] Another estimate put the prediction in the middle on $445 bn.,[359] citing also a report by McAfee[360] mentioning possible loss of 150.000 jobs only in Europe. The criticism of this approach to cyber-crime impact assessment was already mentioned. One may ask, how is it possible that in ten years, during which the connected people to the internet at least tripled, if not

[355] Not an actual infographic, but a very well demonstrative one to show how numbers can be misinterpreted. Go-Gulf Blog, "Online Piracy in Numbers – Facts and Statistics [Infographic]," 2011, http://www.go-gulf.com/blog/online-piracy/.

[356] Joe Karaganis, "Chapter 1 : Rethinking Piracy," in *Media Piracy in Emerging Economies* (SSRC Press, 2011), 16.

[357] B Parker, *Introduction to Globalization and Business: Relationships and Responsibilities* (SAGE Publications, 2005), 343.

[358] Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime," *Mcafee*, no. June (2014), http://www.mcafee.com/kr/resources/reports/rp-economic-impact-cybercrime2.pdf.

[359] Rhiannon Williams, "Cyber Crime Costs Global Economy $445 Bn Annually," *The Telegraph*, June 9, 2014, http://www.telegraph.co.uk/technology/internet-security/10886640/Cyber-crime-costs-global-economy-445-bn-annually.html.

[360] Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime."

quadrupled, has had decreased? To add a different number, another argues that we will face losses in trillions of dollars soon; when speaking in terms of astronomical numbers one begins adding special concepts such as *crime wave* or *epidemic* when it comes to emerging *wave* of cyber-crime; the author is talking about quadrupling between 2013-2015 and thus he is quadrupling to 2019.[361] Different actors approach the problem differently and understandably pushing their well-disposed perspective discursively forward.

There is no one report made by respected institution saying that cyber-crime is on retreat, quite the opposite. If a particular technology is dropped by criminals, they started using something different, more sophisticated, more successful and more focused on target. These reports are from different actors whose interests vary. EUROPOL, as a central law enforcement body of the European Union that finally do not have law enforcement power as it has a supportive role in between national enforcement bodies, publishes every year an annual report concerning current state of cyber-crime. Their perspective is not focused on an annual loss to the industry that has been producing music or distributing movies for decades as it is in a case with BSA. EUROPOL much more focuses on reported frauds against citizens. In that perspective, they do not care about the intellectual property theft too much as their role is to ensure law enforcement capabilities between national law enforcement institutions to combat organized crime e.g. with ransomware that – according to almost all reports – has risen for about 60% only in 2015. In particular, a similar raise is mentioned in a report by EUROPOL named every year IOCTA,[362] in a Kaspersky Lab overall year statistics,[363] in a McAfee Lab Threats Report[364] or in a Symantec Internet Security Report.[365] Ransomware is in contrast to the drew losses by music distribution corporations a real amount of money somebody had to pay to the hackers in order to unlock critical data on his/her computer. In that

[361] Steve Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019," *Forbes*, January 17, 2016, http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6900f7df3bb0.

[362] Europol, "The Internet Organised Crime Threat Assessment (IOCTA)," 2015, https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.

[363] Kaspersky Lab, "Kaspersky Security Bulletin 2015: Overall Statistics for 2015," 2015, https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf.

[364] McAfee Labs, "McAfee Labs Threats Report," 2015, www.mcafee.com/us/mcafee-labs.aspx.

[365] Symantec, "Internet Security Threat Report," vol. 20, 2015, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

perspective, EUROPOL calculates losses based on the amount of money directly paid in clear criminal offense.

So when it comes to troubles caused by cyber-crime, should law enforcement focus on imaginative losses in the middle of collapsing global business models or on a rising trouble in which a single citizen is directly targeted with ransom around $800 and the number of targeted individuals raises to millions? Tough question though; the answer would be both of course, but the perspective changes with interests behind particular actors and these actors are quite successful in cultural shifts that are reshaping the acceptability of new practices of communication, knowledge creation and even digital personal identity.[366] One may ask the question whether nation states should serve transnational corporations and their interests or try to be of help to their citizens.[367] When a hacker uses a stolen credit card to buy Bitcoins, the only result is a blocked credit card, money return by insurance company and zero possibility that the hacker will be caught, but Bitcoins remain in the wallet of a hacker. Police cannot do anything as hackers can easily keep their wallets in a complete anonymity. When a hacker takes control over a computer and uses PayPal to buy digital currency for himself/herself, the possibility is higher as he/she could leave some traces. However, business on the line of the attack such as money exchange portals are closer to solve a problem than a national police. Hacker from China buying Bitcoin in United Kingdom using a Czech account is an unresolvable burden for current police capabilities and with raising number of such attacks their capability to act is again close to zero. Law enforcement agencies tend to go after wider organized crime that is connected to physical world such as dealing drugs on markets of DarkNet in Operation Onymous.[368]

When talking about cyber-crime on individuals on a massive scale, we should also take into consideration crime focused on industries that is not called crime, but *industrial espionage*. The attack defines the consequences, not the actor. That is the reason why the red line between crime and espionage is getting blurred and is discussed here together.

[366] Bauman et al., "After Snowden: Rethinking the Impact of Surveillance."

[367] I personally experienced two attacks on myself in four months that showed me how police are 100% incapable to even grasp the problem.

[368] Europol, "The Internet Organised Crime Threat Assessment (IOCTA)."

States are creating lists of critical infrastructures related to national security; however, they are run by private companies (or transnational private companies or corporations) and thus private companies are responsible for smooth operation of them and consequently smooth lives of citizens. Crime has become espionage and thus a national security concern. *Stealing* intellectual property of a particular industry is called *espionage*. Capability to take control over industry installations is called *cyber war*. Both can be a mere *crime* as corporations simply tend to get some information from their opponents. Intentions behind matters and as intention of an adversary state is higher on a scale of national security, the imagination blossom. One may register the point with EUROPOL, when a EU body does not possess enough law enforcement powers as it only helps the national bodies in their coordination, cyber criminals are quite in a better position when doing business on a global scale with hideouts wherever they want. This element of fear emanating from incapability of states to act is driving states into a maze, into a fully uncontrollable situation related to national security. It is not only about states, but there are plenty of other actors somehow involved and each of them understand the situation differently. When it comes to construction of *industrial espionage*, one had to add a national security concern to a cyber-crime case to call it *espionage*. Stealing massive databases of whole nations is just a massive crime, but stealing AutoCAD plans from industries is understood as a national security concern. The intention behind the attack is important in creating an espionage label to the crime. The label, which is created discursively through formation of the field of concomitance, where the authority is the key to give the label appropriate legitimacy.

3. FROM AN IDEALISTIC MOVEMENT INTO A CHALLENGE FOR A NATION STATE CREDIBILITY

A small group of senior officials believed that they alone knew what was right. They viewed knowledge of their actions by others in the Government as a threat to their objectives.

— Report of the Congressional Committees Investigating the Iran-Contra Affair, November 1987 —

Cyber-crime and cyber-espionage have somehow become parts of our lives. It would be unfair to argue that the whole reality of newly emerged security problem due to characteristics of cyberspace such as near instantaneity, remote accessibility and the communication networks based on nice working, but less secure technologies, is not emerging. The point here is to show how the agenda has been created by particular actors and put it into the context of their presumable interests.

Let me come back to the Figure 2 regarding the structural logic of crypto-anarchist manifesto and briefly summarize its objectives in a relation to current environment, which geeks call *hacktivism,* law enforcement agencies call *cyber-crime*, national intelligence bodies call *espionage* and national security in defense matters *cyber-terrorism*. It is hard to find the line where the crime ends, when it overlaps with espionage and when it triggers alarm of national security. Hence, the perspective I decided to take is to analyze the reasons why national security discourse tend to take cyber-crime activities and call it national security; especially in times, when in order to deepen national security nation states are leaving the principles and values of liberal democracy. Then I will move to the reading of current hacking groups that are considered as actors of *cyber-crime*, I will discuss ethics behind *hacktivism* and then analyze how do these two perspectives relate.

3.1. The enchantment of encryption technology and the reaction of governments

First, in the Manifesto,[369] we can read that one day we might be in near perfect state of technology that help to avoid tampering communication networks. A different

[369] May, "The Crypto Anarchist Manifesto."

reality was unveiled by Edward Snowden. However, the revelation only helps providers to take the problem seriously, improve the technology, refine the system of communication and motivate people in using better encryption technologies. The recent decision by WhatsApp[370] would serve as an example of a corporation introducing near to perfect encryption. They have been working on it since the Snowden revelations, thus for years, but it is unclear how this decision is related to the policy of Facebook, which owns them now, and which was according to Snowden allegedly included in the PRISM operation.[371] However, Facebook now provides a service of peer-to-peer messaging, in which the sender can set the delay before the message is deleted. One may guess that the move to encrypt messages might be just a pleasing move alongside with raising popularity of applications such as Telegram. It can be understood as a corporate marketing strategy of deception aiming on better brand essence and it will be of course hard to believe whether companies such as Facebook can provide the same trusted technology than open source Telegram, in which everybody can check how the technology in fact works.

The outcome is clear. We are seriously on the way to the world of *near perfect assurance against tampering*; at least we are for sure heading towards that world, in which we will be able to choose messaging technology, which will certainly be completely unbreakable by authorities. When it comes to counter terrorism policy of nation states, this heading is a total disaster for general intelligence objectives and the debate that nation states have to step in, and force encryption developers to understand that gathering of intelligence is needed, is really hot.[372] However, this does not play into the hands of nation states as they simply do not have enough power to ban these technologies completely. It had been state, or any sovereign actor, for centuries who granted access (anywhere); now the access is granted by corporations, which even do not need to have access to the encrypted data of a user. It does not matter whether the access is in physical

[370] Natasha Lomas, "WhatsApp Completes End-to-End Encryption Rollout," *Techcrunch*, April 5, 2016, http://techcrunch.com/2016/04/05/whatsapp-completes-end-to-end-encryption-rollout/.

[371] Steve Nolan, "Revealed: Google and Facebook DID Allow NSA Access to Data and Were in Talks to Set up 'Spying Rooms' despite Denials by Zuckerberg and Page over PRISM Project," *Daily Mail*, June 8, 2013, http://www.dailymail.co.uk/news/article-2337863/PRISM-Google-Facebook-DID-allow-NSA-access-data-talks-set-spying-rooms-despite-denials-Zuckerberg-Page-controversial-project.html.

[372] The~Economist, "Going Dark," January 17, 2015, http://www.economist.com/news/leaders/21639506-just-threat-terrorism-increasing-ability-western-security-agencies-defeat.

world or in cyberspace as the point is that the granted access is related to one's everyday life. It is either a corporation such as Facebook that was born in libertarian lair of Silicon Valley or open source decentralized technology such as Telegram that is an exemplary piece, an outcome of crypto-anarchist motivations, who governs the technology development.

We can be assured that national security discourse, especially on the imaginative global terrorism threat, will be built on the raising mountain of evidence of cyber-crime such as bank frauds or ransomware and will additionally be called *cyber terrorism*. The national security will be arguing that this move of global IT corporations of deepening encryption technologies is building unbearable burden to national security bodies dealing with terrorism, cyber terrorism or other threats to a nation state, while the terrorist will operate better as the intelligence will not be able to act. The point is that corporations will not move out from this direction as the need of trust into their services on a global scale is higher in their profit oriented interests that their concerns of particular national security on a nation state level. More probable is that we can experience huge hacks between these corporations to undermine trust into one's security measures rather than seeing corporations how they actively cooperate with states. Last example between FBI and Apple would serve as an example as the iPhone was finally broken by an unknown third party.[373] States tend to add non-state actors into the game who then act according to their interest. This is playing with fire and Red October operation probably run by a private decentralized corporation-like global cyber gang just underline it.[374] Recent description of such global corporate-like run gang should serve as an evidence that this process is already on the way.[375] No one non-state actor will act to fulfill interest of a nation state only because it previously ordered its services. Hacking Team from Italy (see the Table 3 - Selected hacking groups.) should serve as an example

[373] Crilly, "FBI Finds Method to Hack Gunman's iPhone without Apple's Help."

[374] GReAT, "The 'Red October' Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies - Securelist," *Kaspersky Lab Report*, 2013, http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies; Gomez, "Operation Red October Fuels Debate over Cyber Espionage."

[375] "Security Snapshot Reveals Massive Personal Data Loss," *BBC News*, April 12, 2016, http://www.bbc.com/news/technology-36024570.

of such profit run private business, which is fueled by fear of states, which buy their services.

3.2. The miss of PRISM and the dawn of ultra-libertarian technologies

Second, in the Manifesto,[376] the thought regarding *avoidance of taxation* and any kind of *economic control* is moving also to an unpleasant point for governments as a guarantor. States are losing their credibility due to unveiling secrets such as the mammoth espionage operation PRISM revealed by Edward Snowden, which – we can presume here – violated principles of liberal democracy. PRISM unveiled surveillance that was far away from what one can even imagine from a liberal democratic state. The working reason to claim that states are losing their credibility by abandoning liberal democracy values is the fact that states have moved their intelligence strategy from high degree of certainty about a small amount of data to high degree of uncertainty about a large amount of data; literally to watch everybody and everywhere who was accidentally in their way. Up to hundreds of millions, maybe billions, of people.[377]

As Bauman puts it, one may ask a question in whom security such a global surveillance has been conducted? International intelligence efforts of several key countries, which finally taped each other highest representatives, included global corporations, gave them insight into national intelligence strategies and did everything in a mixture nobody probably even understand completely cannot be conducted in the name of national security and it is far from securing the most important – liberal democratic values.[378] Interesting on this moment is that scholars were writing articles to argue how intelligence strategies will have to adopt to a new fluid post-modern environment which is: first, free from boundaries thanks to networking, second, which will have to focus on fragmented targets, third, which will have to deal with mysteries created by all on a global scale like a reproducing fractal, fourth, will have to deal with digital identities and, fifth, one centralized intelligence factory will be lost in the flood of

[376] May, "The Crypto Anarchist Manifesto."

[377] Siobhan Gorman and Jennifer Valentino-devries, "New Details Show Broader NSA Surveillance Reach," *The Wall Street Journal*, August 20, 2013, http://www.wsj.com/articles/SB10001424127887324108204579022874091732470.

[378] Bauman et al., "After Snowden: Rethinking the Impact of Surveillance."

knowledge and information including raising participants from a corporate world.[379] Not a single point on a risk of a nation state dissolution in that post-modern simulacra, while focusing on reactivation of its credibility as a guarantor of security in a classical concept of social contract. Intelligence has been focused on national secrets and national security for millennia and now it is mixed with other states and mainly with global corporations that will never voluntary act in the interest of one single nation state if that action hampers its business.

The outcome is clear, citizens are moving forward to use technologies that can provide them trust, security, guarantee and which avoid state intervention. Some of these sophisticated technologies have been already developed. Blockchain serves as a community controlled transactions system (Bitcoin is based on the blockchain technology) without a need of authority – and thus state – above it. Blockchain as a universal bulletproof method of any meaningful subject-to-subject transactions that can be adopted to the extent that bank-to-bank transactions will become unsecure and illegitimate in the eyes of citizens. It is not only giving hackers their hope about their dreamed world,[380] it is giving a hope to solve securely and reliably any meaningful transactions between anybody without a central authority. It can be used even for real estate transactions as the open transaction method provides buyer with certainty that the seller is owner of the respected property.[381] One may argue[382] that the state was at the beginning of the Internet,[383] but any other would argue back that states do not steer the technology development. Private business does.

What governments tend to steer is the discursive labeling of particular technologies as being part of criminal offensive actions or interstate espionage. When such labeling statements are appropriately established within a *field of presence,* the action taken by authorities is usually to blame it, to produce the *field of concomitance*, to

[379] Andrew Rathmell, "Towards Postmodern Intelligence," *Intelligence and National Security* 17, no. 3 (2002): 87–104, doi:10.1080/02684520412331306560.

[380] Kutiš, "Bitcoin - Light at the End of the Tunnel for Cyber-Libertarians."

[381] The~Economist, "The Trust Machine," October 31, 2015, http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine.

[382] Aimée Hope Morrison, "An Impossible Future: John Perry Barlow's 'Declaration of the Independence of Cyberspace,'" *New Media & Society* 11, no. 1–2 (2009): 53–71, doi:10.1177/1461444808100161.

[383] Ryan, *A History of the Internet and the Digital Future*.

produce new knowledge related to technologies, knowledge that serve the hypersecuritization purposes. The case with block chain technology, which can be used to 100% bulletproof transactions of anything including digital currency, a technology, which is already confirmed as almost 100% bulletproof, is labeled as being part of criminal underground. The only reason why is the uncertainty of the technology governance. However, when two subjects make a decision that transaction of real estate can be conducted using block chain technologies, the authorities will lose their relevance.

The recent Panama Papers cause shows how traditional bank-to-bank transactions to tax heavens are seriously exploited by powerful and rich people.[384] States tend to undermine trust into Bitcoin by putting it into the cyber-crime discourse as Bitcoin is used in DarkNet areas on portals selling drugs such as Silk Road.[385] They build heavy *field of concomitance* as the premises coming from the experience of Bitcoin usage creates a reasoning, models and are produced by authorities that the creates distrust into hard-to-govern technologies. Bitcoin can be used in DarkNet and is vastly used for transactions between criminals; however, it can be completely transparent in comparison to bank-to-bank transfers. Bitcoin can paradoxically play the positive role as it can provide a clearly transparent global list of transactions, because all transactions are already transparent.[386] Nevertheless, such a rational usage of technology is not imaginable as the dystopian curtain that covers these technologies is culturally and not rationally developed.

One may ask how is it possible that the technology thought to be the evil for transparent transactions is finally quite the opposite. Transactions are transparent, not owners of wallets and what people are buying. Both can change, especially in official transactions if one is interested in gaining trust and the ideal state of a democratic government is that the government is under control of demos. In the case of WhatsApp or Telegram we can observe how habits of all can switch very quickly if some service loses

[384] The~Economist, "Leak of the Century: The Lesson of the Panama Papers," April 9, 2016, http://www.economist.com/news/leaders/21696532-more-should-be-done-make-offshore-tax-havens-less-murky-lesson-panama-papers.

[385] Kim Zetter, "FBI Fears Bitcoin's Popularity with Criminals," *Wired*, May 9, 2012, http://www.wired.com/2012/05/fbi-fears-bitcoin/.

[386] Andrew Quentson, "Panama Papers Scandal Shows How Bitcoin Could Stop Corruption," *Bitcoin.com*, April 4, 2016, https://news.bitcoin.com/panama-papers-bitcoin-stop-corruption/.

its legitimacy and see it on a global scale. The same shift from a bank transfer method is not probably meaningful tomorrow, but if one small democracy in the world chooses blockchain as a credible method for subject-to-subject transactions, we might expect a significant pressure on political representatives to adopt technologies that have *hardcoded* trust; especially for governmental credibility based on tougher corruption practices.

This is not wishful thinking as blockchain can bring more trust to international exchange markets and transform them completely; as one wrote this: "Californian state" model of ultra-libertarians will not be in interest of powerful, but the probability of its realization is not a dream.[387] Governments will have to act to keep power and to keep democratic order as they stood at the beginning of this tacit neoliberal revolution since the 30s[388] that is reshaping with radical thought to techno-ultra-libertarian movement that paradoxically undermines them. The direction of the technology adoption is much more driven by the sociological drivers, habits based on more trustful solutions (case of UBER) than any other service regulated by state authorities. However, we observe a different approach by the authorities, discursive production of distrust, which might (or might not) have origin in dystopian cyberpunk predictions. Hence, authorities tend to steer the technology development in untenable regime of non-governable policy.

If we read the manifesto carefully, we are not reading about possible tax evasion, but about toppling down corrupted governments by altering the fundamental relation between citizens, corporations and governments. I am putting emphasis on – governments. They cannot like these processes and will defend current power status quo by pointing on imaginative terrorism, drug dealers in DarkNet and tax evaders while being corrupt and found guilty through leaks such as Snowden or Panama Papers. The point of crypto anarchist manifesto is to keep (as I said geeks are willing to respect authorities to some extent that does not reach a threshold of oppression) legitimacy of governments, manifest is not as radical as it is interpreted in this perspective. However,

[387] The~Economist, "The Great Chain of Being Sure about Things," October 31, 2015, http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable.

[388] George Monbiot, *Neoliberalism – the Ideology at the Root of All Our Problems* (Verso, 2016), http://www.theguardian.com/books/2016/apr/15/neoliberalism-ideology-problem-george-monbiot.

as authorities keep themselves locked in imaginations based on built field of concomitance, new field of truth that particular technologies are hostile, they lose the moment of being able to govern their application. Of course, such an approach is not universal and we can observe differences around the world; nevertheless, the revelation of PRISM does not give the Western democracies too much credit. On the other hand, the situation shows how current western-type democracies need to shape their policy in a legitimate way as much as possible, much more than before.

Right now, we see the tax evaders on the governmental side, which is not going to help governments in their future fight for their credibility when it comes to taxation policy of nation states. If governments are not able to solve this global corruption of leading persons, we might be assured that governmentally uncontrollable technologies will only spread as they have evolved to current state from zero in the last three decades. Combination of Panama Papers and Snowden revelations might give citizens feelings that something is wrong on the side of nation states and will use more secured technologies not only to avoid surveillance, but also to avoid the exploding cyber-crime, which nation states are not able to solve sufficiently due to its global scale and character as in the case of ransomware. Encryption and other community driven security can solve a lot in that perspective and the dawn of such global market is visible. However, it is a nation state in the name of national security who point on developers of these liberating self-controlling technologies as being illicit, fraud, unreliable and devoted to DarkNet that is only about drugs,[389] while they are emerging as a reaction to state surveillance and incapability to solve globally growing massive cyber-crime.

However, the possibility that black market economies will spread enough to be one day bigger that economies controlled by states was argued as well.[390] The counter reaction of a nation state is that they discursively add any of these technologies into the Foucauldian field of presence of general cyber-crime discourse depicting unwelcome changes to fundamental foundations of relation between state and citizen. My point is not to undermine the principles of a nation state, but to point on a generic process of spreading particular self-controlling liberating security technologies, which has a backing

[389] Zetter, "FBI Fears Bitcoin's Popularity with Criminals."
[390] Ludlow, *Crypto Anarchy, Cyberstates, and Pirate Utopias*.

from cyberpunk culture and crypto-anarchic ideology that, as a result of wider global usage, undermines the principle of a nation state as a guarantor of one's security. Additionally, I argue, that policy makers of nation states are directly reacting on that contra-state discourse by securitizing actions of hacktivists as a threat to national security, while the purpose of many of these liberating technologies is to deliver security to the citizen; hence, the same objective.

3.3. The discourse behind construction of evil and the glimpse of a world state

Third, in the Manifesto,[391] we are reading about *CryptoNet*; an anonymous network for global communication and transactions, which will be understood by the governments as an evil needed to be destroyed. Thirty years later hacking groups are approached as one group of cyber-criminals helping to build so called *DarkNet* with no distinction of what is their real objective. They *"can attack financial institutions with a few clicks of a computer mouse"*, but at the same time in the same article they *"have now developed the scale and sophistication to be able to crack even the most robust cyber-defenses"*; or they attack banks for profit, sell the information on DarkNet or did it as a part of a broader intelligence operation.[392] The definition of *DarkNet* would be everything, which is not available as an open website from search engine. However, discursively *DarkNet* is everything related to cyber-crime. It is not only about encrypted communication, but also about all the corners unachievable by indexing robots of corporations such as Google. However, for law enforcement agencies, *DarkNet* is likely equal to Silk Road or other market places with illegal stuff.[393] Illegitimacy is here discursively constructed in order to support interests of a nation state rather than to be discussed as a network of people seeking liberating and secure technologies. We can also observe it in a discursive merger of hacktivism with clear cyber-crimes. *DarkNet* is a great

[391] May, "The Crypto Anarchist Manifesto."

[392] The~Economist, "Hacking the Banks," August 28, 2014, http://www.economist.com/news/business-and-finance/21614181-who-lies-behind-latest-cyber-attacks-jp-morgan-chase-hacking-banks.

[393] The~Economist, "Winning the Battle, Losing the War," November 7, 2014, http://www.economist.com/news/business-and-finance/21631360-fbi-try-close-down-silk-road-again-winning-battle-losing-war.

example of concept that is discursively constructed as a network of cyber-crime, because it is out of governmental sight and power.

When the US government imposed prohibition in 1920s, events led to emergence of Al Capone. The emergence of *DarkNet* is nothing else than a reaction on a prohibition of certain technologies. It is not only the Silk Road; it is a testing bed of liberating technologies from any kind of oppression that are developed by people sensitive on online security and thus can help tackling cyber-crime. These are prevalently the same people – geeks – who work for global security companies. *DarkNet* does not contain drugs only. Silk Road is a side effect as Al Capone. The opposition of a nation state and general fight of law enforcement agencies would only pour fuel into these liberating efforts. State reacts on a deviance from normality they cannot control and require disciplined behavior as observed by Foucault.[394] Cyberpunk literature repeatedly depicts societies at the boundaries of megacities that create impervious social structures by the central authority, which has to depict them as uncontrollable areas, shantytowns, to raise the argument of their normalization from deviance. Nevertheless, paraphrasing Foucault, Julie Cohen argue that neither order as in the colony, nor the freedom of the brothel is a perfect solution[395] even when it comes to the debate between crypto-anarchist revolution and states ordering tendency by calling themselves the authority securing free speech on the internet.

We stand on a brink of the age that will not be governable by two hundred states, especially when a powerful state illegally use their law enforcement power on a territory of the other states in order to preserve justice.[396] The uncritical call for international cooperation to tackle cyber-crime in any single national cyber strategy only reduces power on a national level, gives false legitimacy for conducting massive surveillance programs on a global level, while talking about unbearable scale of cyber-crime they have to beat, which is far from being effectively solved by interstate cooperation. That might help the global law enforcement integration, which might finally lead to inevitable world

[394] Foucault, *Discipline & Punish: The Birth of the Prison*.
[395] Julie E Cohen, "Cyberspace As/and Space," *Columbia Law Review* 107:210, no. 1 (2007): 210–56.
[396] Reuters, "Kim Dotcom Raid Illegal, New Zealand Court Rules," *The Telegraph*, June 28, 2012, http://www.telegraph.co.uk/technology/news/9361759/Kim-Dotcom-raid-illegal-New-Zealand-court-rules.html.

state in cosmopolitan utopias.[397] Nothing good for a concept of a nation state, but the current state of affairs lies in the policy of 70s, in which policy makers thought that technologies can spread liberal democracy worldwide despite the resistance of less liberal states. Authorities of the western-type democracies should rather preserve liberal democratic values rather than hypersecuritize communities that emerged from these values.

3.4. The fluid dissolution of the nation state authority

Fourth, in the Manifesto,[398] as states intervenes into the socially constructed devil of CryptoNet, the resistance will rise, information will be traded freely and will include national security secrets. Parallel Polis or Snowden revelations are exactly the kind of rising resistance. The fact that NSA is spying everywhere on everyone including their own allies, their own US citizens and highest politicians in allied nations at an unprecedented scale, using breathtakingly sophisticated tools sparked a profound debate whether the concept of national security tend to defend itself or whether the purpose of a state is still here to defend the ideas of liberal democracy as Bauman argues.[399] He raises an interesting point by asking a question to whom the nation states are responsible when they include other states into espionage, which was in history reserved to intelligence of that respective states, but moreover, when they include global corporations that walk out from this campaign aware of intelligence practices, but are run by profit. Nation states, driven by imaginative global terrorism threat, are in that perspective actively working on their own removal from public life as the purpose of intelligence once globally enacted is getting locally detached from citizens of that respective state. Whose intelligence it is then? The only result of Snowden revelations will be higher legitimacy of crypto-anarchist movement as it is the source of tools helping citizens' strengthen their privacy and finally also online security, which states are not able to solve as we are witnessing in

[397] D Held, *Democracy and the Global Order: From the Modern State to Cosmopolitan Governance*, Political Science (Stanford University Press, 1995).
[398] May, "The Crypto Anarchist Manifesto."
[399] Bauman et al., "After Snowden: Rethinking the Impact of Surveillance."

examples such as ransomware. Soon or later these technologies spread enough to hamper power of national authorities in cyberspace as they already do now.

However, as mentioned elsewhere and as will be argued and widely discussed in the next chapter, terrorism has become a central threat to national security; a production of new language that has normalized the policy against a threat that is more in our speech rather than in our physical reality.[400] Normalization of policy has forced other states to cooperate in order to achieve ultimate security or being expelled from the group named *coalition of willing.* Making a hacker terrorist is related to the exaggerated language rather than to emerging global threat we all have to face on a daily basis. The enforcement of other states to cooperate so forcefully will not reach to a wider cooperation towards the peaceful world. As the *war on terror* was identified as a trap[401] of too much exaggerated assumptions, *cyber terrorist* in *cyber war* is nothing else. If this perspective is valid, the replicating strategy of *permanent state of exception* tackling the imaginative threat of global terrorism and merging the evidence of cyber-crime with imagination of cyber-terrorism might be clearly base on the same basis; however, the inability to tackle with a constructed threat will lower legitimacy of the authority that is assigned to deal with it. The argument of the trap; a trap of socially constructed fields of concomitance that resonates in churches of knowledge. The threat is perceivable, the threat must be tackled, the threat is a threat to our freedom.

Nevertheless, if the nation state authorities construct a threat in decentralized crypto-anarchists, because they have developed the same technologies which are used by the decentralized terrorist groups for their organization, nation state authorities might find itself trapped similarly as with the global terrorism. The radicalization of the common population caused by the implications of spectacular terrorist attacks is caused even by the spectacular demonstration of sympathy with victims in procession of western politicians in Paris; it constructs enemies to us as it deepens seriousness of one mass murder, it accepts the content of radical Islam, its apocalyptic objectives and will

[400] Richard Jackson, "Genealogy , Ideology , and Counter-Terrorism : Writing Wars on Terrorism from Ronald Reagan to George W . Bush Jr 1," *Studies in Language and Capitalism* 1, no. 1 (2006): 163–93, doi:ideologie; terrorismus; reagan; bush; krieg; R Jackson, *Writing the War on Terrorism: Language, Politics and Counter-Terrorism*, New Approaches to Conflict Analysis (Manchester University Press, 2005).

[401] I Lustick, *Trapped in the War on Terror* (University of Pennsylvania Press, Incorporated, 2006).

challenge the liberal order. The same trap can be perceivable in the construction of cyber terrorist; it will produce a resistance that will challenge the liberal order.

4. HACKTIVIST ETHICS AND THE RISE OF DECENTRALIZED NETWORKS

"We can all be authority"

— The Lawnmower Man 2: Jobe's War (Farhad Mann, 1996) —

The history of hacktivism can be dated to 1984 when the word was coined by Steven Levy in his work *Hackers: Heroes of the Computer Revolution*.[402] Despite the early age of hacking, these early times founded the initial hacking ethics. Especially in principles of "hands-on" meaning that essential lessons about the world around can be learnt by taking things apart. However, seven core tenants were essential in 1984 and are today as well: *"(1) access to computers should be totally unrestricted; (2) hackers should always honor the "Hands-On Imperative"; (3) information should be free; (4) hackers should distrust authority and promote decentralization; (5) hackers should judge their peers only by their hacking, rather than any educational or professional pedigree; (6) it is possible to create beauty and art within the confines of a computer; and (7) computers can better a person's life."*[403] Since the beginning, the idea of being centralized or being under a centralized power was rejected; they have rather chose a decentralized clustered meritocracy.[404]

The ethical understanding of hackers' intentions can be divided into three branches: (1) *good hacker*, who breaks into the system to unveil vulnerabilities and share them with the administrator to alter the security measures, (2) *bad hacker*, with intentions to cause disruption for fame, (3) *greedy hacker,* hackers driven by profit where distinction between good and bad is dependent on further actions of the hacker.[405] The next move to hacktivism emanates from the second kind of hacker, who added a political layer to previously neglected issue. Anonymous fall exactly to this category as they do not seek profit, but they do attack to send a particular political message over a publicly neglected issue. These *performative hackers* have an intention to switch public discourse

[402] Steven Levy, *Heroes of the Computer Revolution* (Anchor Press/Doubleday, 1984), 27–36.

[403] List taken from Kelly, "Investigating in a Centralized Cybersecurity Infrastructure: Why 'Hacktivism' can and Should Influence Cybersecurity Reform"; Original detailed description comes from Levy, *Heroes of the Computer Revolution*, 27–36.

[404] Ibid., 29–30.

[405] Alexandra Whitney; Aw Samuel, *Hacktivism and the Future of Political Participation* (Harvard University, 2004), doi:10.4324/9780203485415.

in order to support an issue that is neglected or outshined by power of corporations or public media domination; it is about raising awareness of an issue they understood as important to public life.[406] Decades of evolution within hacktivist community have led to a development of widely respected movement that is fulfilling the principal initial ethical values ditched deeper in the wider society – The Anonymous.

Anonymous are *„an ontological shift on the terrain of identity at the very moment that identity has become the highest form of selection and exploitation in cognitive capitalism, the first glimpse of a form of life without identity on the Internet."*[407] It is a resistance to rising voluntary totalizing surveillance; a resistance against the perfect Panopticon; they wish to articulate a common voice to oppose these practices through *collective intelligence* of these still possessing consciousness; the hive mind, which we saw in the previous chapter about geeks. It is a resistance to the willingness of authorities to reach totalized power, which Baudrillard calls the *Intergral Real*; resistance to any fields of truths; a movement that does its best to overcome the unachievable crypto-anarchist utopia to answer the most ponderous social questions. However, they do it in decentralized way. Anonymous understand themselves as *an internet gathering* rather than *a group;* gathering that cultivates the hive mind by addressing precarious social issues. The ethics in decentralization of power based on good intentions fighting the rising mammoth of surveillance voluntary accepted by blind units of public life is what runs people to be a part of Anonymous movement; ideas drives them forward, not directives. Moreover, some of them tend to fight corporations willing to concentrate power such as the issue about killing Facebook from 2011,[408] which was quickly denied by another Anonymous representative as being false. However, the ethics behind it is more than the directives coming from non-existent center of the movement – the hacker ethics, the crypto anarchist manifesto and other written ideas are becoming norms of behavior. Despite the denied will to shutdown Facebook, the idea to fight any

[406] Ibid., 73.
[407] Halpin, "The Philosophy of Anonymous: Ontological Politics without Identity."
[408] Adrian Chen, "Hacker Plot to 'Kill Facebook' Is All a Terrible Misunderstanding," *Gawker*, October 8, 2011, http://gawker.com/5829659/hacker-plot-to-kill-facebook-is-all-a-terrible-misunderstanding.

centralization of power coming from Facebook might emerge due to generally known debatable Facebook business intentions.[409]

There were other threats from Anonymous, particularly on February 2012 Anonymous shared on Twitter the idea to shut down the whole internet as a revenge for adopting the law SOPA[410] in the United States.[411] The reaction of national security was quick. General Keith Alexander on 22nd February 2011 speaks about possible electricity outrage in United States as a consequence of a possible attack by Anonymous.[412] Anonymous are based on a participatory system. The one who votes for action participate, the one who is against particular action simply stay out of that action. One may disagree and, if so, he/she will not be part of that operation. In the end, the whole movement is still driven by the same values of individual emancipation from the allegedly corrupted system. The moment when Anonymous became famous was a clash with Scientology Church in 2008:[413]

"Anonymous has therefore decided that your organization should be destroyed. For the good of your followers, for the good of mankind – for the laughs – we shall expel you from the Internet and systematically dismantle
the Church of Scientology in its present form."

The conflict begun with Church's will to take down several websites hosting a video of Tom Cruise fanatically speaking on behalf of the Scientology Church.[414] They even take some legal measures against internet publishers, which finally provoke Anonymous to act. The political basement of their reaction to support free speech on internet was clear in that time and coined their political intentions to be demonstrated

[409] The~Economist, "Imperial Ambitions," April 9, 2016, http://www.economist.com/news/leaders/21696521-mark-zuckerberg-prepares-fight-dominance-next-era-computing-imperial-ambitions.

[410] SOPA - Stop Online Piracy Act. An act that was finally not adopted. It was giving higher power to law enforcement agencies in order to fight online piracy. Introduced in October 11 2011.

[411] Sangeeta Mukherjee, "Anonymous Threatens To Shut Down Internet On March 31 – April Fool Hoax Or Real Threat?," *IB Times*, March 31, 2012, http://www.ibtimes.com/anonymous-threatens-shut-down-internet-march-31-april-fool-hoax-or-real-threat-432468.

[412] Graham Smith, "Hacking Group Anonymous Could Shut down the Entire U.S. Power Grid, Head of National Security Warns," *Daily Mail*, February 22, 2012, http://www.dailymail.co.uk/news/article-2104832/Hacking-group-Anonymous-shut-entire-U-S-power-grid-head-national-security-warns.html.

[413] Anonymous, "Message to Scientology," *YouTube*, January 21, 2012, https://www.youtube.com/watch?v=JCbKv9yiLiQ.

[414] Unknown, "Tom Cruise Scientology Video," *YouTube*, January 17, 2008.

online. Anonymous were fighting for one of the core value of liberal democracy regime. Additionally, to the online campaign, more than 6000 people participated in operation *Project Chanology*, used the famous mask for the first time, and protested in streets of more than ninety cities worldwide.[415] The action against Scientology Church unveiled new characteristics of the online movement: *"(1) an unrelenting moral stance on issues and rights, regardless of direct provocation; (2) a physical presence that accompanies online hacking activity; and (3) a distinctive brand."*[416] They have become authority.

Beginning 2011 Anonymous has started to attack corporate and governmental targets. *Operation Avenge Assange* against Mastercard, Visa or PayPal was one of the first. These political attacks also begun with Arab Spring. Anonymous were distressed by the events when a Tunisian set on fire himself and investigated the background of that political move. They realized that some portions of the internet, especially concerning some truthful stories of the ongoing events, were not accessible in Tunisia and decided to act demonstratively to the Tunisian dictatorship by cyberattacks on Tunisian governmental websites.[417] Later in 2011, an alleged spinoff from Anonymous, LulzSec, attacked CIA.gov and Senate.gov, which was of course understood as a possible breach to the national security[418] despite the fact that having similar credentials for public website administration and access to CIA internal servers would be a monstrous human mistake, which is certainly not dependent on hacker's capabilities. Merging the DDoS attack against websites and politically motivated hacktivism has been recommended as a deliberate policy toward better national cyber security. The argument was that hackers behind Anonymous are prevalently young and thus might be subject to ideological capture before it is too late,[419] because their activities cost taxpayers more money than

[415] Tom Lamont, "Alan Moore – Meet the Man behind the Protest Mask," *The Guardian*, November 26, 2011, http://www.theguardian.com/books/2011/nov/27/alan-moore-v-vendetta-mask-protest.

[416] Kelly, "Investigating in a Centralized Cybersecurity Infrastructure: Why 'Hacktivism' can and Should Influence Cybersecurity Reform."

[417] Quinn Norton, "2011: The Year Anonymous Took On Cops, Dictators and Existential Dread," *Wired*, January 11, 2012, http://www.wired.com/2012/01/anonymous-dicators-existential-dread/all/1.

[418] Ellen Nakashima, "CIA Web Site Hacked," *The Washington Post*, June 15, 2011, https://www.washingtonpost.com/national/national-security/cia-web-site-hacked/2011/06/15/AGGNphWH_story.html.

[419] Kelly, "Investigating in a Centralized Cybersecurity Infrastructure: Why 'Hacktivism' can and Should Influence Cybersecurity Reform," 1707.

common cyber-crime.[420] This is the most common approach in construction of discourse condemning *hacktivists* as a worst group than a group conducting *cyber-crime*, while these two groups should be understood as completely different.

In this moment we can observe an idealist movement helping citizens in their privacy and security, which is fighting for good intention to emancipate the individual; at least *good intentions* in their moral perspective. At the same time the same technologies are helping to create unbeatable hydra of transnational crime. The arguments of crypto-anarchists that the revolution will bring ultimate liberty to everyone is of course a double-edged sword and the usage of the technologies by ultra-libertarians in their business interests would serve as an example. However, the longer consequences of cyberspace and other public services privatization in the name of libertarian ideology is not usually understood as wrong by the left-side of the community, the crypto-anarchists. They understand market as an independent self-organizing organism; thus natural as nature.

Predict, whether encryption technologies can make world more secure is not clear. The discursive practices of national security are in the case of cyber-crime based on debatable financial evidence. Additionally, the term *hacktivist* is by the national security community merged with *cyber-crime* despite the fact that crime cartels do not have political intentions and can be easily distinguished. Being a victim of ransomware would probably raise more attention to the individual citizen rather than a situation in which law enforcement agency acts against a group that defaced a webpage to demonstrate different political opinion.

The following table shows a list of selected known hacker groups and their probable objectives based on actions taken. Table should serve as a depiction of wide varieties of motives that drive these people do illicit activities online. It is understandable that names have usually groups with objectives in hacktivism rather than in transnational crime; the same applies on espionage groups, which might be related to national intelligence bodies, but received a name from global cyber security companies such as Kaspersky Lab. In that perspective, the table should be understood as a limited insight to

[420] Verizon, *2012 Data Breach Investigations Report* (Verizon, 2012), http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.

the world of hacking groups that should serve as a window into what is going on in cyber-space in this matter.

GROUP NAME	OPERATIONAL	SHAPE	OBJECTIVES	ACTIONS	TARGETS	RESULT OF ACTIONS
414s[421]	1980 – 1983	a group of friends	to show their capabilities; script kiddies	hack of industrial systems by choosing default passwords	state industrial installations	celebrities; raised concerns about industrial security, first cyber-crime bills in US
Anonymous[422]	since 2003	*"a very loose and decentralized command structure that operates on ideas rather than directives"*	hacktivism; public protests; sometimes disorganized	DDoS attacks, spread of intellectual property	governments, churches, corporations, Islamic State	TIME: Between 100 most influential people in the world. STATES: Cyber-terrorists
CyberVor[423]	(?) – 2014 – (?)	probably an organized Russian group	unknown	~1.2 billion stolen credentials	about 420.000 websites	US firm Hold Security made money on disclosing who was targeted
Equation Group[424]	since 2001	probably an offensive wing of US National Security Agency	industrial espionage (similar skills as Stuxnet)	*"most advanced industrial espionage group in the world"* (Kaspersky Lab)	500 malware infections by the group's tools in at least 42 countries	suspicion that national intelligence is run by a secretive private hacking group
Hacking Team[425]	since 2003	Italian private company with offices in Annapolis, Washington DC or Singapore	profit from offensive and surveillance capabilities sold to governments	skype taping, deciphering, remote mics and other malware installations	citizens of non-democratic governments	a proof that both law enforcement and intelligence agencies buy from private hacking groups

[421] Philip Elmer-Dewitt, "Computers: The 414 Gang Strikes Again," *TIME*, August 29, 1983, http://content.time.com/time/magazine/article/0,9171,949797,00.html.

[422] Kelly, "Investigating in a Centralized Cybersecurity Infrastructure: Why 'Hacktivism' can and Should Influence Cybersecurity Reform."

[423] Gail Sullivan, "Russian Hackers Steal More than 1 Billion Passwords. Security Firm Seizes Opportunity," *The Washington Post*, August 6, 2014, https://www.washingtonpost.com/news/morning-mix/wp/2014/08/06/russian-hackers-steal-a-billion-passwords-security-firm-seizes-opportunity/.

[424] Kaspersky Lab, "Equation Group : Questions and Answers," 2015, http://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf.

[425] Angus Batey, "The Spies behind Your Screen," *The Telegraph*, November 24, 2011, http://www.telegraph.co.uk/technology/8899353/The-spies-behind-your-screen.html.

Level Seven[426]	1994 – 2000	an organized group, dispersed after FBI raid against the leader	referring to Dante Alighieri novel The Inferno, objectives symbolical	about 60 breaches into in 1999	banks, US federal institutions (embassy in China) or NASA	bridging simple hacking to systems into hacktivism
LulzSec[427]	2011 – ~2014	7 notorious hackers; nicknames are known	no financial profit, idea to make fun and cause mayhem; a bit of political motives	a lot; defacing webpages with messages	PBS, CIA, FOX, SONY, NINTENDO, a row of games, NATO, US SENATE…	first notorious global coordinated raid of corporations and law enforcement
Mazafaka[428]	~2011 – ~2015	decentralized forum of hackers	profit	spread of source code Zeus[429]	hundreds of banks worldwide and security company (RSA)	law enforcement raid against vast amount of decentralized people
Syrian Electronic Army[430]	since 2011	government loyal hacking group	political, support of Bashar al-Assad	spamming, website defacement, malware, phishing, DDoS	opposition, western news, human rights groups	a clear example of political supportive actions

Table 3 - Selected hacking groups.[431]

Groups vary from teenage activist, script kiddies trying to hack industrial systems just to show the possibility, through profit oriented pure cyber bank frauds organized in transnational decentralized gangs or politically oriented actions of hacktivists, or politically supportive groups of particular leader as in the case of Bashar al-Assad. Understandable burden of some hacktivist groups is in their decentralization; one wing might be willing to attack and deface a website to demonstrate a particular political position, whereas the other might have quite the opposite position. This problem usually applies to Anonymous as well. It is an understandable burden of decentralized groups. However, when these groups are decentralized and spreading open source code of

[426] Dorothy E. Denning, "Hacktivism: An Emerging Threat to Diplomacy," *Foreign Service Journal* 77, no. September (2000): 43–49.

[427] Fox News, "A Brief History of the LulzSec Hackers," June 21, 2011, http://www.foxnews.com/tech/2011/06/21/brief-history-lulzsec-hackers.html.

[428] Chris Mark, "Case Study: The Compromise of RSA Security and the Rise of Cyber-Espionage," *PoliceOne*, July 22, 2012, http://www.policeone.com/police-products/communications/articles/5827608-Case-study-The-compromise-of-RSA-Security-and-the-rise-of-cyber-espionage/.

[429] Julie Conroy, *Citadel and Gozi and Zeus, Oh My!* (AITE group, 2013), http://www.emc.com/collateral/white-papers/citadel-gozi-zeus-oh-my-wp.pdf.

[430] Jordan Robertson, "Three Things You Should Know About the Syrian Electronic Army," *Bloomberg*, March 24, 2014, http://www.bloomberg.com/news/articles/2014-03-24/three-things-you-should-know-about-the-syrian-electronic-army.

[431] Data are based on open-source data from various sources on internet.

software such as Zeus with guides how to use it,[432] the impact on online security of end-users' accounts is massive.[433] Especially when it comes to this particular code, which can finally be part of a foreign intelligence operation[434] to serve other than cyber-crime purposes. The genius in Zeus code is its spread into the open source community, which gave it an advantage from the others as it had been developed freely by the community. The ability by law enforcement to stop bank frauds based on Zeus and thus conducted by a software that is installed in the browser of a user was close to zero. Tens of thousands different compilations emerged on internet.

LulzSec was serious enemy to a row of international corporations such as SONY, but also to intelligence agencies such as CIA. In that perspective, their non-profit but politically oriented intentions were addressed as a national security issue by the intelligence agency and put side by side with others who were clearly profit oriented. Both groups are discursively depicted as cyber-crime oriented and approached in that way with no significant distinctions. It is hard to make a distinction when one hacker conducts an operation on behalf of a name such as Anonymous, but violates the very principles of that group. This post-modern fluid reality around is consequently fueled by false positives of attacks against critical infrastructure that drive the discourse of catastrophic future.

[432] Unknown, "User Guide for Zeus Malware," *Pastehtml*, accessed April 12, 2016, http://pastehtml.com/view/1ego60e.html.

[433] BBC News, "More than 100 Arrests, as FBI Uncovers Cyber Crime Ring," *BBC*, October 2, 2010, http://www.bbc.co.uk/news/world-us-canada-11457611.

[434] Thomas Fox-Brewster, "FBI 'Most Wanted' Cybercrime Kingpin Linked To Russian Espionage On US Government," *Forbes2*, August 5, 2015, http://www.forbes.com/sites/thomasbrewster/2015/08/05/gameover-zeus-surveillance-links/.

5. FORMING THE THREAT ON UNCERTAINTY POSED BY TECHNO-GEEKS

"To be free it is not enough to beat the system, one must beat the system every day."

— Anonymous (the movement, undated) —

When a group is driven by profit, it is a case for law enforcement. Groups are global, law enforcement agencies are not. As Heather Brooke puts it: *"The hacker community may be small, but it possesses the skills that are driving the global economies of the future."*[435] The hacker community is at least approached as mysteriously powerful with bright future. You kill one head, and two more grows on that hydra. Sometimes the imaginative national security discourse is reaching an extent that might either cause panic or fascination: *"Cyber hackers are GREATER threat to UK security than nuclear weapons"* which is a title of an article citing *expert on cyber terror.*[436] Hackers and their special capabilities are causing extreme fear based on uncertainty what everything else these *lords of cyberspace* can do. As attacks conducted by a state cannot be easily attributable to the particular state, it is understandable that *hackers* are responsible for all the national security concerns emanating from cyberspace. This logical reasoning is what creates the Foucauldian *field of concomitance*, as we convince ourselves about unimaginable skills of enemies we marked as enemies.

A map created by the National Security Agency reveals about 600 attacks on corporate, private or governmental targets[437] that had been victims of *Chinese Cyber Espionage*. Despite the huge arguments attributing industrial intelligence to China,[438] one may raise an objection that the attribution of these attacks to China – because they are emanating from the Chinese territory – is not fair as a country consisting of 1,3 billion people simply can house enough profit oriented hackers working for private companies,

[435] Heather Brooke, "Inside the Secret World of Hackers," *The Guardian*, August 24, 2011, https://www.theguardian.com/technology/2011/aug/24/inside-secret-world-of-hackers.

[436] James Fielding, "EXCLUSIVE: Cyber Hackers Are GREATER Threat to UK Security than Nuclear Weapons," *Express*, October 25, 2015, http://www.express.co.uk/news/uk/614417/cybercrime-UK-talktalk-hack-security-computer-systems-online-safe.

[437] Robert Windrem, "Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets," *NBC News*, July 30, 2015, http://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211.

[438] William C. Hannas James Mulvenon Anna B. Puglisi, *Chinese Industrial Espionage* (Routledge, 2013).

whose principal objective is profit and nothing more.[439] When it comes to interstate cyber espionage, great example of that simplified threat depiction is the Keith Alexander's famous claim that cyber espionage is the *"greatest transfer of wealth in history",* while it is not difficult to remember decades long US policy about the lawful technology transfer to poor countries, especially to China;[440] or Snowden revelations, which depict China as a small player to US intelligence efforts, the "nationalization" of what can be easily private-to-private espionage is blossoming. Reaction on private-to-private espionage, on can insist to call it transnational corporate crime, in shape of sanctions against a state can finally bring the whole nations on a dangerously thin ice. These sanctions might in contrary cause more harm to both economies, international stability and thus real espionage campaigns than ever.[441] Especially when intelligence in order to strengthen national security order services from third parties that participate on massive mammoth surveillance programs as PRISM; post-modern fluid dystopian chaos emerges.

The combination of objectives depicted in The Crypto-Anarchist Manifesto[442] and the sense of the unmanageability of the alleged power of hackers helps draw a pessimistic perspective of possible future actions with limited options how to cope with them.[443] That is nothing new in cyberspace; however, the fact that cyberspace is socially constructed space in its fluid shape does not help policy makers approach the problem with a solid perspective. The fluid flowing through fingers as any policy approach simply cannot cover each specificity of every single cyber incident combined with constantly deepening technological complexity tend to develop an image of environment that is not under control. The non-governable technological development, which is moving forward out of control will have implications that no-one is even able to imagine. However, everybody is able to draw a solid picture of the threat rhetorically.[444] The Crypto-Anarchist

[439] Greg Austin, "What the US Gets Wrong About Chinese Cyberespionage," *The Diplomat*, May 22, 2015, http://thediplomat.com/2015/05/what-the-us-gets-wrong-about-chinese-cyberespionage/.

[440] Ibid.

[441] Ryan Pickrell, "A Dangerous Game: Responding to Chinese Cyber Activities," *The Diplomat*, September 29, 2015, http://thediplomat.com/2015/09/a-dangerous-game-responding-to-chinese-cyber-activities/.

[442] May, "The Crypto Anarchist Manifesto."

[443] Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (Princenton: Princeton University Press, 1984).

[444] Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse."

Manifesto[445] drives people in developing technologies that are hard to control by governments and governments draw dystopian images of futures as they are not in charge of such development. One may raise a question whether this techno-optimism behind the technology combined with techno-opposition to everything that represent *the establishment* would have been emerged without political statements such as the Manifesto. Additionally, the opposite perspective from *the establishment* might be similar. One may raise a questions whether without the Manifesto states would be so afraid as they are or whether the threat politics help them constitute their state-related power on exclusion caused by fear of unknown[446] and a depiction of deviation.[447] The definition of deviation helps to define the normal state and prepare procedures to react to preserve that normalized state in a normalized way as Aradau and Munster propose.[448] In that moment, when the desirable policy would be to define the state of the technology society is dependent on, national security authorities are harshly conducting super surveillance program to catch each anomaly of the deviance from the enormous amount of data that leads to introduction of fantastical concept of *superhuman*[449] above everybody. The policy against catastrophe constructs the catastrophe itself.

The moments that might play a role on deepening the threat perspective on the side of states are certainly not only related to isolated events such as biggest bank frauds in the history ranging to $1 billion (sub-titled *hunt for the hackers).*[450] Techno-geeks are making political moves that help institutionalization of cyberspace in uncertain way as they are by principle decentralized; they produce more unknowns in an unknown environment. One such example, adding to the Manifesto, with debatable policy intentions, is A Declaration of the Independence of Cyberspace written in 1996 (emphasis in italic by me):[451]

[445] May, "The Crypto Anarchist Manifesto."
[446] Wodak, *The Politics of Fear*.
[447] Foucault, *Discipline & Punish: The Birth of the Prison*.
[448] Aradau and Munster, *Politics of Catastrophe*.
[449] Cliff Weathers, "NSA's Massive Cyber-Spying Efforts Called 'Superhuman,'" *AlterNet*, February 17, 2015, http://www.alternet.org/civil-liberties/nsas-superhuman-cybersurveillance-network-exposed.
[450] Unauthored, "Biggest Cybertheft in History Hits Banks," *WND*, February 16, 2015, http://www.wnd.com/2015/02/biggest-cyber-theft-in-history-hits-banks/.
[451] John Perry Barlow, "A Declaration of the Independence of Cyberspace" (Davos, Switzerland: Electronic Frontier Foundation, 1996), https://www.eff.org/cyberspace-independence.

A DECLARATION OF THE INDEPENDENCE OF CYBERSPACE

by John Perry Barlow

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.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. *Cyberspace does not lie within your borders.* Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. 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.

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.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.

Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.

In the United States, you have today created a law, the Telecommunications Reform Act, which repudiates your own Constitution and insults the dreams of Jefferson, Washington, Mill, Madison, DeToqueville, and Brandeis. These dreams must now be born anew in us.

You are terrified of your own children, since they are natives in a world where you will always be immigrants. Because you fear them, you entrust your bureaucracies with the parental responsibilities you are too cowardly to confront yourselves. In our world, all the sentiments and expressions of humanity, from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits. We cannot separate the air that chokes from the air upon which wings beat.

In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. These may keep out the contagion for a small time, but they will not work in a world that will soon be blanketed in bit- bearing media.

Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.

These *increasingly hostile and colonial measures* place us in the same position as those previous lovers of *freedom and self-determination* who had to reject the *authorities of distant, uninformed powers*. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.

We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.

Davos, Switzerland February 8, 1996

This declaration sparked a row of reactions. The critical camp tends to be critical on its utopian shape; it questions achievability of the depicted utopian world as a world that is limited to its discursive imaginative reality of metaphors, but with no power to materialize; an impossible future.[452] Morrison is convinced that the declaration continues to be reduced to popular journalism[453] rather than to spark a revolution. However, a good point might be that such a radical text is written to motivate people to struggle for the utopian future; to achieve a portion of its goodness. As I point out in the theoretical part, metaphors are not to be considered as an isolated *word* without a potency to materialize in reality; especially when it comes to the history of internet, metaphors played a significant role in the famous Dot Com Bubble[454] which motivated thousands of investors to fund debatable projects, which collapsed. Their conviction was based on served metaphors; such an empirical evidence at the dawn of cyberspace show us how metaphors can serve in the interest of those who deploy them.[455] Imaginations of future help people focus on their efforts. When one is driven by a vision of space exploration, a construction of something physical with high-end engineering is needed; when one is driven by a vision of liberal cyberspace and given by ideas how to reach it, despite the debatable result, the efforts are driven by these imaginations and soft software engineering skills. While cyber-space is built through its social construction, through our practices and routines how we use it,[456] and through metaphorical description of its functions, the threats to national security are driven by the same metaphorical imagination as will be shown in the chapter concerning nation-defense discourse. The existence of the document itself is enough to materialize the policy in action and legitimize the consequences in political life. If properly proliferated on specific places,

[452] Morrison, "An Impossible Future: John Perry Barlow's 'Declaration of the Independence of Cyberspace.'"
[453] Ibid., 54.
[454] Alexander P Ljungqvist and William J. Jr. Wilhelm, "IPO Pricing in the Dot-Com Bubble," *The Journal of Finance* LVIII, no. 2 (2002): 723–52.
[455] Sally Wyatt, "Danger! Metaphors at Work in Economics, Geophysiology, and the Internet," *Science, Technology, & Human Values* 29, no. 2 (2004): 242–61, doi:10.1177/0162243903261947.
[456] Schmidt, "A Sociological Approach to Cyberspace Conceptualization and Implications for International Security."

times and identities, such as Parallel Polis, Bitcoin meetup or DEF CON congress, the discourse can materialize and become a norm of the related community.

The working critic of the declaration lies in its simulation of crisis. Its visible intentional division of outer world with those who are called for action. The depiction of the evil in *weary giants of flesh and steel* and the divine *home of Mind* (Bitcoin meetup named *Hivemind)* is a binary opposition visible throughout the whole declaration: *our world* vs. *your world* or the intergeneration of a conflict, which is more comprehensible to young generations willing to rebel. In particular *children are natives*, while the others are *immigrants,* authorities are immigrants. The evolution of technology and related evolution of linked culture is by Baudrillard understood as an eternal progress, while the players of this evolution tend to create an irreconcilable conflict; in Baudrillard words a simulation.[457] He described this process of denunciation of scandals on the case Watergate[458] during which the investigative journalists are doing in fact the same as they are criticizing – wiretapping. While the national security discourse is focused on what is threatening us by pointing on massive cyber-crime or cyber-espionage operations, the opposite side quite perfectly in contrary see the threat in massive surveillance unveiled by Edward Snowden. Both can be understood as an extreme position of a natural societal evolution that will significantly alter the way how we practice democracy. To make the argument also against Snowden, I would name for example Edward Lucas. His piece about Snowden goes exactly the opposite direction than Bauman as he depicts the whistleblower as the biggest disaster to national security and in the end into a general belief to a liberal democratic order.[459] Both sides of the Snowden operation or Snowden revelations caused damage to the liberal democracy credibility. The fact that intelligence agencies have conducted such operation, did not react on Snowden objections before the revelations and then, finally, the revelations itself. It is hard to recognize which side has a higher moral integrity when both caused damage to western-type of liberal democracy.

[457] Baudrillard, *Simulations*.
[458] J Baudrillard and M Poster, *Selected Writings* (Stanford University Press, 2001), 172–4.
[459] Lucas, *The Snowden Operation*.

Dahlberg argues that other means of electronic communication were able to evolve the democratic environment by spreading the information and that there is no reason why the cyberspace might be excluded from this process, whilst we still do not know into which model of democracy it can lead.[460] While some critics found it naïve and point on an exactly opposite direction already in 2003; a direction towards society massively controlled by networked surveillance system with implanted chips from milk boxes to humans,[461] which was kind of appropriate prediction concerning current state of the affairs. The reaction of crypto-anarchist is not indistinctive as was shown on proliferation of peer-to-peer encryption. One may argue that such critical approach is based on the same binary perspective as in the case of Baudrillard's observations. It would be true; it is hard to be oriented in such a post-modern liquid modernity as Bauman continuously argue.[462]

The Declaration has a lot of antagonistic propositions. For example, the renouncing the government in cyberspace, while calling for our own social contract. In that perspective, it is not hard to accept the idea of its inapplicability,[463] but also it is quite brave to denounce it at all. Its political implications are visible throughout the core ideas in decentralized approach of various hacking groups; Anonymous in particular[464] and the idea that such hydra can be slain by law enforcement only supports its incapability to secure people in cyberspace from regular cyber theft such as ransomware. Recent example when a single unknown programmer was able to crack the Petya ransomware[465] by his/her hacking skills shows the power of decentralized community. The tendency of law enforcement to fight these communities without distinction between hacker's intentions would serve as an example how slaying the hydra might also be a double-edge sword. The decentralized community, *the Mind*, is able to solve these problems usually quicker, effectively and without state intervention. Such recognition motivates them and convinces them that their efforts make sense.

[460] Lincoln Dahlberg, "Democracy via Cyberspace," *New Media & Society* 3, no. 2 (2001): 157–77, doi:10.1177/14614440122226038.

[461] The~Economist, "Digital Dilemmas," January 23, 2003, http://www.economist.com/node/1534303.

[462] Bauman, *Liquid Modernity*.

[463] Morrison, "An Impossible Future: John Perry Barlow's 'Declaration of the Independence of Cyberspace.'"

[464] Halpin, "The Philosophy of Anonymous: Ontological Politics without Identity."

[465] "Petya Ransomware Encryption System Cracked," *BBC News*, April 11, 2016, http://www.bbc.com/news/technology-36014810.

6. CONCLUSION

We should start understanding geeks, crypto-anarchists and cyber criminals as distinct groups. While one may be willing to break systems for fun, the others call for emancipation from corrupted governments and develop online security related technologies in order to support privacy, security and freedom online; the criminals are interested in development of global cyber-crime cartels. Crypto anarchists in the role of hacktivists may have strong ideologist background supporting *political liberty* of doing whatsoever in cyberspace as their conviction lies on an initial question why states need to control what do we do in cyberspace; especially after such denouncing revelations by Edward Snowden. Authorities in the contrary discursively construct every uncontrollable activity in cyberspace as a part of global cyber-crime super cartel that is used to vindicate moves of total surveillance while the law enforcement agencies are incapable to solve general crimes such as ransomware.

Nation states fuel process of denationalization of security by adding third party agents into a massive global surveillance program, which detaches intelligence from national security boundaries, drives the crypto-anarchist movement forward, fulfilling their dream of legitimate decentralized power and tacitly includes global corporations with profit oriented interests. As an outcome, nation states leave the principles of securing liberal democratic values in order to secure citizens from imaginative and statistically extremely low probable cyber terrorism. Inclusion of corporations driven by profit and rules of the market into intelligence collection denies liberal democratic values. The construction of the threat in hacktivists does not produce more security, it produces more insecurity. It seems that authorities are mixing geeks with unreachable skills, crypto-anarchists passionate in their liberation and global cyber crime cartels into the same community. Some examples have been made such as the one with Keith Alexander's reaction to the announcement of anonymous. The drawn catastrophic imaginations in minds of people having decision making power is what causes the construction of such insecurities in the continuous demonstrative reasoning in their isolated world Foucault calls *field of presence* that is detached from the socio cultural worlds where the addressed actors grow. The move of Keith Alexander is the typical example how the *field of presence*

he lives in shifts into the *field of concomitance* where analogical confirmations took place. If Anonymous say there are going to shutdown internet, the answer of experts how impossible it is does not matter. The statement by the authority responsible to answer newly emerging threat is what seems to be more credible, because he speaks on behalf of that authority. It is based on presumptive experience rather than on empirical evidence. However, as Gartzke argued,[466] the rising number of events will create more tangible experience that will finally mitigate such overemphasized imaginations.

The current inability of states to tackle with growing global cyber-crime supports ideas of transnational cooperation to the extent of violating certain nation state principles, e.g. local law regimes; paradoxically using arguments with global impact as in the case of Megaupload in New Zealand. That supra-nationalizing of law enforcement might lead to institutionalization of transnational law enforcement bodies and to a world state authority. EUROPOL occasionally calls for more powers as any other institution. However, as seen in the previous chapter, the ideas of total independent networks on states are not just a painting on the walls of science fiction artists, but a real ideology that drives a significant portion of technologically enabled people toward decentralized politically driven structures capable to deal with online security better than nation states. *Currently still in perspective of knowledge production, not body augmentation, yet.*

Governments especially of western-type liberal democracies should deepen their active cooperation with crypto-anarchist movements and support them in development of more secure technologies. Governments are aware of this need; however, the currently visible cooperation is for example the mentioned DARPA intentions to give $3 million of dollars to the hacker group that develop the most effective artificial intelligence capable to patch exploits autonomously. Such an idea only fulfills the darkest dystopian nightmares we have been able to imagine. The cooperation between governments and crypto-anarchists would not be an easy task as it is against their ideology; however, if successful on particular projects, it can help make the governance of technology development more steerable.

[466] Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth."

III.

NATIONAL LEADERS AND THE (UN)CERTAINTY OF THE FUTURE OF NATIONAL SECURITY

[An] invasion force … of digital signals marched across the border into Estonia… [467]

467 Robin Bloor, Large-Scale DOS Attack Menace Continues to Grow, The register (June 11, 2007), http://www.theregister.co.uk/2007/06/11/dos_security_cyberwarfare/

1. INTRODUCTION TO THE MAZE OF CONCEPTS AND MEANINGS

The area where cyber meets national security is probably the most one discussed today. When banks losing money in credit cards frauds and facing DDoS attacks on a daily basis and biggest corporations experience credit card numbers leaks of hundreds of millions of users from their databases, it seems legitimate to ask when the national security will be threatened by hackers. The first problematic question is where crime ends and national security concern begins. Usually this question is answered by adding state as an actor with assumption that the state is a special actor. It is special at least in the way what language it uses to secure its interests – it is a national security concern. However, how can we deal with a situation where we expect security to be provided by a state? When it comes to cyber security against cyber crime frauds, we saw in the previous chapter that decentralized networks or particular non-state actors are much more effective in dealing with these troubles. Where personal responsibility regarding my credit card number as a client of a bank ends and where responsibility of the bank to take care of security of their customers begins? The same can be easily applied to national security. We expect from a state to take responsibility over general security of our daily life, we expect electricity to be delivered, that transportation works without traffic jams, prices are stable, other states do not wage wars against us etc. However, do we expect to keep electricity running by military units guarding electric wires from our homes to servers' switches? It is really cyber that threatens our lives to be the first threat in NATO strategy?[468] It is a deliberately suggestive question as the following chapter deals with similar suggestive discourse of civil defense of "national" cyberspace.

There are two terms, which are intermingled or used in confusion when authors talk about cyber related threats to national security. *Cyber war* and *cyber warfare*.[469] The former usually deals with interstate conflict on a general level using cyber means, while the latter might sometimes thoroughly discuss mean of waging a cyber war. According to NATO CCD COE online dictionary, which collects different definitions from sources such

[468] NATO, "Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization" (Lisbon, 2010), http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf.

[469] I would like to specifically thank here to Alex Crowther from National Defense University for our inspirational debate in Baku, Azerbaijan where we both presented our thoughts regarding cyber security on January 2016 at NISA Winter Session.

as national strategies, other dictionaries or academic literature, there is no clear distinction and the institution does not provide its own definition.[470] Moreover, it is not hard to find academic articles, which use both terms with no regard to their different meanings. For example, a book called Cyber Warfare: A multidisciplinary analysis[471] deals with both problems (if we take the above mentioned possible distinction) and deliberately use the word *warfare* while referencing to articles criticizing the exaggeration of possible *cyber war* by pointing on a specific kind of conflict in future, in particular espionage, sabotage, and subversion. Especially the Rid's article called Cyber War Will Not Come and subsequent book discussed at the beginning in the literature review do not deny the capabilities or means of conducting an attack using cyber means or using cyberspace,[472] they conversely tend to put attention on means of warfare by addressing what is in their perspective the real problem we face. However, James Green, the author of introduction to the mentioned book on Cyber Warfare[473] cites Rid's thoughts as *"views of a minority of commentators who have downplayed the threat."* The one who has read Rid's thoughts carefully would never said that Rid *downplayed the threat.* He tried to seriously analyze the exaggerated term, which is in policy analytically flattened into undisputable threat while cyber-attack causes serious trouble somewhere else by other means. Rid falls into the group of scholars who through reconceptualization of a settled concept rises questions that critically approach the newness of the discussed threat.

The problem of this different meanings does not end easily as some authors proposed to make distinction between *cyber-attack* and *cybered attack*.[474] Demchak proposes to distinguish between attack that emanate in cyberspace and ends in cyberspace (cyber-attack) and attack that emanate in cyberspace and ends in physical space (cybered attack). However, I would guess that this distinction would not be a favorite one for policy makers that need to apply humanitarian international law on

[470] Dictionary of NATO CCD COE can be found at https://ccdcoe.org/cyber-definitions.html
[471] James A. Green, *Cyber Warfare* (Abingdon, UK: Routledge, 2015).
[472] Rid, "Cyber War Will Not Take Place," April 20, 2012.
[473] Green, *Cyber Warfare*.
[474] Demchak, Chris. Cybered Conflict, Cyber Power, and Security Resilience as Strategy In D.S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Georgetown University Press, 2012), http://books.google.cz/books?id=v576FVMpdcAC.

cyber-attack without distinction to move the meaning and reflection of the term *use of force* further by denouncing a need of physical destruction as I will analyze later.

Cyber war is usually used in exaggerated articles full of threat imaginations, which aim to make short bridges between conventional war and hypothetical cyber war or builds new images of possible future war on which we need to be prepared. Preparation means real activities in order to face imaginations. On the other hand, *cyber warfare* supposes to be used to describe measures, practices, methods or advancement in capabilities concerning using ICT to conduct an attack against an adversary, usually a state if it is used in relation to interstate conflict. There is no doubt that a strong state can possess critical knowledge and capabilities to conduct a specific operation leading to identification of a vulnerability on a critical system, exploit it and even physically destroy it. Stuxnet event[475] would serve as an example of such capabilities demonstration. However, this chapter deals with discursive formation of *cyber war* rather than discussion of *cyber warfare* or dealing with the described confusion scholars like to multiply. Concerns behind the *radical uncertainty* what might happen is what matters in this discursive analysis. Making such distinction helps me avoid criticism that I am denying existence of tools to conduct a kind of attack which can be credibly called as an exercise of tools, measures, practices or methods related to cyber warfare. That brings us to the exact moment where Rid criticize the usage of concept *cyber war*, as this is a new kind of activity challenging national security which is not similar or easily comparable to conventional war, but requires appropriate conceptualization to assess what all possible strategic advantages can be reached by cyber warfare means.

[475] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival (00396338)* 53 (2011): 23–40, doi:10.1080/00396338.2011.555586.

2. THE BIRTH OF CYBER WAR

2.1. Chaos and uncertainty trigger the unease

"Cyber war is coming" was mentioned in the title of an article published in Comparative Strategy in 1993.[476] Two decades later we can hear about cyber military commands around the world: *"these military and intelligence organizations are preparing the cyber battlefield with things called 'logic bombs' and 'trapdoors,' placing virtual explosives in other countries in peacetime",* a citation from a famous book called "Cyber War : The Next Threat to National Security and What to Do About It" written by Robert Knake and Richard Clark; the latter was a cyber expert in the White House between 2001 and 2003.[477] The citation is obviously built on imagination coming from the uncertainty of *geeks' capabilities* (referring to the definition of geek on the page 129) *as geek is "someone with ridiculous skills on a computer/phone/iPod/other electronical device and scares us mere earthlings. They have a habit of breaking these after stretching them beyond their ability for normal usage. They also sometimes know more about a product than the producer."*[478]

Famously, authors developed a scenario what might happen with these *logic bombs* if we do not commence ourselves to understand this threat and do not respond; usually in advance, preventively. The scenario they developed contains ideas such as derailment of metro, aircraft collisions, nuclear power plants shutdown or explosions in chemical and oil refineries. The relation to Leon Panetta's speech is self-evident (I analyzed it on the page 87). To make this scenario more alarming authors intentionally use words such as *cyber warriors* meaning hackers or *cyber battlespace* meaning Internet or other communication networks or *battle corridors* meaning domain name system translating IP addresses in numbers into website domains. This book has been seriously

[476] John Arquilla and David Ronfeldt, "Cyberwar Is Coming!," *Comparative Strategy* 12, no. 2 (1993): 141–65, http://www.tandfonline.com/doi/abs/10.1080/01495939308402915.

[477] Clarke and Knake, *Cyber War: The Next Threat to National Security an*.

[478] Iamme986, "Tech Geek," *Urban Dictionary*, 2010, http://www.urbandictionary.com/define.php?term=tech+geek.

criticized by scholars being too suggestive[479] and ICT experts[480] to be extremely fictitious or lacking footnotes or literature to find out on what evidence their statements are based.[481] However, the book and its imaginations repeats and reconstitute the *church of knowledge* within particular security professionals; it starts with *field of presence* – the military doctrine and transforms into the *field of concomitance* by the demonstrative reasoning and analogical confirmations. The book is familiar to any cyber security expert as it is one of the first books related to cyber security as a national security agenda in post 9/11 world, which put significantly bigger attention to our security in comparison to post-revolutionary 90s.

Clark and Knake claim that the blackout in 2003 was caused by cyber-attack, because former CIA agent Tom Donahue was authorized to tell the public in 2007.[482] This claim is probably made on a newspaper article in The Washington Post from 19th January 2008[483] where authors mentioned that Donahue told this claim in front of 300 U.S. and international security officials, but cannot say any other details. The whole event of the blackout was precisely analyzed much earlier[484] by various experts of U.S. Department of Energy and Ministry of Natural Resources with a list of other national bodies concluding that no cyber-attack happened, which is supported by the timeline of series of events that were not caused by a human, but a system failure.[485] Telling 300 security officials that something happened according to the knowledge of intelligence community was clearly in conflict with this report; however, this event is what transforms the *field of presence*, the well-founded reasoning, the necessary presupposition of an assured cyber war emergence into the *field of concomitance* based on analogical confirmations. Three hundred high ranked people left the room convinced that the intelligence officer is not

[479] Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse."

[480] Ryan Singel, "Richard Clarke's Cyberwar: File Under Fiction," *Wired.com*, 2013, http://www.wired.com/2010/04/cyberwar-richard-clarke/.

[481] David Vanca, "Richard A. Clarke and Robert K. Knake's 'Cyber War: The Next Threat to National Security and What to Do About It,'" 2013, http://georgetownsecuritystudiesreview.org/2013/12/10/richard-a-clarke-and-robert-k-knakes-cyber-war-the-next-threat-to-national-security-and-what-to-do-about-it-harper-collins-2010/.

[482] I was using epub version of the book without page numbers, but you can find it in 7th paragraph from the end of third Chapter.

[483] Ellen Nakashima and Steven Mufson, "Hackers Have Attacked Foreign Utilities, CIA Analyst Says," *The Washington Post*, January 19, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/01/18/AR2008011803277.html.

[484] Bob Liscouski and William J.S. Elliot, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," 2004, https://reports.energy.gov/BlackoutFinal-Web.pdf.

[485] Ibid., 132.

spreading an unconfirmed disinformation. Authority works in these situations; no facts are needed, as it is in the post-factual world; discourse matters.

Moreover, the book completely avoids the report, but focuses on what the intelligence officer said. Even the authors of the book continue the discourse in the cloud of the field of concomitance that is based on beliefs and imaginations, which have never been confirmed. Additionally, the authors are pointing to a virus called Slammer worm. According to Clarke and Knake, this virus slowed down SCADA systems in power grid causing the blackout. In fact, Slammer worm was an experiment whether a virus can be written so short that it fits into one data packet; concretely 376 bytes and the objective of the virus was clear, to show how quickly a virus can spread and it spread to dozens of millions of servers in 30 minutes throughout the world.[486] Clarke and Knake connects Slammer worm with power probably thanks to a case of Ohio nuclear power plant, where Slammer worm crashed the cooling circuit. However, that event happened due to absolute security negligence by administrators who connected a telephone line from their offices to the power plant just because they needed comfortable access to the system from office during a maintenance period.[487] Poulsten, who analyzed the Slammer worm in 2003, also wrote an article in 2008 to directly refute ideas that Slammer worm caused 2003 blackout calling the ongoing events *cyber hysteria.*[488] Poulsten is reacting to an article citing particular intelligence officers on National Journal, the article is deleted and there is no one article on the server mentioning Slammer Worm in 2016. The connection with 2003 blackout is just Clarke's and Knake's imagination. However, an imagination coming from a former White House cyber expert must have serious policy impacts – it builds undisputable church of knowledge that spread into major offices in Washington DC. The book has almost thousand citations on google scholar and can be found in numerous libraries. This book has created an unbeatable *church of knowledge* that

[486] David Moore et al., "Inside the Slammer Worm," *Security & Privacy, IEEE* 1, no. 4 (2003): 33–39.

[487] Kevin Poulsen, "Slammer Worm Crashed Ohio Nuke Plant Net • The Register," *Theregister.co.uk*, 2003, http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke/.

[488] Kevin Poulsen, "Did Hackers Cause the 2003 Northeast Blackout? Umm, No," *Wired.com*, 2008, https://www.wired.com/2008/05/did-hackers-cau/.

materialize into *norms* backed by *productive power* that is established to exercise this power.

The book is full of such warring and warning statements based on imagination rather than on undisputable evidence. This approach of writing is causing an *escalation of imagined danger* as Kaiser pertinently puts it.[489] This mentioned report on 2003 blackout written by international experts had existed at least 7 years before the Clarke's and Knake's book publication. In that perspective, move by Tom Donahue to leak classified information or to mention this suspicion in front of 300 hundred important people in decision making concerning US policy seems to be similar to the whole purpose of the book – to produce a suspicion under *radical uncertainty*, to produce false knowledge based on undisputable *church of* knowledge, to depict future possibilities rather than to discuss threats that have daily evidence. Repeating the language that is focused on low probability high impact events rather than acting against high probability low impact events, which is so hard to solve on a global scale as massive and numerous DDoS attacks. One report of widely recognized experts in the field with a row of evidence seemingly cannot stop spread of this alarming discourse, the book is well cited (about 648 according to Google Scholar on 23rd January 2016 and about 742 on 8th August 2016) and some authors use the book to argue that the military capability in cyberspace cannot be destroyed by arms control measures as it can only forbid certain acts.[490] Academics in political science seriously cite the Clarke's book – without footnotes and references – to support their argument in serious professional journals dealing with a problem of possible cascade effect in critical infrastructures: *"Cascading failure is seen as potentially catastrophic, extremely difficult to predict and increasingly likely to happen"* and the article begins with a reference to the Clarke's book.[491] The newly produced knowledge, despite its foundation on pure imagination, is actively reproducing itself and looks for confirmations in *correctable constructed analogies* that are based on fear and uncertainty.

[489] Kaiser, "The Birth of Cyberwar."

[490] Adam P Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (November 10, 2012): 401–28, doi:10.1080/01402390.2012.663252.

[491] MICHEL VAN EETEN et al., "The State and the Threat of Cascading Failure Across Critical Infrastructures: The Implications of Empirical Evidence From Media Incident Reports," *Public Administration* 89, no. 2 (2011): 381–400, doi:10.1111/j.1467-9299.2011.01926.x.

The current approach does not provide us with an option of normalized reaction as Aradau and Munster propose;[492] it only builds a huge imagination of doomed near future in the dystopian way where nobody is in control. It also legitimizes actions in creating cyber related capabilities that in the end lower the credibility in the liberal democratic state as we saw in the case of PRISM.

While this *cyber capability* is measured by imagined attacks, which were turned down by experts' reports, it certainly still plays a role in keeping us vigilant against incoming cyber war. These moments are what creates radical uncertainties in policy making. *"It may happen you should not deny it"* is what we usually hear at cyber security conferences. In the Czech Republic the Czech National Security Authority is given with the agenda to run national CERT at the National Cyber Security Center, in particular the director Dušan Navrátil constantly reiterate the discourse about DDoS attacks on Czech news in 2012 (last time heard on conference in Prague in 2015). In fact, nothing to national security happened that week, just a simple DDoS attack against websites of news and telecommunication companies, but a director of Czech NSA uses this event of simple DDoS attack on unprepared servers which were down for hours to demonstrate why the agenda is critical from the national security perspective. He calls this action as a proof of ongoing *cyber war*[493] while at the same time the director of Czech National Cyber Security Center openly and proudly shows the book signed by Clarke to demonstrate clear inspiration from world-class experts how to deal with it.[494] Risk cannot be calculated when one attack can cause blackout and according to Clarke and Knake a group of such attacks can *certainly* fulfill the scenario of total cyber Armageddon leaving us in the ash of cyber fallout. In the meanwhile, Clarke's and Knake's book use word "nuclear" 152 times, while it does not deal with anything related to nuclear. It just stresses what *might* happen if an attacker make a link to any nuclear facility as the Slammer Worm did, but it was not an intended attack as it did spread to dozens of millions servers and did so because of total negligence of security by the network administrators. Message delivered

[492] Aradau and Munster, *Politics of Catastrophe*.

[493] Cyber security conference on 28th May 2015 co-organized by Czech NSA and CEVRO Institut. Report in Czech language at http://www.cevroinstitut.cz/cs/akce/uspesna-konference-a-medialni-ohlasy-cyber-security-and-national-defense/

[494] Personal experience as an employee of Czech National Cyber Security Center in 2012-13.

by these two authors and others focused on alarming the public without providing appropriate evidence is clear.

2.2. Emerging truth

I have discussed some tricky moments in cyber discourse production above, which is certainly not complete, but the objective was to show how some experts deliberately spread imagined dangers to support the argument that national authorities must act. The logic of these efforts is to produce *new security related statements* such as cyber war, cyber battlefield, cyber warrior, logic bomb, cyber offense, cyber defense etc. to militarize the space for information exchange – cyberspace. The tricky part of the statements materialization is a finding that this discourse generally omits weaponization of information in sense of propaganda, which is visibly deconstructing liberal democracies after decades of stability. Despite the fact that this negligence is what Thomas Rid criticized on cyber war hysteria in his mentioned article Cyber War Will Not Come,[495] or what I criticized recently as well in perspective on incoming hybrid war[496] or as a negligence in power conceptualization in cyberspace exactly in relation to this one-sided militarization discourse of Clarke and his brotherhood,[497] which almost completely (a word "propaganda" show 6 times in the book in comparison to 152 occurrence of a word "nuclear") neglects the potential of propaganda.[498] The new truth is not produced on ongoing cyber-empowered troubles, but as several times stated above – on a projection of unease by escalation of imagined dangers through formulation of imaginative threats.

There are examples in literature of academic works that deliberately produce new knowledge by conceptualizing cyber war on examples of conventional war, on particular historical events to show how something *comparable* can happen in cyberspace – the analogical confirmation of fields of concomitance. These efforts clearly produce a new *field of concomitance* by so called proving of the applicability of conventional warfare perspectives to cyberspace[499] by applying particular analogies in the history (9/11, Cyber

[495] Rid, "Cyber War Will Not Take Place," April 20, 2012.
[496] Schmidt, "Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War."
[497] Schmidt, "Super-Empowering of Non-State Actors in Cyberspace."
[498] Pomerantsev and Weiss, "The Menace of Unreality : How the Kremlin Weaponizes Information , Culture and Money."
[499] Rattray and Healey, "Proceedings of a Workshop on Deterring CyberAttack."

Pearl Harbor, Battle of Britain…). These analogies – here – are not used in the genealogical repeatability of these *"truths"* in order to constitute them, nor they serve here as a discursive materialization as will be shown later in how they are used by political authorities consequently in time. These analogies serve to establish credible foundations for any further related security statements. A knife can be used as a tool in kitchen or as a weapon; the same probably applies to cyber tools, so we have to establish cooperative cyber security centers throughout the world. The emergence of such *fields of concomitance* is exactly what I understand as a preliminary step to *church of knowledge* where these truths cannot be beaten as they fit into the adopted logic carved in the locutory nexuses discussed everywhere.

Another example of adding to the process of *field of concomitance* building is a combination of cyber with some traditional academic disciplines and then the exercise how easily they can be applied on modelling cyber warfare despite the fact that some of them simply do not relate to the topic at all.[500] Chapter 11, Active Discovery of Hidden Profiles in Social Networks Using Malware, of the cited book is seriously, but interestingly geeky. It deals with a problem of terrorism cells communication using social networks. While the idea of implementing malware into social networks in order to unveil some hidden nodes seems to be a brilliant approach in social network analysis, it can be prevalently used by the intelligence community. The relation to cyber warfare remains questionable. Moreover, after reading some of the chapters, one may become aware of the fact that the authors of the literature repeat quickly. There are dozens of people which know each other in the world of cyber security and who are authors of the topic related to cyber warfare perspective in such writings.[501] Another Chapter from the same book starts as follows: *"Cyber-war is a growing form of threat to our society that involves multiple players executing simultaneously offensive and defensive operations"* and continues to name the list of important events to argue that war is shifting from

[500] Sushil Jajodia et al., *Cyber Warfare: Building the Scientific Foundation* (Springer, n.d.).

[501] Shakarian is author to at least two books called Cyber warfare. Deception techniques are written usually by Frank Stech from MITRE Corporation who I personally deeply respect, but it is hard to find a flow of new texts on cyber deception that are not somehow related to Frank's perspective.

conventional sphere to cyberspace[502] with no regard that stealing information can be hardly an act of war.

There is no way to argue, as Rid argued, that these actions are limited examples of sabotage and such a modelling of cyber war games would probably never meet next brilliant piece of code sneaking to another nuclear facility. It is a *church of knowledge* what we see growing. Questions are not welcomed.

2.3. National security becomes geeky and the establishment of new truth

Metaphors are used to understand abstract depictions in certain rules we already understand. However, metaphors have also one magic function – they can easily prove truth by making a statement in a rising concern of strange field of knowledge. Making metaphors in cyber security discourse with conventional war is what triggers concerns that possible cyber war delivers indisputably comparable serious destruction. Framing the insecurities in metaphorical structures[503] deepen the confidence in emerging *field of concomitance* as these frames resonate in discourse despite their beneficial role of better understanding of unknowns. Newly emerged knowledge structure with respected authorities in new cyber experts became a *church of knowledge*. The concern about cyber war described using metaphors of conventional war will certainly deliver the same concern not before but until we receive some empirical evidence. That is the Gartzke's argument;[504] but until then we will have established new truths about these unknowns and will be harder to challenge them. The Clarke's and Knake's book do exactly this; the book is rising concerns based on radical uncertainty without respecting already existing empirical evidence or references that would disqualify their overemphasized statements as the claim about cyber-attack on electrical grid was confuted years ago. Metaphors itself can produce enough power in our cognitive perception to believe the novel meaning they bring.[505] Metaphors of international security frame our perception of the global security

[502] Noam Ben-Asher and Cleotilde Gonzalez, CyberWar Game:A Paradigm for Understanding New Challenges of CyberWar In ibid.

[503] Cavelty, "Cyber-Terror--Looming Threat or Phantom Menace? Th."

[504] Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth."

[505] R Little, *The Balance of Power in International Relations: Metaphors, Myths and Models* (Cambridge University Press, 2007).

environment[506] by using the word *security* which is etymologically based on a word *secure* or *to secure.* Related metaphor denotes an activity securing us from undesirable state of war.

However, Chilton puts it in another way: that the war can be desirable while we are eradicating much worse condition; then the whole discursive process using the metaphor catches attention.[507] The concept of security then encapsulate images of stability, security and safety[508] and of course it encapsulates the opposite when challenged by uncertain threats nailed into an imaginative cyber war drawn as the cyber fallout after cyber-nuclear Armageddon. That image of stable society, the ideal model drawn on a horizon of our desirable future, is what drives national security policy makers. The managers of unease, to performatively materialize the Others who might cause unease – the geeks as terrorists; an indisputable future development that has to be preventively stopped. Security can be then produced only by materializing the insecurity by securitization discourse promising a brighter future.[509] Metaphors are powerful tools, because they add the previous experience new realities. While metaphors are important tools in developing imaginations that help us develop normalized reactions and thus become resilient against threats,[510] they also easily constitute groupthink, bring undesirable eventualities or produce self-fulfilling prophecies.[511]

Terms such as "critical infrastructure" embrace the uncertainty of undefined term *cyber war*, which embeds the security measures as a *constant state of emergency*. Critical infrastructure, a term, which boomed in the security policy recently[512] and which finally makes *critical* almost everything what is (had been) in fact the state infrastructure. This state of looming collapse of everything what is critical to the modern civilization and what

[506] Paul Anthony Chilton, *Security Metaphors: Cold War Discourse from Containment to Common House* (Peter Lang GmbH, 1996).

[507] Ibid., 77.

[508] Michael P. Marks, *Metaphors in International Relations Theory* (New York: Palgrave Macmillan, 2011), 108.

[509] Ben Anderson, "Security and the Future: Anticipating the Event of Terror," *Geoforum* 41, no. 2 (2010): 227–35.

[510] Aradau and Munster, *Politics of Catastrophe*, 46.

[511] David J. Betz and Tim Stevens, "Analogical Reasoning and Cyber Security," *Security Dialogue* 44 (April 2013): 147–64, doi:10.1177/0967010613478323.

[512] Cavelty, "Cyber-Terror--Looming Threat or Phantom Menace? Th."

emanates from cyberspace is visible almost every single week in news. Let me give it a quick try right now[513] and let's look just days ago from now, the day I am writing this paragraph: an article titled *"State on high cyber alert after Anonymous threat"* saying that the state is under attack on a daily basis with varied severity (Detroit Free Press, 22nd January 2016),[514] or article titled *"FireEye bulks up for 'cyber arms race'"* quoting words of chief executive of cyber security company FireEye who is convinced that all the governments around the world are chasing others in cyber arms race (FT.com, 20th January 2016)[515] or another example *"Australia not prepared for cyber war; response to threats 'slow and fragmented', report warns",* the report reportedly mentioned that Australia is *badly lagging* behind their counterparts and calls for *"rapid catch-up in Australian capabilities for military security in the information age"* (ABC News AU, 19th January 2016).[516] Extensive research of news in the last years would be a gargantuan task, but the direction of the narrative is clear – the cyber is under the process of militarization by discourse, it leads to that undesirable state where all nations are arming up without any possibility of arms control as these arms cannot be counted, destroyed, stored or discarded. On the one hand they are *badly lagging,* whereas at the same time everybody is arming in cyberspace – it looks like a new security dilemma. Studies have been published about this narrative in news. One of them – where one of the author was working for NATO CCD COE in Tallinn, Estonia – concluded that the term *cyberwar* is at least a hyperbole.[517]

Under this pressure in media, decision makers are producing *statements* about the current national security or about the current defense capabilities against *threats emanating from cyberspace*. Statements have particular meaning with sophisticated crucial analyses based on calculations of risk, anticipation of catastrophes, calling for

[513] I looked for a keyword "cyber" on news.google.com and chose only national security related topics on first three pages.

[514] Paul Egan, "State on High Cyber Alert after Anonymous Threat," *Detroit Free Press*, January 22, 2016, http://www.freep.com/story/news/local/michigan/flint-water-crisis/2016/01/22/activist-hacker-group-anonymous-starts-flint-campaign/79157780/.

[515] Hannah Kuchler, "FireEye Bulks up for 'cyber Arms Race,'" *Financial Times*, January 20, 2016, http://www.ft.com/cms/s/0/35b30470-bfb0-11e5-846f-79b0e3d20eaf.html#axzz46jzMnJpC.

[516] Francis Keany, "Australia Not Prepared for Cyber War; Response to Threats 'Slow and Fragmented', Report Warns," *ABC News*, January 19, 2016, http://www.abc.net.au/news/2016-01-19/australia-not-prepared-for-cyber-warfare-experts-warn/7097796.

[517] Cyrus Farivar, "A Brief Examination of Media Coverage of Cyberattacks (2007 - 2009)," *Cryptology and Information Security Series, The Virtual Battlefield: Perspectives on Cyber Warfare* 3 (2009).

preemptive actions drawing on imaginative outcomes if measures are not taken. These calls for preemptive actions in discourse is made like this: in 1991 we can read in a book from a respective National Academies Press *"Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."*[518] 21 years later, in 2012, Leon Penetta, that time U.S. Defense Secretary, calls for cyber defenses and called that moment a *"pre-9/11 moment"*[519] making an analogous link to a serious event to increase attention.

Finally, in 2013, Keith Alexander, that time Director of the National Security Agency (NSA), is preparing a nation for defense in cyberspace. Keith Alexander is making a relation to "*Armageddon strategy*," which was used against Germany in 1912 by United Kingdom. The logic of this strategy was to simultaneously cause sabotage attacks against infrastructure of Germany to cause its complete collapse. Then, Alexander uses the narrative of current dependence on our infrastructure, calling it critical infrastructure, and warns against similar Armageddon strategy one *can* conduct against America. Subsequently he is making an analogy to cyber-Pearl Harbor, which will be a wake-up call for Americans in new kind of a war in the world. To prove his perspective, he is remembering great power switches in the past such as Mongol empire conquering China, Spanish sailors conquering Americas or European empires in 19th which conquered a huge portions of the world territory. Now we see "*hundreds of thousands terabytes*" transferred somewhere, which he uses as an example of *"systematic pillaging of a rival state without military conquest and the ruin of the losing power."*[520] One must object here, that such lamentation grows in time, when that state – China – does not need to have the whole industrial espionage under control, [521] while the national security discourse will understand the situation quite exactly in the opposite way.[522] While these statements can be staggering or exaggerated, Alexander is supporting them by the argument that NSA has been a leader in signal intelligence since 1952. They certainly do understand their

[518] National Academy of Sciences (NAS), *Computer Science and Telecommunications Board. Computers at Risk: Safe Computing in the Information Age.* (Washington D.C.: National Academies Press, 1991).

[519] Pan Benson, "Panetta: Cyber Threat Is Pre 9/11 Moment," *Cnn.com*, October 12, 2012, http://security.blogs.cnn.com/2012/10/12/panetta-cyber-threat-is-pre-911-moment/.

[520] Keith B. Alexander, Emily Goldman, and Michael Warner, "Defending America in Cyberspace," *National Interest*, 2013, 18–24.

[521] Austin, "What the US Gets Wrong About Chinese Cyberespionage."

[522] George Patterson Manson, "Cyberwar: The United States and China Prepare For the Next Generation of Conflict," *Comparative Strategy* 30, no. 2 (November 14, 2011): 121–33, doi:10.1080/01495933.2011.561730.

job, but they are not those who can predict cyber Pearl Harbor if it can emerge *by one click*. However, one can ask what other authority should be the guarantor of knowledge than NSA with 60 years of expertise in studying communication networks?

2.4. From geeky politicians to critical events nailing their truths to the memorial plaque

There have been several events in the past, which can be understood as serious to national security. However, the problem lies exactly in this assessment – claim of seriousness to national security, which is then generalized in the term about *threats emanating from cyberspace*. Wiping out all the data in thirty thousand computers of Saudi Aramco[523] could be prevented by choosing at least some backup technology, maybe cloud backups would help to restart the whole system in seconds by deployment of new operation systems and downloading only critical data and settings from the cloud. I am making this quick assessment on information that the only thing that happened was a complete deletion of data, respectively overwriting of data by images on office computers, so no data could be recovered and the whole computer network has to be reconstructed. Such an attack should not halt operations. However, Saudi Aramco reportedly worked with pen and paper instead of computer database for weeks: *"employees used typewriters and fax machines."*[524] Here, we are not so far from moments where politicians or analysts are threatening public that a single cyber-attack can plunge us into the *stone age*,[525] while other deny that imaginative scenario. [526] Nevertheless, the risk to be plunged by cyber war to the *stone age* has been born. Debates concerning possible measures to be taken in future to avoid similar results after similar attack are simply nonexistent or very rare, especially in political discourse. Stone Age, Cyber Armageddon, first symptoms of cyber 9/11 is what we usually hear after a batched deletion process in one oil company. The

[523] Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival* 55 (May 19, 2013): 81–96, doi:10.1080/00396338.2013.784468.

[524] Fahmida Y. Rashid, "Inside The Aftermath Of The Saudi Aramco Breach," *Information Week. Dark Reading.*, August 8, 2015, http://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676.

[525] Jon E. Dougherty, "It's Time to Negotiate a Cyber War Treaty before the World Is Thrown back to the Stone Age," *Cyber War News*, September 28, 2018, http://www.cyberwar.news/2015-09-28-its-time-to-negotiate-a-cyber-war-treaty-before-the-world-is-thrown-back-to-the-stone-age.html.

[526] David Gewirtz, "Could Cyberwar Knock Us back to the Stone Age?," *ZDNet*, August 3, 2015, http://www.zdnet.com/article/could-cyberwar-knock-us-back-to-the-stone-age/.

network/computer administrators in Saudi Aramco certainly made some countermeasures, but that is not mentioned in the attack analysis which draws the imaginative future as it does fit in this hypersecuritization discourse. Saudi Aramco is a proof of incoming *cyber war* and we should start thinking about upcoming *Cyber Apocalypse* to deter or preventively diminish the number of future cyber terrorism attacks.[527]

In 2003, Shawn Carpenter, who was a network administrator unveiled some anomalies in his network and after some time uncovered one of the biggest cyber espionage campaign ever. We can read in a book published by Routledge[528] that Carpenter was inspired by famous novel Cuckoo's Egg[529] what made him vigilant and attested. Carpenter later cooperated with FBI, which called the campaign Titan Rain. The alleged result of the campaign was uncountable amount of military classified information stolen about facilities such as Fort Dix, the Redstone Arsenal, the Defense Contract Management Agency and the World Bank. All this information was stolen probably by China, or at least, transferred to China. Such event and some other similar ones led to calling this period *"the greatest transfer of wealth in history."*[530] China was accused more than one time. A cyber security firm Mandiant (recently bought by FireEye) in 2013 published a famous report called APT1 – The Advanced Persistent Threat no. 1, in which they convincingly show for the first time how an attack can be attributed to a state, particularly in this case to the Chinese People's Liberation Army, Unit 61398, using network forensics methods.[531] Despite the fact that APT1 shows pure espionage activities, it is used as an argument that we stand in front of the *cyber warfare*[532] or to let stirring journalist to "*declare a cyber war"* on China on behalf of the US government, while the whole case ends smoothly with a single charge of a jury on five Chinese hackers.[533]

[527] Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent," *Vanderbilt Journal of Transnational Law* 43 (2010): 57–118.

[528] Green, *Cyber Warfare*, 9.

[529] Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (Doubleday, 1989).

[530] Rogin, "NSA Chief: Cybercrime Constitutes the 'greatest Transfer of Wealth in History.'"

[531] Mandiant, "APT1 Exposing One of China's Cyber Espionage Units," *Report*, 2013, 1–76, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[532] Green, *Cyber Warfare*, 12; Paulo Shakarian, Jana Shakarian, and Andrew Ruef, *Introduction to Cyber-Warfare*, *Introduction to Cyber-Warfare*, 2013, doi:10.1016/B978-0-12-407814-7.00010-5.

[533] Rupert Cornwell, "US Declares Cyber War on China: Chinese Military Hackers Charged with Trying to Steal Secrets from Companies Including Nuclear Energy Firm," *Independent*, May 19, 2014,

However, these actions were mentioned as *probable* by the U.S.-China Economic and Security Review Commission in the late 2010 due to the rapid evolvement of Chinese telecommunication capabilities[534] with no regard on their espionage nature. We can find reasons of this Chinese behavior in their traditional strategic literature mentioning the tacit advantage in information over your enemy as the key strategic factor.[535] The merging of waging war with the conduction of pure espionage causes only chaos in conceptualization of the threat in a hypersecuritization manner. It amplifies its possible security impact and hinders the real problem. China is not conducting a war; China, or private business on its territory, probably conduct espionage in cyberspace.

Another attack which is understood as the first cyber war is with no doubt the DDoS attack on Estonia.[536] International law lawyers analyzed the claim of its state sponsorship at least problematic,[537] but that does not stop others using Estonia as an example of future cyber war despite fining particular persons for criminal offense in this case.[538] Estonia has become an inseparable partner for the West in any cyber related threats.[539] Critical part on Estonia example is the political impact it caused. NATO described cyber-attack higher than nuclear attack.[540] President Toomas Hendrik Ilves asked what is the difference between naval blockade and DDoS attack when they completely paralyzed a country.[541] Experts in NATO, in a division of Emerging Security

http://www.independent.co.uk/life-style/gadgets-and-tech/us-charges-chinese-military-hackers-with-cyber-espionage-bid-to-gain-advantage-in-nuclear-power-9397661.html.

[534] USCC, "The National Security Implications of Investments and Products From the People's Republic of China in the Telecommunications Sector," 2011, http://www.uscc.gov/sites/default/files/Research/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf.

[535] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999).

[536] Kampmark, "CYBER WARFARE BETWEEN ESTONIA AND RUSSIA"; Cassandra M. Kirsch, "Science Fiction No More: Cyber Warfare And The United States," *Denver Journal of International Law & Policy* 40 (2012): 620–47; Shackelford, "ESTONIA THREE YEARS LATER: A PROGRESS REPORT ON CO."

[537] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law* 27 (2009): 192–251.

[538] BBC, "Estonia Fines Man for 'Cyber War,'" *BBC News*, January 25, 2008, http://news.bbc.co.uk/2/hi/technology/7208511.stm.

[539] Atlantic Council, "Exclusive Interview with Estonian President Ilves on Cyber Security," 2013, http://www.atlanticcouncil.org/blogs/new-atlanticist/exclusive-interview-with-estonian-president-ilves-on-cyber-security.

[540] NATO, "Active Engagement, Modern Defence," in *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted at the NATO Lisbon Summit* (Brussels: NATO Public Diplomacy Division, 2010), http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf.

[541] NATO Review, "Cyberattack, NATO and Angry Birds," *Nato.int*, 2013, http://www.nato.int/docu/review/2013/Cyber/Cyber-attacks-NATO-angry-birds/CS/index.htm.

Challenges, are thinking about how to include NATO capabilities in cyberspace as a next domain to land, sea, air and space.[542] The development of such a strategic perspective is backed by well-known and globally recognized expert Eugene Kaspersky who founded and owns one of the leading top anti-virus companies.[543] These epistemic communities of computer experts are becoming authorities supporting the narrative of a relation between cyber and national security. Kaspersky employees argues that the whole cyber war hysteria is helping to grow their business, understandably.[544] Geeks are becoming members of a cyber global defense league if they are converted on the side of national security.[545]

Especially when it comes to Estonia attack, immediately after the attacks Estonians became world-wide recognized experts on cyber security due to their first-hand experience as transactors or translators of expertise.[546] They were immediately invited in specific cyber related researches as being respected world-class experts on cyber security; Estonians were two out of four contributors from Europe.[547] Estonians even personally admitted that the process of this recognition was an amazing gift;[548] even the Minister of Defense admitted it.[549] Beside this geek-to-national security expert transaction, we can witness the opposite direction, which is probably due to the enlarging cooperation between states and private sector. Microsoft launched a program called Government Security Program (GSP) already in 2003 to let governmental officials check their source code for vulnerabilities. NATO was involved in this program later, in September 2015, reaching numbers of 44 agencies and 26 governments checking the code right now. DARPA is willing to add artificial intelligence exactly to this process of

[542] Jamie Shea, "New Security Challenges And Nato's Future," *Turkish Policy Quarterly* 10 (2011): 53–59.

[543] Andrew E. Kramer and Nicole Perloth, "Expert Issues a Cyberwar Warning," *New York Times*, June 3, 2012, http://www.nytimes.com/2012/06/04/technology/cyberweapon-warning-from-kaspersky-a-computer-security-expert.html.

[544] A personal meeting at International Conference on Cyber Security organized by Fordham Univerisity and FBI arranged in New York in August 2013 with Kaspersky's employees.

[545] Kelly, "Investigating in a Centralized Cybersecurity Infrastructure: Why 'Hacktivism' can and Should Influence Cybersecurity Reform."

[546] Latour, *Science in Action: How to Follow Scientists and Engineers Through Society*, 108–121.

[547] McAfee, *Virtual Criminology Report 2009: Virtually Here: The Age of Cyber Warfare* (Santa Clara, CA, USA: McAfee, 2009), www.mcafee.com.

[548] Based on a personal discussion at the Ministry of Defense of Estonia in Tallinn with Siim Alatalu, 21st Novemebr 2013.

[549] J Aaviksoo, "Cyberspace: A New Security Dimension at Our Fingertips," *CSIS Statesmen's Forum*, 2007.

code checking. Quoting ambassador Sorin Ducaru, an assistant secretary general of NATO's emerging security challenges division, *"we see this signing as another step forward in the NATO-Industry Cyber Partnership, building a stronger cyber defence network today with Microsoft, but also with other industry partners across the world."*[550] Private global corporations are now part of the global cyber defense campaign dealing with cyber war. The intermingling process between national security experts dealing with national defense and experts on computer security is inevitable; however, despite the fact that the Estonia case might never happen again as the computer experts took countermeasures to avoid the same scenario.[551] Not to mention that according to widely available sites such as digitalattackmap.com we are facing quite bigger attacks today if the load of traffic is a measure than we witnessed in the Estonian case. Yet, we are not witnessing any political consequences as we have observed since the Estonian DDoS attack throughout the whole world; in every single national cyber strategy, from Africa, through Europe to South America and Oceania.

NATO is just the second step; Microsoft has been giving data under the GSP for years to US government when was asked to help with crime investigation by FBI. Microsoft is in this case under pressure from US government to handover not only data of US citizens or companies, but data from all around the world arguing that source of the data does not matter, only the location of Microsoft headquarters matters. Microsoft of course opposes this practice arguing that breaking this line would be *"unilateral law-enforcement incursions into a foreign sovereign country."*[552] Being part of NATO strategy now, Microsoft does not help to tackle crime only, but helps national security. They were called to do that. However, the untouchable foreign sovereignty is for Microsoft a stronger argument when *defending the nation in cyberspace*. What seems to be obvious to Microsoft is not obvious to state authorities. As I argue in the end, technology can become mature and more secure; however, if we step over the core principles today and communication technologies become more secure tomorrow, we will already found

[550] Liam Tung, "Microsoft Signs Deal to Let NATO Check Its Products for Backdoors," *Zdnet.com*, September 25, 2015, http://www.zdnet.com/article/microsoft-signs-deal-to-let-nato-check-its-products-for-backdoors/.

[551] Based on a personal discussion at the Ministry of Defense of Estonia in Tallinn with Siim Alatalu, 21st Novemebr 2013.

[552] "Should Governments Be Able to Look at Your Data When It Is Abroad? | The Economist," *The Economist*, 2015, http://www.economist.com/news/business-and-finance/21663902-test-case-set-determine-whether-fbi-can-access-microsofts-foreign-data-should.

ourselves breaking the red line of decades long stipulated core principles of international law. That can have a massive impact on international security and I believe much more significant and important than a risk of cyber-attack on critical infrastructure of whatever immediate effect such an attack can cause.

Another *threat emanating from cyberspace* was apparently Stuxnet. I will be brief in this case as Stuxnet has been thoroughly studied from all meaningful perspectives.[553] The point I would like to make here is that Stuxnet proved existence of cyber weapons in hands of states, supposedly. We were told that it was a cyber weapon, because with this piece of code we were able to avoid an airstrike: "*To some degree, this piece of software replaced a squadron of fighter aircraft that would have violated foreign airspace, dropped laser-guided bombs, and left a smoking crater in the Earth's surface."*[554] Stuxnet hit Iranian nuclear program by implementing a piece of code into their systems causing fluctuation of nuclear centrifuges spin speeds and thus physical destruction. No reason to lower the seriousness of the attack character, exactly the opposite. We cannot omit the fact that we live in information age where some kind of conflict related to information is more than possible, but there are voices criticizing linking full-scale war to a targeted sabotage.[555] Stuxnet is a clear example of 21st century precise state sponsored sabotage sending a message to Iran that we do not want to see Iran with a nuclear bomb. Nothing else. However, Stuxnet attack is ordinarily analyzed along with Estonia attacks discussed above. The reiteration of alarming discourse production can be seen on making relation between easy-to-conduct attacks such as DDoS, which anyone can buy on internet – not to mention that the scale we witnessed on Estonia is quite different at least in its orchestrated shape from what we can buy – with extremely sophisticated attacks such as Stuxnet: *"As demonstrated in the preceding paragraphs, cyber tools, like Stuxnet and the*

[553] Alexander Nicoll, "Stuxnet: Targeting Iran's Nuclear Programme," *Strategic Comments* 17 (2011): 1–3, doi:10.1080/13567888.2011.575612; Nicolas Falliere and Chien, "W32.Stuxnet Dossier"; Sean Collins and Stephen McCombie, "Stuxnet: The Emergence of a New Cyber Weapon and Its Implications," *Journal of Policing, Intelligence and Counter Terrorism* 7 (April 2012): 80–91, doi:10.1080/18335330.2012.653198; Richard A. Falkenrath, "From Bullets to Megabytes," *New York Times, The (NY)*, accessed January 1, 2028, http://www.nytimes.com/2011/01/27/opinion/27falkenrath.html?_r=1.

[554] D E Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (Crown Publishing Group, 2012), 188–225.

[555] Rid, *Cyber War Will Not Take Place*, 2013.

wide-scale DDoS attacks on Estonia, have the potential to inflict massive amounts of damage on a state computer network, or even a nuclear reactor."[556]

To summarize this empirical part, I wanted to demonstrate how easily political statements developed into a constant state of insecurity,[557] where no one can predict what can happen tomorrow. That however is not too important, the point is that due to the fact that we cannot predict it and we only *know* what *may* happen policy makers tend to act. The high-rank officials call on our responsibility that there is no doubt what awaits us as in the speech by Leon Panetta during hearing of his nomination: *"There is no question that the whole arena of cyber-attack s, developing technologies in the information area represent potential battlefronts for the future. I have often said that there is a strong likelihood that the next Pearl Harbor that we confront could very well be a cyber-attack that cripples our power systems, our grid, our security systems, our financial systems, and our governmental systems."*[558]

No one can simply become minister of defense without having a portion of securitization discourse, I would argue. The imaginations of possibilities is important. Denying threats is not what the audience is willing to hear. The ability to name, form and materialize the threat by discourse with as much as possible alarming connotations is a lift to the office. The ability to predict near futures is critical for any leader. However, one has to take into consideration what Pearl Harbor meant to United States of America in December 1941. President Roosevelt had been working hard to explain to American public why it is important to support United Kingdom against Nazi Germany. About 8% Americans wanted to see their country in World War II during the Battle of Britain in summer of 1940. Using analogy with Pearl Harbor is a game with emotions, which put Americans into war that time. As Gartzke argues, probably no other event in 20th Century realigned American public opinion and then US foreign policy more than the Pearl Harbor catastrophe.[559]

[556] Kirsch, "Science Fiction No More: Cyber Warfare And The Uni," 629.

[557] J. Hagmann and Myriam Dunn Cavelty, "National Risk Registers: Security Scientism and the Propagation of Permanent Insecurity," *Security Dialogue* 43, no. 1 (2012): 79–96, doi:10.1177/0967010611430436.

[558] Committee on Armed Services, "U.S. Senate Committee on Armed Services Hearing to Consider the Nomination of Hon. Leon E. Panetta to Be Secretary of Defense" (Washington D.C., June 9, 2011), 206.

[559] Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth."

3. THE KNOWLEDGE FLOW INTO NATIONAL SECURITY DISCOURSE

3.1. The takeover of knowledge by national security structures

As I cited Sheila Jasanoff in the theoretical part, nation states lost their ability to govern society in this technological labyrinth.[560] Calling everything a cyber war, led to exaggerated journalist articles translating charge of a judge as a hyperbolic declaration of war between nations.[561] The moment between state of peace and state of war has been blurred, but certainly not due to the war declaration, but thanks to the construction of the state of unease by discourse,[562] the escalation of imagined dangers,[563] calling for defenses against any possible threat[564] and finally opening a Pandora box with ideas such as active cyber defense, which consists of active hacking and thus open offense.[565] Active cyber defense is a policy proposal that will lead to the escalation, at least on espionage and diplomatic levels and as the policy makers are threatened enough, their capability to transfer the knowledge appropriately to balanced policy making remains problematic and hasty. The following example show it clearly.

In 2007 the U.S. Department of Energy conducted a test of cyber-attack on an electric generator called "The Aurora Test."[566] The test was, briefly said, focused on changing the tolerance of frequency changes within which the power grid still takes the power from the generator. Frequency is changing with the spinning of the generator. If the frequency of the generator is different with the frequency in the network, usually the generator overheats and can break up. Logic seems to be easy, but after reading of the technical details regarding Aurora Test,[567] I do not see anything special that might be linked to possible catastrophe event. It is the most common glitch that can be exploited

[560] Jasanoff, *Designs on Nature: Science and Democracy in Europe and the United States*.

[561] Cornwell, "US Declares Cyber War on China: Chinese Military Hackers Charged with Trying to Steal Secrets from Companies Including Nuclear Energy Firm."

[562] Claudia Aradau, *Critical Security Methods: New Frameworks for Analysis* (Oxon: Routledge, 2015), chap. 7.

[563] Kaiser, "The Birth of Cyberwar."

[564] Clarke and Knake, *Cyber War: The Next Threat to National Security an*.

[565] Irving Lachow, "Active Cyber Defense - A Framework for Policymakers," 2013, http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf.

[566] Do not confuse it with Operation Aurora, which was targeted to steal intellectual property from Google and other corporations.

[567] Mark Zeller, "Common Questions and Answers Addressing the Aurora Vulnerability," in *DistribuTECH Conference* (San Diego, CA, 2011), https://cdn.selinc.com/assets/Literature/Publications/Technical Papers/6467_CommonQuestions_MZ_20101209_Web.pdf.

only with very uncommon knowledge. An attacker needs to have a connection to the system including very special knowledge of local settings. Hence, the broadcast attack against all generators around the world is in this perspective impossible and thus armageddon-like disasters as well. The amount of specificities need to be taken into consideration is a long list: *"In order to execute a successful Aurora attack, the perpetrator must have knowledge of the local power system, know and understand the power system interconnections, initiate the attack under vulnerable system load and impedance conditions, and select a breaker capable of open/close switching that is fast enough to operate within the vulnerability window."*[568] Hence, it is blunt to compare this possible attack to what happened with Slammer Worm.

At least, somebody created a name for a possible attack to a critical infrastructure – an *Aurora attack* – a name that creates the whole catagory of possible attacks, against which we have to be prepared. I read the problem as follows: difference between a knob on physical controller and remote control of this generator is only in distance, to overcome the distance we need specific knowledge, which is known to workers operating the system, the vulnerability is just the possibility in a *potential ability* and it does not poses risk: *"The Aurora vulnerability exists because of an attacker's potential ability to access key protection and control systems."*[569] The technical article then concludes with an assertion that the vulnerability pose risk only to an unprotected system and that: *"current technology, much of it very low cost, is available to mitigate this risk."*[570] Hence, we are very close to the possibility that this particular vulnerability in the used systems has been already patched. On the other hand, we saw how much time it took to solve the vulnerability in Siemens S7 systems after the Stuxnet attack, in fact years.[571] However, even if solved, some other would exist and will exist forever as there is no way how to make future communication systems bulletproof as they evolve. That being said, the architecture of the systems can be designed to be less prone to attacks; e.g. by avoiding

[568] Ibid., 1.
[569] Ibid.
[570] Ibid., 6.
[571] Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment," *Journal of Strategic Studies* 36, no. 1 (February 2013): 120–24, doi:10.1080/01402390.2012.742014.

standard configurations or standardized technologies or use multifactor authentication, which is not a norm in industrial systems.

Nevertheless, another book called Introduction to Cyber Warfare: A multidisciplinary Approach[572] is using Aurora Test as an example that attacks on industrial systems are possible, but the possibility does not equal risk and risk is critical in assessing the threat. The imagination grows as repetitions of these possibilities multiply in literature. Clark's and Knake's book[573] from 2010 uses the Aurora Test to demonstrate their armageddon-like scenario and put it into the hands of *cyber warriors* as follows: *"If the attacks destroy generators, as in the Aurora tests, replacing them can take up to six months, because each must be custom built. Having an attack take place in many locations simultaneously, and then happen again when the grid comes back up, could cripple the economy by halting the distribution of food and other consumer goods, shutting down factories, and forcing the closure of financial markets."*[574] Clarke and Knake are convinced that the vulnerability does pose a direct risk to national security and that simultaneous attacks are possible. The technical paper[575] showed us that it is simply not the case. CNN reports just after the Aurora Test in 2007 that *some experts fear bigger* in terms of months long period before the generators are rebuild.[576] In the same article we can read a quotation of DHS undersecretary that the threat had been eliminated. This vulnerability has not been a threat since 2007 and the wider attack is only a hypothesis of energy experts, according to the same CNN article. [577] Other vulnerabilities might remain, but no other attack has happened to day.

Aurora Test, a one test, one hack, one vulnerability, one case, one event is discursively repeated everywhere. All kinds of national critical infrastructures are mentioned in a relation to Aurora as the initial argument of possible critical infrastructure collapse despite the technical analysis by ICT experts who denied such armageddon-like scenario. I used this particular example to demonstrate how the

[572] Shakarian, Shakarian, and Ruef, *Introduction to Cyber-Warfare*.
[573] Clarke and Knake, *Cyber War: The Next Threat to National Security an*.
[574] Ibid.
[575] Zeller, "Common Questions and Answers Addressing the Aurora Vulnerability."
[576] Jeanne Meserve, "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid," *Cnn.com*, 2007, http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html?iref=topnews.
[577] Ibid.

awkwardly is technical knowledge translated into policy implications. I admit that critics of my writing might argue that the whole argument cannot be based on one event; however, I would argue back that this is the case almost in the entire cyber security discourse – enforcing global cyber security policy based on imaginations that are inspired in awkward evidence interpretations of single events. The number of events that have happened until today is critically low to raise the cyber defense walls in no-border cyberspace. Especially by giving specific power to authorities to act, counteract, counterattack and to do all this even preventively. There cannot be better example of security dilemma and as some argue, we are not going to wage war in cyberspace until we develop weapons and use them.[578] The fictitious imaginations can be at the beginning of particular technology development and thus some of these dystopian imaginations can become true.

3.2. Resonation of newly acquired knowledge in national cyber strategies

Three important international organizations exist that support the development of national cyber strategies: ITU – International Telecommunication Union[579] on a global scale, ENISA – European Union Agency for Network and Information Security[580] which works more on the European level and NATO CCD COE – North Atlantic Treaty Organization Cooperative Cyber Defense Center of Excellence[581] that supports NATO countries at first. We might be able to find some others within the nexus of international bodies, but for further analysis I decided to put my attention to these three. Then I will put attention to Microsoft and Oxford University.

Each of the mentioned institution have done to some extent a comparative analysis of national cyber strategies, but mainly produce recommendations to national bodies responsible for national cyber strategy development. ITU is working on a list of these rules – or good practices – concerning the content of the national strategies, which

[578] Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better."
[579] Homepage: http://www.itu.int/
[580] Homepage: http://enisa.europa.eu/
[581] Homepage: http://ccdcoe.org/

will show comparison between these recommending documents.[582] ITU is mentioning the following guides in the list to be compared. First ITU recommends its own guides, ITU National Cyber Security Toolkit (the one under development) and ITU National Cybersecurity Strategy Guide (2011),[583] followed by similar documents form ENISA: National Cyber Security Strategies, a practical guide on development and execution (2012)[584] and An evaluation Framework for National Cyber Security Strategies (2014)[585] and one document by NATO CCD COE called National Cyber Strategy Framework Manual (2012).[586] These documents are supported by corporate perspective from Microsoft with a document called Developing a National Strategy for Cybersecurity (2013)[587] and academic perspective from Oxford University called Cyber Security Capability Maturity Model.[588]

The above mentioned manuals and frameworks do not vary too much from each other. Differences are usually coming from the purpose of the document, e.g. Microsoft focuses on the same topics as ENISA. The red line across these documents stress on developing response institutions such as CERTs, building public awareness along with particular new education programs, supporting technological development towards more secure technologies and promoting international cooperation and engagement. These four pillars are widely understood as the building blocks of national cyber security strategy. Additionally, they focus on some organizational structure such as national cyber security coordinator or specific training programs focused on developing key skills for

[582] Work on this project is not finished during the time of writing this dissertation, however, some preliminary presentations has been already made public at ITU, "National Strategies," 2016, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx.

[583] ITU, *National Cybersecurity Strategy Guide* (International Telecommunication Union, 2011), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

[584] ENISA, *National Cyber Security Strategies - Practical Guide on Development and Execution* (ENISA, 2012), https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide.

[585] ENISA, *An Evaluation Framework for National Cyber Security Strategies* (ENISA, 2014), https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1.

[586] Alexander Klimburg, *National Cyber Security - Framework Manual* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012).

[587] Cristin Flynn Goodwin and J. Paul Nicholas, *Developing a National Strategy for Cybersecurity* (Microsoft, 2013), http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf.

[588] Globa Cyber Security Capacity Centre, *Cyber Security Capability Maturity Model* (University of Oxford, 2014), http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM Version 1_2_0.pdf.

cyber security professionals. Last, but not least, documents stress that appropriate legal measures should be adopted. All of these documents harshly stress on development measures that are producing self-living bureaucratic organism within a particular state. When it comes to debates regarding purpose of these strategies, we can read that the first priority is to tackle with this *national security threat* as a *global challenge*.[589] Bauman in the aftermath debate in the consequence to Snowden revelations raised a question, who's strategy is this when the operation is interlinked between nation states, corporations and subcontracted persons?[590]

This perspective changed after the annexation of Crimea, after witnessing the related cyber strategy to the annexation. The whole discourse focused on critical infrastructure was shaken by the serious empowerment of information by Russia in its intensive propaganda campaign.[591] Since then, the world has been talking about a new threat and the confusion of strategists led to an emergence of new concept – hybrid warfare. While the core part of this new strategy lies in a tacit, precisely aimed, persistent and devoted propaganda that seriously undermines beliefs in liberal democratic regime. This policy switch from cyber-attacks against physical critical infrastructures towards attacking minds and hearts that can undermine beliefs into liberal democratic values has been visible throughout the cyber security discourse since 2014.[592] In that article I put attention on processes that might seriously undermine credibility of liberal democratic regimes and that what are we witnessing in the aftermath of Crimea annexation is not just a mere propaganda, but exactly this coordinated effort towards such an objective. I still understand it as a critically serious threat to national security, which is hidden, tacit, slow, but effective and hard to tackle. The military imaginations applied on future cyber possibilities did not help us to predict how serious can be the massive operation of Russian trolls that influence democratic process throughout the western world; completely different perspective on the defense is needed as the evidence building against propaganda by mainstream media does not reach the same audience as Kremlin

[589] ITU, *National Cybersecurity Strategy Guide*, 26.
[590] Bauman et al., "After Snowden: Rethinking the Impact of Surveillance."
[591] Pomerantsev and Weiss, "The Menace of Unreality : How the Kremlin Weaponizes Information , Culture and Money."
[592] Schmidt, "Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War."

targeted or because the whole propaganda campaign is much more focused on undermining credibility of established institutions rather than to adore Russia.[593] The militarization of information space proves to be effective and no infrastructure need to be attacked.

Additionally, propaganda using cyber means is not understood by international experts as use of force or violation of territorial integrity, as written in Tallinn Manual: *"…non-destructive cyber psychological operations intended solely to undermine confidence in a government or economy do not qualify as uses of force."*[594] This is despite newly emerging discourse concerning the hybrid threat as a national security concern in shape of complex operations including conventional and non-conventional force to reduce the power of state response.[595] Majority of national cyber security strategies (NCSS) did not even mention this problem as a national security concern, and again, until the annexation of Crimea. In comparison of selected and available NCSSs of leading EU states and USA between years of 2007 to 2013 shown that there is only one usage of word *hybrid*; in Estonian strategy from 2013.[596] The problem was not existent before, at least in relation to cyber security; especially not in crucial books focused on policy recommendations how to draft cyber security strategy from think tankers[597] or even from NATO.[598] However, new policy frameworks for national cyber security strategies written after the Crimea annexation are mentioning the hybrid threat as a new concern to national security in relation to depletion of nation state power and dissolution of nation state as the actor having monopoly to power.[599] The new security discourse for cyberspace has been born.

[593] Edward Lucas and Peter Pomerantsev, *Defending and Ultimately Defeating Russia's Disinformation Techniques. Recommendatins. A Report by CEPA's Information Warfare Project in Partnership with the Legatum Institute* (Center for European Policy Analysis, 2016).

[594] CCDCOE, *Tallinn Manual on the International Law Applicable* S1, R11, par.3.

[595] Partnership for Peace Consortium, "Hybrid Conflicts as an Emerging Security Challenge: Policy Considerations for International Security" (PfPC Emerging Security Challenges Working Group Policy Paper No. 3, 2015).

[596] Comparison of national cyber security strategies between years 2007-2013 including states: Czech Republic, Estonia, France, Germany, Hungary, Netherlands, Norway, Poland, Slovakia, Spain, United Kingdom of Great Britain, United States of America.

[597] Jennifer L. Bayuk, Jason Healey, and Paul Rohmeyer, *Cyber Security Policy Guidebook* (Somerset, NJ, USA: Wiley, 2012).

[598] Klimburg, *NATIONAL CYBER SECURITY - FRAMEWORK MANUAL*.

[599] A Vaseashta, P Susmann, and E Braman, *Cyber Security and Resiliency Policy Framework*, EBSCO Ebook Academic Collection (IOS Press, 2014), 58.

4. NATO GOES CYBER

"NATO Tests Cyber-Defense Firepower to Combat Internet Terror"

— Ian Wishart, Bloomberg —

First note to the sources. As I mentioned earlier, I am choosing open source articles from websites as they constitute discourse that later resonates within authorities. When the argument requires it, I am choosing official document or official website of particular institutions, here prevalently NATO, to support the text that constitute the discourse. Finally, if these articles argue on technical details, I am citing technical reports by experts. In this chapter, all articles were recommended by NATO NCIRC bulletin; hence especially officers in NATO probably read them or recommended them, but certainly circulated them. NATO itself put attention on these articles and I am choosing only those that NATO tagged in the bulletin as *NATO related.*

NATO has established NCIRC (NATO Computer Incident Response Capability) in order to defend allies from cyber-attacks. In particular, it focuses on detecting and responding on cyber-attacks, which is the core activity of any CERT (Computer Emergency Response Team),[600] which are dated to 80s when the Carnegie Mellon University established the first such a team. Today, every nation state with working cyber security policy usually has such a team. CERTs have been established relatively recently, beginning in 2000 until now. However, the explosion of CERT teams can be dated to the event in Estonia in 2007. Today, they are common throughout the world.

I analyzed 774 news bulletins that were sent by NATO NCIRC in period beginning 28th February 2013 ending 28th April 2016. In this bulletin, NATO sends unclassified information on a daily basis in form of links to other websites discussing actual cyber security issues divided into certain categories. From 774 bulletins, 149 included articles that have been by the decision of NCIRC team tagged as *related to NATO*. In the following table, I analyzed only these 149 bulletins to show into what categories these articles break up according to the topic that is *related to NATO*. Other articles, which count to thousands, where used randomly to study the *cyber defense* discourse. The following

[600] Carneggie Mellon University, "CERT Software Engineering Institute," accessed April 28, 2016, www.cert.org.

table shows my subjective separation into topics based on analysis of more than 149 articles that are related to NATO according to NCIRC. Sometimes the category contains more than one link or the article visibly discussed more topics. This is why the sum is not 149.

	Topic	occurrence
attacks	Cyber-attack *occurrence* on NATO or allies (non physical, DDoS)	5
	Cyber-attack *occurrence* on NATO or allies (serious, critical infra*structure*)	0
	Cyber-attack *occurrence* on NATO or allies (espionage)	4
law	Article 5 discussion	6
	General international law debate	4
policy	Securitization of cyber (general policy perspective)	12
	Securitization of cyber (strategy perspective)	41
	Securitization of cyber (criminal perspective)	1
	NATO strengthen cyber power *(policy or action concerning NATO capabilities)*	8
action	Cyber defense against states *(action took)*	12
	Cyber defense against geeks/hackers/unknowns *(action took)*	9
	Cyber defense against hybrid/info/propaganda threat *(action took)*	7
	NATO against Russia or supporting Ukraine *(action took)*	14
events	NATO cyber exercises *(events)*	15
	NATO allies and partner cooperation *(events or policy actions)*	22
	NATO private business cooperation *(events or policy actions)*	5
	EU / NATO cooperation *(events or policy actions)*	4
info	Technical information	8
	General information	9

Table 4 - Topics break up of articles related to NATO in NCIRC bulletin[601]

Table depicts several groups of topics: particular attacks, international law debate, policy part, action part, events part and general information part. What I personally found

[601] The zip file of analyzed bulletins can be download from: https://dl.dropboxusercontent.com/u/2590527/ncirc.zip

interesting is the zero occurrence of attacks on the critical infrastructure. We can of course understand this zero as either: a mistake coming from the decision making on the side of NCIRC over information that should be *related to NATO* or that no one attack was conducted against an ally. However, one may seriously ask a question, why NATO has not reacted once in their bulletin on critical infrastructure attack as a *NATO related*? Especially when articles concerning cyber crime or DDoS attacks on national (not only NATO CCD COE) websites were understood as *NATO related* articles? We can read through out all the articles, official documents, statements, speeches, simply everywhere how attacks are rising especially on the critical infrastructure and the bulleting does not mention one in years. The subjectivity on the side of NCIRC is undisputable; however, this bulletin goes to hundreds of specialists and high-rank secretaries, policy makers, academics and so called cyber experts as they accidentally uncovered the whole list of recipients. The bulletin precisely covers the public debate regarding cyber security, but as I will show bellow they omit a critical event that is critical in shaping the image of current cyber security situation. One may argue that one event is not crucial; however, I would argue that this is not only about one event, but exactly about the critical point that evidence is not a source for discourse formation. Discourse is formed by *repeating* the *church of knowledge* signed by respected *authorities*, not by evidence and articles how cyber-attacks are serious by the words of authorities are abundant.

One significant cyber-attack happened against Ukraine on 23rd December 2015, which caused a blackout. The event was quickly considered as a cyber-attack;[602] however, later some experts denied the blackout to be directly caused by a cyber-attack.[603] Nevertheless, the report conducted by US experts from SANS Institute[604] in cooperation with Ukraine government unveiled how the cyber-attack was precisely planned. It was perfectly conducted, including novelties such as reprogramming firmware in routers and showed professional time plan and organization between the attackers who included also the execution of logic bombs with killdisk malware in computers managing power grids

[602] Dustin Volz, "U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage," *Reuters*, February 25, 2016, http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K.

[603] Sara Peters, "Questions Remain On How Cyberattack Caused Ukraine Blackout," *Information Week. Dark Reading.*, January 5, 2016, http://www.darkreading.com/attacks-breaches/questions-remain-on-how-cyberattack-caused-ukraine-blackout-/d/d-id/1323749.

[604] SANS ICS, *Analysis of the Cyber Attack on the Ukrainian Power Grid*.

just after the blackout to avoid quick restart. This Ukrainian cyber-attack in the end of 2015, the day before Christmas Eve, showed how orchestrated attack can seriously paralyze significant part of the country (about 1,2 million people); nothing that can be easily compared to simple Estonian DDoS. This was a sophisticated orchestrated attack against power infrastructure, professionally prepared and executed; *"the most seen attack against critical infrastructure to date"*[605] and there is no significant article in the whole NATO bulletin (not only in the *related to NATO* category, but in the whole bulletin). Ukraine is not a member of NATO, but this attack was not mentioned in the bulletin at all in reference to NATO strategy (some minor articles were mentioned, such as the one denying it as a cyber-attack, but nothing which would be related to NATO strategy, NATO reaction, NATO assessment, experts' assessments in order to reconsider NATO approach etc.). Only the article that questions the cyber-attack,[606] in which experts are not convinced about the malware implementation and the blackout itself. Attacking computers in power grid operator allegedly did not directly cause a blackout. Why so much panic regarding the possible cyber war conducted against critical infrastructure and then so low attention to the most visible example of such an attack? I would add here, that some of the outcomes from the experts' report mentioned that multifactor authentication would made it really hard to attacker, maybe this easy-to-set-up security measure would completely prevent the attackers from conducting the operation as stolen credentials would not be enough.

Any single geek or technical expert behind the analysis of the attack would recommend (and they did in the report) what security measures the operator has to adopt to avoid comparable situation in the future. This is not a cyber war; this is a flagrant mistake in taking common computer security measures seriously. An easily adoptable security measure, which is elsewhere called *cyber defense*. However, any law enforcement specialist would raise penalties for these intrusions seeing criminal hacktivists behind it. And finally, any *cyber defense* or *cyber terrorist experts* would raise cyber defenses of national defense or allied defense in NATO.

[605] Ibid.
[606] Peters, "Questions Remain On How Cyberattack Caused Ukraine Blackout."

As a result, we have a huge historical attack, no attention in NATO bulletin and the fact that despite one of the best cyber security measures (Ukrainians had measures sometimes higher than some operators in US have according to SANS institute)[607] the attack would be prevented by easy-to-set-up cyber security measures such as multifactor authentication. However, the analysis of the NATO bulletin showed about 41 instances of articles *related to NATO* that calls for strategic perspective of strengthening NATO cyber defenses against cyber-attacks from states or terrorists, but missed the evidence that should perfectly help think about these measures.

Cyber War, a term that can be found in 55 out of 774 bulletins. I chose only selected articles that are oriented roughly to deepening *cyber defenses*. The first example is written directly by the secretary general of NATO Anders Fogh Rasmussen,[608] in which he starts by comparing economical loses on Dow Jones exchange market based on a bogus tweet about a bombing in White House. That is the beginning, however, the article is clear in its securitization message, which follows: *"How times have changed. During the age of the Berlin Wall, tanks and ideologies faced off across closed borders. In the age of the firewall, borders are open, ideas are free and war can be virtual—but its consequences just as devastating and real"* and then he continues mentioning loses of corporations rising up to $1 trillion or that *"Computer viruses can shut down key infrastructure such as nuclear power plants, international airports, or power grids. Cyberattacks are a cheap way for terrorists, activists and state-sponsored agents to do extensive damage."*[609] If they were cheap and easy, we would witness the predicted armageddon. The attack on Ukraine was not cheap, was not conducted by a lone terrorist, was done because some security measures were not taken seriously and NATO did not give attention to it in its core information bulletin. Rasmussen is using language, which is strictly about *cyber defense,* while it is not clear what is the difference between *cyber defense* of a nation and *cyber security* of particular installations. Probably both, but *cyber defense* sounds more familiar to policy experts we expect to read these bulletins. On the one hand, Rasmussen is talking

[607] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[608] Anders Fogh Rasmussen, "NATO's Next War—in Cyberspace," April 28, 2016, http://www.wsj.com/articles/SB10001424127887323855804578508894129031084.

[609] Ibid.

about primary objective in securing NATO networks in headquarters and units deployed, on the other hand *"cyberattacks are a global challenge, and NATO can contribute to a global response."*[610] So what is the possible cyber war for NATO?

As we can observe across media articles, there is a consensus between security experts that *cyber* and *terrorist* attacks have been witnessed in recent years and that these experts along with political observers agree that these attacks can be orchestrated by political adversaries in order to constitute a state of cyber war.[611] A group of experts met in 2014 to discuss the events to date in order to set the threshold that constitutes an act of war in cyberspace; the result is that each of the core three security principles in cyber security (availability, confidentiality, integrity) can constitute an act of war.[612] Even experts on international law,[613] who were later working on Tallinn Manual on the International Law Applicable to Cyber Warfare[614] concluded that certain actions can constitute use of force. However, they later added (what is discussed in the manual exactly vice versa) that even economic disruption (e.g. the one mentioned by Rasmussen) without physical damage could also warrant retaliation under the right of self-defense (Schmitt, the author of the manual shares this position); the *severity* of the attack is what will answer the threshold[615] and severity is dependent on case-by-case assessment. However, some attributes of severity are discussed in the manual and they are scope, duration and intensity.[616]

Later on, the developments led to the debates whether to change the original Washington Treaty signed in 1949 establishing NATO as the Article 5 should be reformulated as the so called Cyber Defense Declaration from the Wales Summit counts cyber-attack as a serious as physical attack. The result of the summit is a declaration

[610] Ibid.

[611] DW, "Cyber Attacks, Energy Security and Terrorism – A NATO Perspective on Emerging Security Challenges in the 21st Century," *Deutsche Welle*, April 10, 2014, http://www.dw.com/en/cyber-attacks-energy-security-and-terrorism-a-nato-perspective-on-emerging-security-challenges-in-the-21st-century/a-17533087.

[612] Robert Morgus, "NATO Tries to Define Cyber War," *Real Clear World*, October 20, 2014, http://www.realclearworld.com/articles/2014/10/20/nato_tries_to_define_cyber_war_110755.html.

[613] Schmitt, "International Law in Cyberspace: The Koh Speech an."

[614] CCDCOE, *Tallinn Manual on the International Law Applicable*.

[615] DW, "NATO Moves to Apply Armed Conflict Law to Cyber Warfare," *Deutsche Welle*, July 2, 2014, http://www.dw.com/en/nato-moves-to-apply-armed-conflict-law-to-cyber-warfare/a-17754359.

[616] CCDCOE, *Tallinn Manual on the International Law Applicable* S1, R11, par. 9.

saying that Article 5 can be triggered as a response to cyber-attack and will be triggered on a case-by-case basis.[617] On the one hand, allied states will receive *cyber arsenal* to defend themselves as NATO wants to keep its priority in defending its networks, but wants to provide assistance to states in need stating that cyber-attack can cause direct physical damage.[618] On the other hand, states such as US, UK and Germany declined to brief NATO on their *cyber arsenals* openly saying to prevent other NATO members obtaining this information.[619] However, the result from Wales is clear in the way that cyber-attack may constitute allied retaliation to the adversary. This move is linked with the idea of reformulating Article 5 to include non-physical damage as an act of war. As a result of the Wales conference, media published a huge quantity of policy oriented articles such as the one titled *NATO Must Boost Its Cyber Defenses Now*[620] or the one coming from the US Secretary of Defense Ashton *Carter "NATO Must Bolster Cyberdefense before Addressing Cyberwarfare."*[621] Some articles circulating in NATO are contributing to the discourse so harshly that raising emotional feelings cannot be avoided: *"NATO Tests Cyber-Defense Firepower to Combat Internet Terror."*[622] As Wales Declaration showed, cyber-attacks are at the highest concern of NATO and the circulating articles through the NATO bulleting strengthen the conviction of its need. The reformulation of Article 5 towards addressing a non-physical attack is one of the central topics[623] as cyber-attacks rival terrorism threat and thus cyber threat is now treated as being significant enough to trigger Article 5 according to Anders Fogh Rasmussen.[624] However, this raises some critical concerns; e.g. how can NATO retaliate if the enemy is a private company or a

[617] NATO, "Wales Summit Declaration" (Press Release 120, September 5, 2014), http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[618] Tim Ring, "NATO Members to Get Cyber War Protection," *SC Magazine*, September 2, 2014, http://www.scmagazineuk.com/nato-members-to-get-cyber-war-protection/article/369026/.

[619] Matthew Broersma, "NATO Set To Ratify Cyber-Defence Declaration At Summit," *Tech Week Europe*, September 1, 2014, http://www.techweekeurope.co.uk/workspace/nato-cyber-151717.

[620] Klara Tothova Jordan, "NATO Must Boost Its Cyber Defense Capabilities Now," *Defense One*, September 11, 2014, http://www.defenseone.com/ideas/2014/09/nato-must-boost-its-cyber-defense-capabilities-now/93836/?oref=d-channelriver.

[621] Lolita C. Baldor, "Carter: NATO Must Bolster Cyberdefense before Addressing Cyberwarfare," *U.S. News*, June 24, 2015, http://www.usnews.com/news/world/articles/2015/06/24/carter-nato-must-bolster-cyber-defense.

[622] Ian Wishart, "NATO Tests Cyber-Defense Firepower to Combat Internet Terror," *Bloomberg*, November 20, 2015, http://www.bloomberg.com/news/articles/2015-11-20/nato-tests-cyber-defense-firepower-amid-fears-of-internet-terror.

[623] ASP, "NATO Article 5: Collective Security in the Cyber Era," *American Security Project*, September 30, 2015, http://www.americansecurityproject.org/rethinking-nato-article-5-challenges-to-collective-security-in-the-cyber-era/.

[624] Ruth Green, "Cyber-Attacks Rival Terrorism Threat, Says Former Head of NATO Rasmussen," *Ibanet*, October 21, , http://www.ibanet.org/Article/Detail.aspx?ArticleUid=d4ffe859-ed9d-4f83-8ecc-919dac460e9f.

civilian? The other trouble comes from a lack of interest of states of Five Eyes.[625] NATO is living in a discourse of *cyber defense,* while some of its allies are focused on signal intelligence against these allies as unveiled by Edward Snowden. Ironically, allies from the group of Five Eyes are dependent on Snowden revelations to measure the cyber arsenal of their allies.[626]

[625] Jamie Collier, "NATO's Role in the Cyber Domain Is Unclear," *Cyber Security Intelligence*, November 6, 2015, https://www.cybersecurityintelligence.com/blog/natos-role-in-the-cyber-domain-is-unclear-775.html.

[626] Broersma, "NATO Set To Ratify Cyber-Defence Declaration At Summit."

5. CONCLUSION

This chapter showed the production of discourse within the national security community. I wanted to show the distinction between two different worlds; between technical facts of particular events and the policy reaction on that events. Technical experts can produce relevant reports on particular events, but these interfere in policy implications only occasionally. It is hard to argue that this is happening as a rule, but it is self-evident how the policy makers are overwhelmed with securitization discourse, while the serious technical characteristics are omitted in the analysis. This applies to every single important event that is used as an argument of emerging security threat from cyberspace. Aurora Test, and the negligence of Ukrainian sophisticated attack causing real blackout were used as some of the examples.

Policy makers are living in a bubble of circulating alarmist discourse. The quick switch from critical infrastructure to hybrid warfare as the pivotal cyber related threat after the Crimea annexation and the consequent debates that propaganda must be addressed as a violation of state sovereignty, while the same interference of other state is in Tallinn Manual clearly described as a non-intrusive event, only underlines how aim of policy makers are based on quick proliferation of discourse. Some particular events can quickly change perspectives and thus production of discourse, but the attention of the audience is of course oriented towards the authorities. However, on which assessments these authorities are making their decisions? One will say on their intelligence, however the reproduction of titles tackling *cyber terror,* dealing with *cyber war,* raising up *shields of cyber defense* in the age of *firewall* instead of Berlin Wall shows how the imagination of possible future in order to be able to tackle with newly emerging threats is continuously based on debatable fictitious imaginations of policy driven experts or any other experts publishing on internet. By the way, this correlation is completely wrong as firewall does not divide people in one nation. However, it does add a layer of seriousness on cyber firewall. These correlations are typical for authorities. We can remember once again Leon Panetta and his speech repeating words of so called *cyber terror* specialist Richard Clark about train derailment. These examples show how the overemphasized imaginations fill minds of people that are called to support our security,

while they misses technical realities, which cannot be omitted. Then the discourse switches quickly, when another use of information systems prove to be effective.

However, including non-physical activities into international law as a violation of state sovereignty, or as an action that can constitute use of force or right for self-defense are dangerous ideas despite the fact they can seriously undermine confidence of citizens to their governments. Accepting this new norm would certainly lead to escalation of a conflict. On the one hand, it is understandable that one of the most important role of leading persons is to motivate people towards the same objective. Simplified securitization is doing exactly this job. While the *simplifying* attribute of alarming discourse helps to stimulate the motivation of people appropriately, it does also aim on imaginative threats that are far from being realized; if badly interpreted or chosen. The case of Ukrainian blackout would serve as an example. Ukraine was one of the highest topics in NATO bulletin by the end of 2015, but the blackout somehow did not make it to the minds of authorities and thus was not replicated thousand times as other events were despite its crystal clear seriousness that would help materialize the more precise imagination of cyber war that would lead into a state of prepared normalized reaction.

This third chapter was written in a way to show how a particular group of people in high-ranking positions can seriously shape what are the objectives of national defense structures. The discourse of cyber war, cyber terrorist or cybergeddon gives content to the traditional conventional defense thinking, which these structures desperately need to preserve its existence. NATO was seriously discussing its objectives or its obsolete existence in the age after the fall of Iron Curtain.[627] *Terrorism*, *cyber security* and finally *cyber terrorism* is a new substance to the national defense and NATO policy. Ironical accent to this moment is added by mixing cyber defense with cyber espionage. Experts behind the PRISM operation have been conducting serious operations in time, when NATO was conducting a row of simulated exercises and still has not played a role in a serious attack on its member state. The lack of interest in sharing cyber capabilities (NATO call it *cyber arsenal*) between NATO allies only underline how states value

[627] Wallace J. Thies, *Why NATO Endures* (Cambridge University Press, 2009), http://www.cambridge.org/cz/academic/subjects/politics-international-relations/international-relations-and-international-organisations/why-nato-endures.

differently covert espionage operation and visible deterrent. In that perspective, national cyber defense discourse seems to live in its pure imagination aside the reality that can change with mature and secure technologies.

Finally, the mantra that international cooperation is crucial for tackling cyber related threats leads to harmonization of law systems as either intentional or unintentional side effects. Soon or later this approach will lead to emergence of a supranational authority despite the fact that integration of states in security matters of the most visible integration efforts in humankind history, the EU, has been the most difficult one and certainly will. Production of securitization discourse based on social construction of security threats, which are threats to national security, creates a threat to national integrity as well. We will probably not be witnessing cybergeddons, but we will be certainly witnessing how the discourse strengthening national security subsequently corrode national identities towards globalized world.

THE BIRTH OF CYBER AS A NATIONAL SECURITY AGENDA

1. KNOWLEDGE AND THE CONTEXT OF ITS FORMATION

1.1. Beliefs, understanding and the proliferation of hybrids

We have never been modern! How is that possible? We have developed so many new technologies that have made our lives easier, we understand processes in nature to that extent that we can predict weather we have developed political institutions that radical ideas such as wiping out whole nations have become, hopefully, harder, but still, we have never been modern, I would agree. Bruno Latour came up with the idea in his masterpiece[628] to show how networks of knowledge are deepening the complexity of knowledge, so the purification process is becoming harder and harder. Let me introduce the idea, before I apply it to the whole work. Bruno Latour is talking about two distinct processes that are needed to develop *modern critical stance*. The *translation* creates mixtures and bridges between both types of naturally and culturally created beings – the networks, while the *purification* is needed for the exact opposite process, for the ability to distinct between them and understand them as two distinct ontological zones. The ability to distinct what have been out there since ages and what is culturally created is, for Bruno Latour, the key for *modern critical stance.* Differing nature from human also reveal a discourse *"that is independent of both reference and society."*[629]

He argues that science students usually do only the first part, *the translation*, but the inability to detach the cultural layer from scientific facts in the second part called *the purification*, or the lack of incentive to do it, drive them to the inability to distinct what is science and what is culture. That have tremendous consequences; the idea can be easily applied to any political statement regarding technologies. Remember the analysis between the ferocious explanation of what can happen if we do not take any countermeasures against incoming cyberwar in the book of Clark and Knake and the technical analysis of the 2003 blackout. Both texts are completely detached. Clark's and Knake's book is not purified from their personal subjective insights, they construct a cultural perspective of the needed policy.

[628] Latour, *We Have Never Been Modern*.
[629] Ibid., 10–11.

It is interestingly visible on the divided concept of technological determinism. After the post-war enthusiasm of Vannevar Bush's policy, it divided into two antagonistic groups: the optimistic technological determinism and the pessimistic technological determinism. The division clearly shows how different approaches interpreting possible impacts of technologies to the society are culturally bound. Technologies do nothing without one's intention and intentions are culturally bound. Perspectives on current threats are created by the argumentation of people, by the established *field of concomitance* that resonate in the discourse, by the creation of new *fields of truths* that emerged as *churches of knowledge* nobody dares to argue. War on Terror after the 9/11 became a lever to push other nations together, but also against others in the *Coalition of Willing.* It created the others and a norm of appropriate behavior as it is unacceptable to keep terrorists conduct their tremendous and cruel actions; however, some scholars later argued this policy – the discourse around the War on Terror – has constructed the terrorism itself, the appropriate behavior, the appropriate reaction and the final ideal state.[630] Similar cultural processes can be distinguished within reaction on the development after the optimistic technological determinism despite they are thematically far from itself. It was an argumentation what role the technology can play in our lives and the subsequent debate of its societal impacts.

In that perspective, I argue that it is not the critically analyzed and unveiled intention, but the cultural cloud over technologies what drives the policy of cyber threats. Cyber is the problem, they said, not the intentions. Intentions are taken as granted: who has the possibility, the capability and the opportunity has a chance and will act. Intentions are taken as the opportunities lying in unsecure technologies, so intentions are understood as the implication of the opportunities. It is hard to sue intentions, so they are taken as granted, as an inevitable outcome from possibilities provided by technologies. However, the insecurity of communication technologies can be fixed by adopting more mature technologies; ironically very often thanks to technologies developed by crypto-anarchist communities. Policy makers should stop talking about undisputable cyber terrorist intentions in the near future, when no statistics of cyber

[630] A Hodges and C Nilep, *Discourse, War and Terrorism*, Discourse Approaches to Politics, Society and Culture (John Benjamins Publishing Company, 2007).

terrorism is available, and start working on more mature technologies with the communities. State is made by people, the detachment of state authorities from highly capable communities will create resistance.

It seems we experience two realities, the imaginative one about cyber terrorism on the side of policy makers and the technical one, when more mature technologies are under development. It would be really interesting, if we could observe the day in 50 years and see the last 50 years of technological development towards more mature and secure communication technologies. This direction of development is inevitable and if so, the future cyber terrorist will have much harder task to conduct an attack and the current panic policy may be gone. Nevertheless, there is not a judgement day as it was in the case of Y2K. The question whether this technological development towards more mature and secure technologies will be governed by nation states still prevails.

However, the debate has been lasting already for decades as the imaginative ideas of cyber terrorism had existed in the national security discourse even before the Estonian events in 2007,[631] technologies are still insecure and we have not observed one significant cyber terrorist attack and if there is a sophisticate cyber-attack against electrical grid, no serious resonance of that event is visible in the biggest alliance in the world. This alarming policy also confuses balanced risk calculations as they are driven by possibility. The low attention on the analysis of the intentions behind the possible cyber-attack puts forward just a mere probability as an indicator and thus fulfills simplified requirements of possible operation reaching to a cyber doom scenario.[632] This has not changed too much in recent history, cyber doom was a question since the invention of internet, but has never materialized into national defense as it has recently. We need to unbound the cultural layer of our threat assessments and be able to assess threats in their factual possibility; we need to purify the analysis from the cultural layers, in this case, from the layer of tacitly existent cyberpunk imaginations. The reflection of technical assessments should be seriously taken into the discourse; however, how this is possible

[631] Michael Stohl, "Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?," *Crime, Law and Social Change* 46, no. 4–5 (2006): 223–38, doi:10.1007/s10611-007-9061-9.

[632] D. Barnard-Wills and D. Ashenden, "Securing Virtual Space: Cyber War, Cyber Terror, and Risk," *Space and Culture* 15, no. 2 (2012): 110–23, doi:10.1177/1206331211430016.

when expertise can be easily policy driven or ordered by political decision makers remains unclear.

In another work, Bruno Latour, builds this perspective on a weather forecast.[633] A genius example as weather forecast cannot be based on pure facts, which are then put into a calculation model that produce 100% certain forecast. The prediction models rather draw a red line through the most probable events in forthcoming weather development; however, as each moment in the atmosphere can cause a huge chain of consequences and they do, the prediction must be affected by people's imaginations. This was at least the final interpretation after the 30s once television news had to provide insight into the future weather. The causal link is dependent on an enormous number of variables. Each increases needed computing capacity exponentially and make the forecast more reliable, but the reach of absolute certainty is impossible – similarly to Zeno's turtle. However, we were predicting weather also before having weather satellites or any primitive weather measurement technologies. The cultural line over the infinite fractal weather model is inevitable. Hence, for Bruno Latour, weather forecast must include a bit of *beliefs* about the weather and some general *knowledge* of weather development.[634] Weather forecast started as a discipline based on beliefs of one's observation without no technology available centuries ago; that has changed much, but the cultural layer of final forecast remains. Subjective beliefs can sometimes even today win over the objectively observable knowledge. In a weather forecast this is due to the infinite fractal character of variables' influence to the overall model; the number of variables is infinite, looks like a fractal. Belief of experts become relevant, it is authority with a final word and will never be eradicated from the forecast process as we cannot reach the absolute certainty. In fact, we have a threshold of preciseness that is needed for our personal planning; hence, the absolute certainty is not needed and the subjective interpretation of incomplete data is desirable solution. The cultural layer will never be unbounded.

[633] Latour, *Science in Action: How to Follow Scientists and Engineers Through Society*, 181–182.
[634] Ibid., 182.

The inability to detach the cultural bound from science is in Latour's early work understood in accordance to impossibility to avoid cultural influence of science; the process then as a proliferation of hybrids, in his words the *"proliferation of hybrids has saturated the constitutional framework of them moderns."*[635] In his meaning, the horizontal axis is the process of purification, while the vertical axis, as it is getting further from the horizon between nature and society, between science and culture, hybridizes deep into the abys of a non-modern dimension as the process of *translation* becomes more complicated. This is the problem of complexity of scientific facts, of the continuous technology development. The inability to detach the cultural bound of that development and research leads to the abyss of possible mediation, of existence of being – the cultural being. As the horizon is the essence of nature and society, the abyss of mediation gives birth to the one's existence.[636] The existence is not possible without non-modern existence, without culture; seeking for scientific truths has been performed, but never achieved[637] and thus, *we have never been modern*, we cannot perfectly detach culture and purify these facts. The hybrids are inevitable, they are not human nor nonhuman, they are not society nor science, they are not facts nor beliefs, they are connecting points, of the observable, of both, of a process in which networks of things and people generate each other into a post-modern world, a quagmire of existence, of social being, of cultural, of everything mixed into one liquid reality. Inability to disentangle this puzzle leads into an unstable post-modern liquid world, in which the hybrids flow from the horizon into the abyss of the very existence, *which have never been modern.*

If we take this perspective, the reality of discourse formation I have discussed in preceding chapters cannot not be understood as a critical perspective that completely denies the processes of cyber policy formation. The critical perspective I proposed primarily shows how the particular cultural content plays a significant role in the cyber policy formation.

[635] Latour, *We Have Never Been Modern*, 51.
[636] Ibid., 86.
[637] Ibid., 144.

1.2. Technological radical uncertainty and its risk measurement

Baudrillard understands *radical uncertainty* in a relation to media production, to the production of vast number of articles, which are interpretative results of scientific facts; he is convinced that in the future we will never be able to separate reality from its depiction in statistics or simulative projections. That *inability* despite *will* produces *radical uncertainty*.[638] Deeping of this uncertainty looks very similar to the Latour's vertical axis between essence and existence, a post-modern existence, which enlighten another Baudrillard's argument with irreparability of this uncertainty by the *excess of available information*.[639] What kind of knowledge is deepened by repeated depicted threats of possible cyber doom? Only beliefs that are culturally bounded us together in the victim of the others who cause the situation. The same process is well studied in critical studies of terrorism.

I have been working throughout this dissertation with a concept I called *technological radical uncertainty.* The added value of the concept delves from the technological aspect. Technology is developed to reflect particular needs of humans that are achievable only through the technology or through better technology – better application of the technology. Better application means here, better utilization for human's needs and these needs are prevalently culturally driven. Hence, in the case of technology, in contrast to science, it is clearly visible that the social construction of technological projects is inevitable; similar to Latour's perspective proposed in his work Laboratory life regarding science.[640] The idea of objective should (but not need to) precede the idea of technological solution. However, the fact that the intention is critical in assessing possible security implications is clearly visible in the case of The Onion Network, designed by U.S. Department of Defense and exploited by criminals in doing business over Silk Road. The discourse is what creates a cloud of meaning above

[638] Baudrillard and Poster, *Selected Writings*, 210.
[639] Ibid.
[640] Latour and Woolgar, *Laboratory Life*.

particular technology[641] and it is discourse that shape our reflecting of technology if its application missed its intended objectives.

However, how to make a decision over particular technological development when democratic decisions can lead to technological paralysis and expert decisions to popular opposition?[642] Policy makers tend to overcome responsibility by changing mind of public to accept moves as rational, responsible and necessary according to national security. Then *truths* flowing from *churches of knowledge* in general and *truths* interpreting previous events build on *metaphors correlating* with *constructed analogies* consequently lower the impression of risk we take while adopting particular policy. Nevertheless, will we be able to judge such policy of imaginative threats one day? One of the biggest trouble in taking critical perspective on cyber security discourse is the absence of the judgement day. The day we had in the case of Y2K, so these who were intensively working on spreading panic worldwide could apologize as I discussed in the introduction. The circle of repeating adopted truths imprinted to rationality of adopted policy creates conviction of acceptability of taken policy and mediate public concern related to the taken policy. Social construction of both, the scientific facts and the related policy emerge.[643] They exist in their own world of knowledge*. It is a combination of constructed analogies on national security level based on empirical evidence in cyber crime and mystified by geeky culture with colorful depiction in cyberpunk.*

The distinction between knowledge, beliefs and discourse is hard to identify. When discourse actively creates new correlations underlining rationale, these correlations fall into beliefs of policy makers who produce the discourse. Experts' impressions are taken as knowledge, the same dynamics we discussed with weather forecast, applies to construction of expert knowledge. Complexity, non-linearity and policy driven technology inventions are widening the incomprehensibility of its development, which is the spark of *technological radical uncertainty.* Computers has had since their beginning a special aura of being understood by special people only; geeks,

[641] B. Wynne, "Risk and Environment as Legitimatory Discourses of Technology: Reflexivity inside-Out.," *Current Sociology* 50, no. 3 (2002): 459–77, doi:10.1177/0011392102050003010.

[642] Collins and Evans, "The Third Wave of Science Studies: Studies of Expertise and Experience."

[643] Irwin, "Constructing the Scientific Citizen: Science and Democracy in the Biosciences."

those who govern the digital world. Some of them later gather in epistemic communities called crypto-anarchists, libertarian socialists or anarcho-capitalists according to their personal values. As expertise required for policy decisions is moving strictly different direction than expertise driven by curiosity, states cannot be step ahead of hackers in such technological development. It is not a requirement of state institutions to be a curious geek seeking how to disentangle systems around to find a job in cyber-security institutions. Their expertise is much more devised from the loyalty to the nation state, especially in security sector, rather than from their knowledge and ability to look through to the center of the problem, the Latour's ability being close to modern avoiding traps of hybrids. There are voices calling for building bridges between *us* and *them*, states and hackers who possess enormous power even when they are young and are curious to disentangle systems without criminal intentions,[644] but these are rare and not visible in nation state policies.

Moreover, the ability to be close by the experts in nature sciences or engineering do not need to be accepted as a reasonable argument when policy needs visible results as we observed e.g. in the investigation of Challenger Space Shuttle disaster.[645] The resonation of Challenger and Columbia disasters is visible in currently adopted no-failure policy of NASA that burdens its technological development in order to achieve some meaningful results in human space flight.[646] The case of the European Environment Agency as a typical example of a translation of scientific knowledge to environmental policy shows dilemmas how objectively observable knowledge is translated into policy recommendations, that are based on particular beliefs as they simply cannot meet the Latour's perfect modernity of socially detached facts about nature.[647] It is simply not possible to cover all the variables. The effectiveness of such institution is based on resonation within public. If they are too forceful in adopting environmentally friendly policies that clash with people's interests, public annoyance with their activities will lower their social acceptability with no regard of positive impact to the nature and thus

[644] Lauri Love, "As a Hacker, I Know How Much Power Some Teenagers Have - We Need to Start Building Bridges with Them, and Fast," *Independent*, May 9, 2016, http://www.independent.co.uk/voices/as-a-hacker-i-know-how-much-power-some-teenagers-have-we-need-to-start-building-bridges-with-them-a7020331.html.

[645] Harry Collins and Trevor Pinch, *The Golem at Large: What You Should Know About Technology* (Cambridge University Press, 2002).

[646] Robert Zubrin, "The Case For Mars," 2012, doi:10.1016/0019-1035(85)90164-2.

[647] Jasanoff, *States of Knowledge: The Co-Production of Science and Social Order*.

undisputable impact of human survivability. If authorities propose subsidies of better isolated windows leading to energy savings, they would be welcomed with hug. This trouble with populism is in security matters solved by the imagination of possible dooms giving rationale to any adopted policy; policy seems to precede the analysis as the threat is expectable. Risk calculation does not play any role.

Expertise in cyber security fits policy agenda, not vice versa. It is a special role of national cyber security expert who can deal with these new threats. Taking the co-production[648] of natural and social knowledge and perceiving the security as being a co-produced hybrid between natural facts of technology and societal imagination of its usage is what gives the risk assessment completely different layer of reflection. U.S. Department of Homeland Security approaches the security of critical infrastructure by reminding the corporations that security is not given, but must be preserved; the DHS is convinced that corporations running critical infrastructures are motivated by profit and thus they preserve security to keep the systems running without needed state intervention, only through support and encouragement to develop more secure technologies.[649] The state policy, in that case, seems to be detached from the technology invention. However, it has to be policy to keep systems running within the corporation. The argument of DHS is based on a conviction that policies of corporation and state in consent work better than policies in conflict. The conflictual policy is the one, which requires a change to the policy of the corporation, while the policy of consent is the one that encourages the corporation policy to do the same. Both policies would be the same from the general security perspective, but who is shaping the policy on the lower level when a particular technology is given green and the other red light within huge corporations? Knowledge-making is thus inseparable practice of any policy, either state-making policy or corporate-making. In general institution-making policy, however, the loop-back works as well, as it is also the state-making process that influence knowledge-making.[650] Nevertheless, the point is that consent between actors is productive, while conflict consumes time to explain why each actor prefer particular position. And here we come to the point. The idea that state

[648] Ibid.
[649] Based on an interview with Michele Markoff, deputy coordinator of cyber issues. July 2013.
[650] Ibid., 3.

is enforcing policies only to serve people would be naïve. It is the most common clash in democratic societies, the clash between liberty of individual and security of social. Whereas policy of individual liberty lowers power of the state, policy of national security strengthens power of the state. The policy approach by DHS strengthen both and reduce the non-modernity in Latour's terms.

In that perspective, the detached expertise from policy is an unachievable ideal, nothing we can take seriously. The modernity is an unachievable ideal. Distinction between expertise driven by curiosity and expertise driven by policy might be fictitious as some cases seems to be pure production of illegitimate knowledge (case of Patterson) that helps business interests, while the other helps health interests. Then, which knowledge is legitimate, what is a good science? We have seen exceptional cases in which scientists were able to preserve their credibility by detaching themselves from policy.[651] Morale gives hint here, but nothing more; however, morale could be understood also as expertise to protect things, species or human dignity[652] and as such it is clearly a product of culture. Hence, totalization of objectivity of expertise cannot be understood as desirable and thus it is all not about the problem of cyberpunk role in the cyber security policy formation; it is clearly about the policies of consent between the actors involved in the post-modern quagmire. However, we have seen exactly opposite situations, which are usually easily found in the pharmaceutical business operating in *ring-fences* of reproduced knowledge.[653] When it comes to expertise required for immediate security concerns, experts might be under pressure to produce results that will smoothly go through the policy intended to be adopted as soon as possible.[654] The ideal does not exist and cannot be reached and motives of particular policies cannot be detached from cultural and moral imperatives.

Expertise completely detached from policy is hard to achieve if not completely unachievable; finally, it is not desirable. When there is not enough empirical evidence, we

[651] Sheila Jasanoff, *The Fifth Branch: Science Advisers as Policymakers* (Cambridge, Massachusetts: Harvard University Press, 1990).

[652] Francis Fukuyama, *Our Post Human Future: Consequences of Biotechnology Revolution* (New York: Farrar, Straus and Giroux, 2002).

[653] John Abraham, *Science, Politics and the Pharmaceutical Industry: Controversy and Bias in Drug Regulation* (London and New York: UCL Press and St. Martin's Press, 1995).

[654] Nowotny, "Democratising Expertise and Socially Robust Knowledge."

could expect more culturally influenced policy as the call for preventive action drew on doom consequences raises on its relevancy by adopting correlative analogies as facts. The desirable policy would be to draw these analogies well-balanced to develop secure technologies, but to avoid filling the discursive space with only one possible threat.

1.3. Social construction, semiosis and discourse

Social construction provides us with insight that the world out there is not given rather it is socially constructed through speech acts;[655] the social construction perspective made us a relationship between the object out there and our reflection of it in words. Words, thus, do not represent the reality itself, but a reality imprinted in *signs* words represent. If Pearl Harbor makes an emotional resonation in U.S. nation, using the name of the harbor in order to deepen attention on security threats from cyberspace adds a sign to whatever one says. No real threat, rather real fear based on particular experience without rational connection to today events, is what drives others to pay attention. This is what Ferdinand de Sausser understood as a difference between *signifier* and *signified* that the sign they produce by *signification* is the content behind the word. It is distinct in different languages,[656] but the *signifier* can be transferred to other *signs* giving a specific language driven content; signs are the *content of meanings*. Words are inherently empty; the addition of the content to the words is contingent as they *constitute signs*, but as they are, they produce *contingent relationship between signifiers.*[657] My perspective is that the *church of knowledge* produced by *cyber experts* in the field is a process narrowing this contingency. The *meaning-full* claim in the field is then much more related to other comparable statements of cyber security discourse, which in the repeating circles produce unbeatable *dictums* of truth. *Meaning-full* statements are not related to reality out there (remember the case of blackout in 2003 discussed on the page 195) they are

[655] Matt McDonald, "Securitization and the Construction of Security," *European Journal of International Relations* 14, no. 4 (2008): 563–87, doi:10.1177/1354066108097553.

[656] Johnathan D. Culler, *Ferdinand de Saussure*, Cornell Paperbacks : Linguistics, Literary Criticism (Cornell University Press, 1986), 138.

[657] Charlotte Epstein, *The Power of Words in International Relations: Birth of an Anti-Whaling Discourse* (Cambridge University Press, 2008).

articulatory practices producing discourse; a product of a *political articulation*, which certainly has implications on real events.

The contingency is critical in understanding why implications in discourse analysis cannot be approached as a positivist implication of cause. I do not want to show that the discursive practices are the only explanation of cyber security politics production. I would rather answer the classical criticism of post-structuralist approaches[658] by adding the explanation how certain discursive practices imply real events, because they are based on a shared *perceptual field*. Attacks are real, implications are real as well, but they are not related to the politics production as we can observe it from the first hand. The corpus of knowledge surrounding current national cyber security agenda is giving vindications to particular political moves. Explanation of these moves aside what seems to be ordinary action by a nation state in order to deliver security is my research objective. Unveiling powers of discourse as implication to particular events might be criticized as a detour from epistemological perspective, but this move was taken also to avoid criticism that the discourse analysis equals to *"relativism, nihilism, nominalism, solipsism or subjectivism"*[659] as the poststructuralists are usually criticized, but also that the clear Foucauldian focus on discourse as a power was not enough to depict these processes. Of which I wanted to find a relation between the three discourses: the skills covered by the ideologies giving them additional content, motivation and implication, the field of crime giving the discourse empirical evidence and the field of national cyber defense focused strictly on imaginations (see the Table 1 - Perspectives taken in the following three discourse analyses).

Different perceptual fields taken from different theoretical and scientific disciplines and practices of national security overlap to produce one perceptual field of national cyber security. They influence each other to later delimitate their own space in one resulting perceptual field and then the new one sue any critically oriented questions as being asked without proper expertise or being totally blind to the truth, because if ignored, everything may transform into Cyber World War III. Repetition, transformation

[658] Clayton W. Dumont, *The Promise of Poststructuralist Sociology: Marginalized Peoples and the Problem of Knowledge* (State University of New York Press, 2008).

[659] Ibid., 3.

and reactivation of unimportant historical events or emotionally shaking game changing historical events by discourse form new reality of serious national security concern. New concepts are produced to delimitate new strategies against constructed threats in the perceptual field of newly respected experts. As seen, the evolved discourse has been born on *analogical historical correlations* rather than on an assessment of current events that are happening.

1.4. Corpus of knowledge and the beginning of beliefs

For Michel Foucault, perceptual field is a corpus of knowledge that presuppose the way of looking at things.[660] Before we can practice any skills in the same way, someone has to put all the observations, methods, techniques, used instruments, classification of information or relation to other theoretical domains into one cohesive corpus of knowledge we understand as the best practices. Healthcare, weather forecast, building a rocket, governing a state, all of these skills requires its own very special cluster of skills, but also institutions to teach them, analogies to show comparable examples, authorities to let them decide and evolve the field of knowledge we work in. Perceptual field is a system in which skills, authorities, institutions, correlations, analogies, statements and concepts are used in a specific linguistic system applicable to the particular field of human knowledge. Concepts are used in a particular relation, *cloud* means something else in meteorology than in computer science.

I was wondering about dynamics in several dilemmas. First, how is it possible that something like a DDoS attack on some companies and administrations in Estonia could spark an enormous interest into something *possible?* Second, if that spark could keep itself alive for years, finally already a decade, what has driven it to deepen, widen and brighten during that time? Third, if the fear seems to be so real and people you talk to on each cyber security conference around the world are shockingly, vigorously and ferociously explaining how extreme threat this is while there are no burning cities around, what drives these people to believe the others? Fourth, along this panic around

[660] Foucault, *The Archeology of Knowledge*, 36.

there are still people who would like to answer questions with a bitter but sober tone[661] focusing on solutions to current cyber security troubles that have measurable impacts – no comparable attack would cause the same and thus no reason to deepen the fear. Fifth, as I mentioned several times, cyber security as a national security agenda do not have a judgment day as we had in the case of Y2K. This fact helps the securitization discourse deepen without restrictions, what does that mean to possibility to narrow it to a sober approach? Sixth, if there is still a driver despite statements such the one from Estonian Ministry of Defense that comparable attack to 2007 would not cause simply nothing today, what fuels this driver? Where is the source of the fear?

[661] These feelings are coming from personal interviews with particular people. I would mention those:

James Lewis at CSIS, Washington DC, who like to take a look on statistics in real economic loses or causalities while comparing other threats to cyber security threats.

Michel Markoff, a deputy chief responsible for cyber security at Department of Homeland Security, Washington D.C. is focusing on motivations of corporations and believe in their capability to keep critical infrastructures running. The policy is oriented on their support rather than on building walls around critical infrastructure that must be strong according to law.

Siim Alatalu from Estonian ministry of defense who openly told me that the DDoS attacks were a gift from a God as Estonia could become serious partner for NATO. The political implications were quite far more important than the real attack and that comparable attack would cause nothing today.

2. THE PERCEPTUAL FIELD OF CYBER SECURITY AS A NATIONAL SECURITY AGENDA

Thinking about the whole cyber security agenda from a perspective of these questions led me to a development of the below depicted figure of a perceptual field concerning cyber security as a national security agenda. Let me explain the whole logic, which is based on the Table 1 - Perspectives taken in the following three discourse analyses. I will summarize the core of my argument in the following paragraphs.

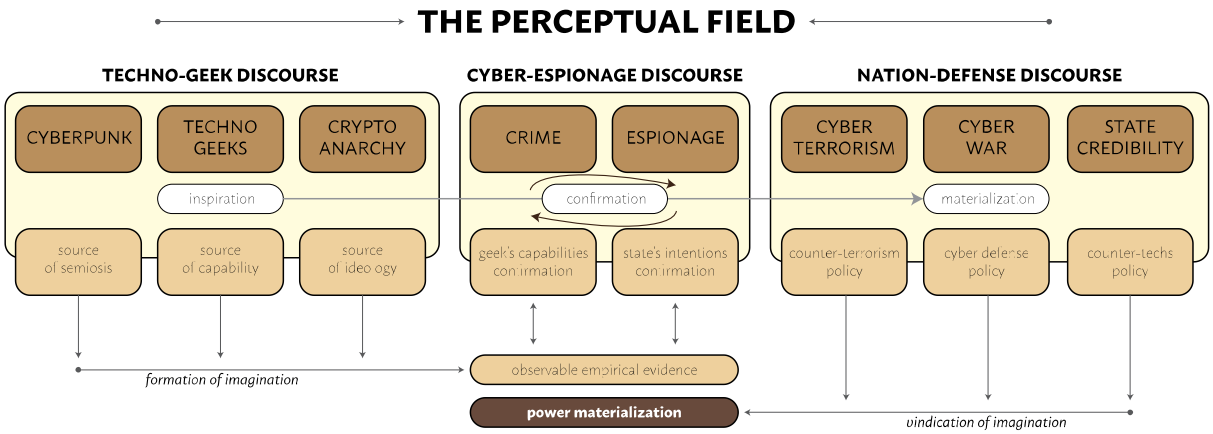


Figure 3 - The Perceptual Field of Cyber Security as a National Security Agenda

In that table, I showed the reason to choose three discourses, however, I decided not to approach them in a way that each will be studied in isolation, but rather in a perspective of its constitutive role of the entire perspective. The Foucauldian method was a methodological approach of reading these discourses as mentioned in their respective parts (see the chapter 4.7 Method overview); here the point is to put them into relation of each other and show the perspective of national cyber security discourse formation. I propose this perspective for your critical consideration.

2.1. Techno-Geek Discourse

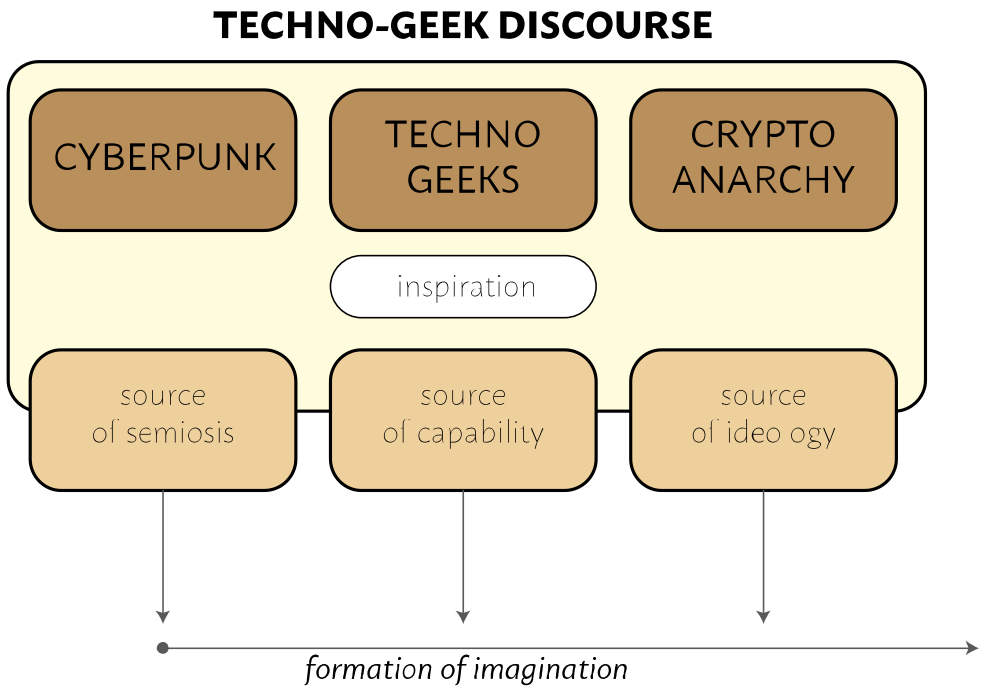


Figure 4 - Techno-geek discourse structure

Cyber-punk, geeks, crypto-anarchists, libertarian socialists or anarcho-capitalists. Although cyber-punk is a subculture full of a fictional world, it is an important source of philosophical thought dealing with rising power of technologies. The relation between one's liberty and global corporations, which do their best to make people dependent on their products or even addictive to their mind enabling drugs is certainly an exaggerated fiction as we would expect from science fiction writings. However, the relation between individual and the corporate, the ability of individual to stand against the powerful entity driven by neoliberal global capitalist ideas flattering our lives is very close to Baudrillard's[662] simulations or Bauman's post-modern writings about liquid society.[663] Cyber-punk is a source of *semiosis*, the whole vocabulary that was taken over by a nation state cyber security discourse. There has been a question heard in the last decade in the academic environment, why somebody switched terminology from *computer security* to a *cyber security.* I proposed an answer. Cyber-punk, driven by curiosity how to *steer* systems, is upgrading a mere computer security paradigm with a *man* and *intentions*. Who

[662] Baudrillard, *The Consumer Society: Myths and Structures*; Baudrillard and Poster, *Selected Writings*; Baudrillard, *Simulations*.

[663] Zygmunt Bauman and T May, *Thinking Sociologically* (Blackwell Publishers, 2001); Bauman, *Liquid Modernity*.

would talk about computer security without a man? Are computers our adversary? Fortunately, not yet, but as shown on example of DARPA's artificial intelligence patching exploits autonomously online we may be adding one more actor very soon. The addition of a man's intentions was needed to construct a rationale. A man, that possess power – *the power of a man over a man*[664] is what stimulates insecurity feelings.

Geek, a man that is able to disentangle every system causing fascination and fear of his/her capabilities to others (see 130), is a real entity in our world that is driven by cyber-punk dystopian visions of dark future he/she can avoid. Geeks exist, they are not in literature, they are significant part of cyberspace development. Laughing to faces of mere earthlings by running global search engines they show vulnerabilities of critical infrastructures. The demonstrations of capabilities of the search engine Shodan[665] are the moments when mere earthlings are hardly taking breath. The capability of a man-geek is visible everywhere. The whole world of invisible viruses and malwares deployable without our awareness is proving their capability every single day. Anti-virus companies talking about hundreds of thousands of exploits developed and spread every single day is deepening the fear and confirming their capabilities.

Finally, what drives the political agenda of geeks, the man rising from a dystopian world of cyber-punk, is the ideology behind movement of those people. The ability to stand against the system is coming from the capabilities geeks possess and will the movement formulate. Crypto-anarchy is filling the political gap of needed ideology to make cyber-punk dystopian depictions real by adding a political agenda to them. It is clearly written in the Crypto-Anarchist Manifesto (see Figure 2 - The Crypto Anarchist Manifesto logical structure)[666] what is the agenda and it is clearly observable how the technology development of particular technologies within this epistemic community has been developed in accordance to it in the last two decades. I also briefly mentioned other ideologies such as ultra-libertarians, sometimes called anarcho-capitalists; however, I approached those as renegades from the crypto-anarchy movement, as those who

[664] Arendt, "On Violence."

[665] Kashmir Hill, "The Terrifying Search Engine That Finds Internet-Connected Cameras, Traffic Lights, Medical Devices, Baby Monitors And Power Plants," *Forbes*, September 23, 2013, http://www.forbes.com/sites/kashmirhill/2013/09/04/shodan-terrifying-search-engine/#4100e5a5174c.

[666] May, "The Crypto Anarchist Manifesto."

decided to take the liberating technologies and make fortune on them. Silicon Valley is often called a lair of libertarians as these people found a way to be much more powerful than a row of whole countries worldwide. However, they are not too much driven by ideology as crypto-anarchists, they much more show how the liberating technologies can be so powerful and how they can liberate people from states when used massively. They also fulfil the predictions of cyberpunk writers when they spread these technologies contributing to the emergence of post-modern liquid reality where nobody governs, nobody is oriented, nobody has the central power. Nevertheless, the decentralization of power is the objective of all these actors I currently mentioned.

The techno-geek discourse is then encircling these three constitutive pillars. Whose perspective to take? Geeks or policy makers on behalf of governments? I believe that putting these two into a conflictual state make sense in reading both discourses, the techno-geek discourse as well as the nation-defense discourse. While some geeks driven by the ideology of crypto-anarchism (not all are crypto-anarchists) have their agenda clearly written, their goal is to liberate people from governmental power by developing liberating technologies. Bitcoin, encryption, TOR, torrents, CryptoNet in the eyes of geeks and DarkNet in the eyes of policy makers, but also services such as AirBnB or Uber are showing how the ultra-libertarian agenda seeking for a world without a super-authority, a nation state is not a complete fiction, but at least a fulfilling fiction that is proliferating to our everyday lives. Statements in the Declaration seeking ultimate liberty are visibly conflictual to the very principles of a nation state. The steady *repeating* argumentation about oppression by the state within the community deepen the belief that fighting the nation state back with liberating technologies is an inevitable fate of every geek. Crypto-anarchy gives political agenda to the geek community. However, geeks should not be understood as an epistemic community, whereas crypto-anarchists clearly are. Statements such as *a state system is hostile, does not possess sovereignty, we never sign social contract, we will create Mind of Civilization, we do not need laws but auto-regulative technologies, privacy will be sacred, the switch from iron revolution to information revolution is ongoing, ultimate equality is emerging* are all the core ideas creating the inner perceptual field of crypto-anarchist epistemic community. The discourse produced within these three pillars (cyberpunk , geeks, crypto-anarchy) has certainly a constitutive

role in a creation of particular online authorities, let's name one – sourceforge.org, a community for all open-source developers, bring millions of people together is certainly an example of global epistemic community;[667] however, as said, not all geeks need to be motivated by the same ideology.

Their authorities are decentralized, but powerful by inspiration (Anonymous), online reputation principle has proliferated to commercial world and already gave kind of liberty to common people, which is the proof (for them) that their efforts are successful. Statements about nation state hostility are repeated in every single occasion, on conferences organized by Institutes of Crypto-Anarchy, hackers' communities or computer scientists. Respected people by the community are giving them "proofs": Snowden and Assange are geeks; both are computer scientists. The surveillance machine enabled by technologies is giving more motivation to the community to develop technologies that encrypt all communications without encryption authorities. It is for certain that future will be devoted to better encryption without a central authority as there are two critical arguments. The first argument is the fact that a central authority can be hacked (DigiNotar example[668]) and leak all the keys. The second argument is that peer-to-peer encryption cannot be accessed by any authority. If states are going to be blamed for developing a surveillance machine ordinarily, we should be assured that these technologies will only spread more quickly. The result is not desirable for anyone as shown on the case of DHS. The conflictual policies will produce only a deeper conflict and will give power to raising resistance.

If we take an easy leap, crypto anarchy provides a source of ideology that is through *signs* inscribed in its source of semiosis, in the cyber-punk subculture. Geeks are drivers of these signs by their capabilities as they fulfill the ideas by particular acts. As a whole, the epistemic community of crypto-anarchists are making an alternative to a global governance model that is driven by the technologies invented, built and funded by

[667] Adler and Haas, "Epistemic Communities, World Order, and the Creation of a Reflective Research Program."

[668] Rid, *Cyber War Will Not Take Place*, 2013, 26–32.

these *weary giants of flesh and steel*[669], in fact by nation states,[670] which crypto-anarchists are so keenly willing to topple down. In that perspective provided by Morrison[671] their visions are utopic, but as well visible through out popular journalism or personal website of respected geeks who behave in line of crypto-anarchism.

2.2. Crime-Espionage Discourse

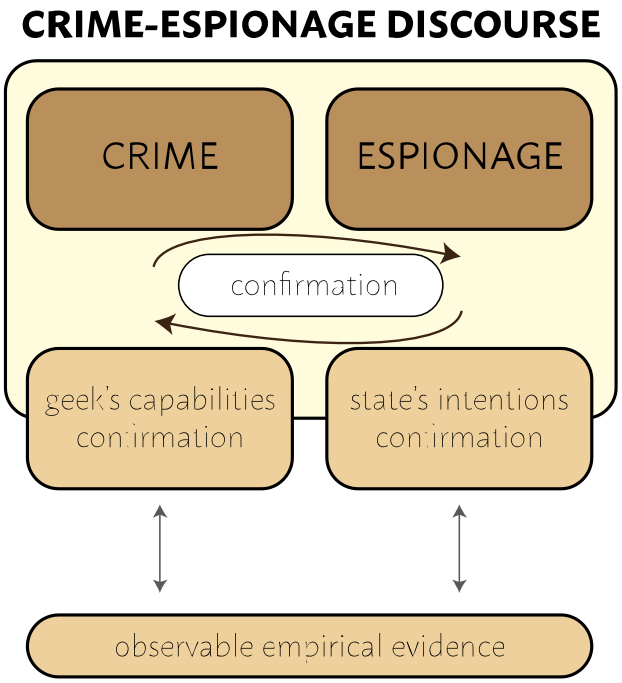


Figure 5 - Crime-Espionage Discourse structure

The measurement of cyber crime impacts is tricky as you could see in the empirical part (see the chapter The blurred empirical evidence and its (mis)interpretation on a page 152). However, there is a consensus of rising events, e.g. in number of ransom ware cases that are reaching more and more people every year without a capability of law enforcement agencies to do anything seriously against it. Cyber crime is a strong argument for those who think that states should possess more power in cyberspace to be able to tackle with the new kind of crime. Statements about the seriousness are usually enchanted by adjectives enlarging the power of cyber crime groups: *cyber crime global empires,* or using word enchanted by emotions – *lords of*

669 Barlow, "A Declaration of the Independence of Cyberspace."
670 Morrison, "An Impossible Future: John Perry Barlow's 'Declaration of the Independence of Cyberspace.'"
671 Ibid.

cyberspace or the switch giving the name different more dark connotations, switch from *CryptoNet* to *DarkNet.*

The evidence of cyber crime, the fact that the capability of geeks is projected into lawless actions that are happening and that the impact of single attacks on banks can rise to billions of dollars is naturally shaking with policy makers. However, one of the most recent example in Bangladesh, in which hackers were close to steal almost a billion of dollars, show how these actions are taking place due to incapability of particular computer security administrators and thanks to specific knowledge of the attackers.[672] It is important to understand these attacks in the light of particular technological glitches and human errors, but they are approached as waves of new knights in cyberspace instead. As cyber crime produce evidence, which is evaluated in financial loses that vary from real amount of money stolen to very debatable economical loses due to software piracy, it provides policy makers a confirmation concerning the *real* capabilities of hackers. No regard on specifics of particular attacks. The one from Bangladesh is not confirming rising capability of cyber crime empires, but shows that somebody very well oriented in the SWIFT system could alter it in order to follow the hacker's intentions. On the one hand, the electronic transfers lower the risk of millennium thefts of gold in the train coming from mountains down to the cities with mined gold; on the other hand, it rises the risk of theft over wires, but that requires very specific knowledge. One needs a very specific imagination to understand it as a disaster of burning cities. Crime is taking new opportunities emanating with new technologies and understandably some of them are becoming global with very well organized management system. Criminals are exploiting the state of unpreparedness on the side of banks due to lack of empirical evidence, which banks can use to secure them. It is expectable that banking systems will significantly more secure in the near future that they were at the beginning of electronic transactions from our homes. Nevertheless, state authorities see these criminals as raising empires that threaten our liberties.

[672] Jim Finkle, "Bangladesh Bank Hackers Compromised SWIFT Software, Warning Issued," *Reuters*, April 25, 2016, http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR.

Cyber crime produce evidence that can easily support the imagined knights or lords of cyberspace in their empires of dystopian cyberpunk lairs. "*Few clicks"*[673] are everything what one has to do to become fabulously rich. Evidence is coming from all sources, usually from the ones who possess authority in the expert field such as Kaspersky Lab, McAfee, Avast, Eset, Crowd Strike, Mandiant etc. Precisely from all the companies that are making money on deepening fears of cyber crime. As these companies are reacting on cyber crime, sometimes giving us a notification in upper right corner of our monitors that they have stopped "245.489" attacks just today; they are gaining respect to produce new respectful knowledge and expertise. Who understand the security of our computers better than the anti-virus companies? One may ask this questions while reading advertisements all around the world wide web. They have also become anti-malware, internet security, cyber defense or cyber security experts. The raising number of attacks creates *field of truth* that these authorities have the right to create a specific *church of knowledge* as they beat the cyber crime on a daily basis with certain success*.* They have become authorities as they are experts that have the logical right to introduce us into the dark areas of cyberspace they understand as nobody else. The good geeks.

The statistics are interpreted in a *successive series* as a multiplying proof of newly emerging global crisis. Sometimes even interactive suggestive tools of live numbers about online theft, today stopped attacks or current ransom required globally are shown in advertisements by antivirus companies. The number of cyber crime events, which is rising to enormous numbers, provides fuel to the discourse that is in the interest of states as these proofs gives the rationale to build more robust cyber defenses. However, one may raise a question why states are not inviting these companies in cyber defense operations when they are making contracts with these companies to secure systems running critical infrastructure? However, the argument is that state must possess its own capacities to defend the state. This moment raises an interesting perspective as all the claims on the discourse formation and its implications are easily debatable, the question why states do not tend to defend critical systems using these companies, but settle

[673] The~Economist, "Hacking the Banks."

contracts with companies experienced in national defense (BAE)[674] is not sufficiently answered, but it might be answered by BAE's motto*: "It's not just security. It's defense."*

In the empirical part, I discussed that some cyber espionage attempts or successful operations do not need to be treated as nation driven espionage. I argued that some massive cyber crime campaigns are switching to the category of industrial espionage because the attackers aimed on systems that are marked as critical infrastructure. State thus understand attack on these system as espionage rather than a mere crime; first of all, as other states might have interest in data of critical infrastructure. However, the line between crime and espionage is blurred. It is the discursive marking that easily rises the perception of these attacks as espionage despite the fact that they should be treated as crime, especially when the state involvement is seriously hard to prove – the attribution problem. The fact that something is interpreted as espionage is clearly discursively driven as proving state driven espionage is simply impugnable. The repeated attacks on critical systems, the fact that geeks operate search engine on vulnerabilities of critical infrastructure devices, the fact that geeks are stealing money and can make money by stealing information related to national security are all arguments why crime is becoming a national security concern.

There are allegedly two enemies to a nation state. Geeks and the other nation states conducting espionage. Increasing non-state actors' capabilities proved by the cyber crime statistics is giving argument to a nation state why particular security oriented technologies should be introduced and why we should understand anonymity online as something else to our privacy online. This rising hackers' capability is also giving an argument to policy makers that states will be able, and are currently willing, to steal all our knowledge. The evidence of cyber crime gives rationale to the necessary evidence of espionage and thus gives rationale to treat crime as espionage, which is consequently giving rationale to establish new national security institutions that are clearly materialization of power in hands of a nation state. The fact that states are not able to deal with certain rising cyber crime threats to citizens (ransomware example) is leaving

[674] "BAE Homepage," 2016, http://www.baesystems.com/en/cybersecurity/feature/it-s-not-just-security---it-s-defence-.

state security administrations in a position of a need to socially construct or discursively bend the criminal reality into the perspective of rising threats to a nation state in shape of a rogue state espionage. This process is the contribution to the *perceptual field* that builds on the established *church of knowledge* producing new *hierarchies of authorities.* However, the materialized result in new power is international surveillance monster, which does not follow interests we would expect from a liberal democratic nation state.[675]

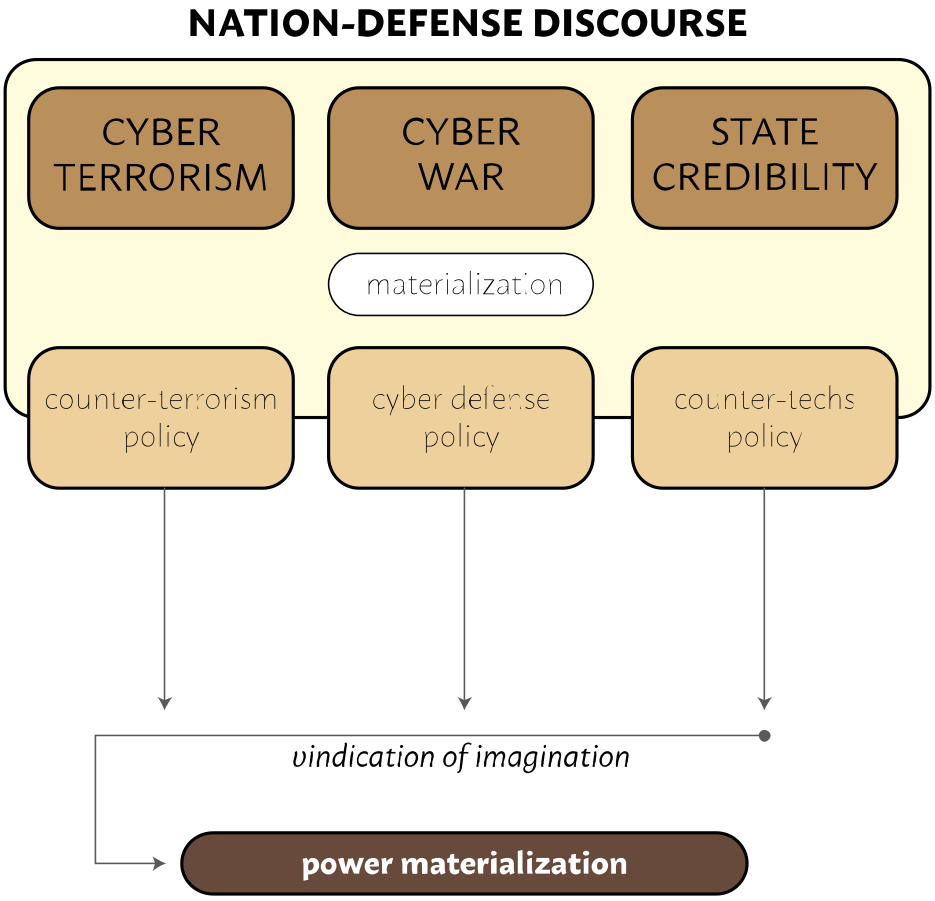
At this same time, the liberal West was caught in the middle of shocking massive surveillance operation PRISM, which dispute the principle of social contract in the eyes of citizens supporting liberal democratic political system. Result of such revelation would be nothing serious than quicker proliferation of liberating technologies securing privacy of citizens and hampering nation states to conduct espionage or tackle crime, which they are expected to beat. However, the result is not only a *lower ability* of a liberal democratic nation state to tackle cyber crime by inability to adopt appropriate counter-crime technologies in the eyes of its citizens,[676] the more important results is a *lower credibility* of a liberal democratic nation state as a principal authority at the international level. These implications do not need to be visible immediately, but the mood in global affairs has utterly certainly demonstrated in last years that the western-type of liberal democracy is not currently the most desirable regime people globally strive for. Authoritarians are gaining undisputable credit in the eyes of voters even in the liberal democracies and the reason would be found in all events that undermined the very principles of liberal democracy. PRISM and Panama Papers are certainly part of this decadence.

However, crime has to become espionage to rise the argument of a needed new powers in hands of states. This is trickier than ever as states incorporated private corporations in surveillance operations that operate globally and certainly do not have interests in national security – and liberal democracy. Some libertarians think that world without governments would be more secure and these are certainly coming from places such as Silicon Valley, so where all the giants of cyberspace, giants that found a way how

[675] Bauman et al., "After Snowden: Rethinking the Impact of Surveillance."
[676] Jasanoff, *States of Knowledge: The Co-Production of Science and Social Order*.

to make money in cyberspace, are situated. Liberal nation states are caught in their own trap that is irresolvable as they cannot leave the monstrous surveillance machine to private corporations to be used for business purposes. In that case, the darkest cyberpunk nightmare where corporations reign would become reality. The circle between crime and espionage (as shown in the figure) is confirming the depicted reality by evidence, which is consequently reproduced by discourse, which consequently produce new environment that is hostile to the principle of a liberal nation state. An environment in which the liberal nation state is not delivering needed security to citizens, who would rather buy it from antivirus/malware companies, from those who adopted liberating technologies produced by geek community. This process shows lowering confidence to a liberal nation state to the extent that is incomparable to 19th-20th century nation state centralism. States need to act in order to address novel threats of cyberspace citizens allegedly cannot deal with and *nation cyber defense* is the key in their eyes.

2.3. Nation-Defense Discourse



Now we have the striking evidence of *the geeks' capability* and *the nation state espionage intentions* paradoxically confirmed more by the liberal democratic than authoritarian countries. Liberal democratic states found themselves in a mess of surveillance conducted along with global corporations, which seriously hamper any ideas of any meaningful intelligence oversight required in democratic societies. Moreover, no government can now handover the whole monstrous surveillance machine developed in cyberspace to corporations or simply leave it as corporations are already incorporated and would therefore exploit it to support their market oriented interests. At the same time, the institution that was the outcome of Vannevar Bush recommendation after the World War 2, DARPA – The Defense Advanced Research Projects Agency of the United States of America, which was directed to run super-advanced research and technology invention programs to let the U.S. dominate the world by mastering technology is organizing a Capture The Flag competition called Cyber Grand Challenge in Las Vegas, just days before the DEF CON,[677] where geeks usually meet every year to discuss liberating technologies and demonstrate the most difficult hacks. However, as said already several times, DARPA enlarged its interests to DEFCON and triggered competition between hacking teams who will develop better artificial intelligence patching exploits autonomously, which will certainly add another actor to the current quagmire. It would be great to see both cooperating, but I do not perceive a development of possible hostile artificial intelligence as a harmonization of policies; especially when such system can be completely decentralized and will need to gather information globally to distinct from malign and benign behavior. Somebody will have to learn the artificial intelligence to distinguish an enemy from an ally. As such, this is clearly a development of Skynet depicted in cyberpunk movie Terminator.

We can observe a shift of meaning, a shift from two kinds of operations, from gathering information to conducting offensive operations. The border is blurring and the artificial intelligence will do both to be effective patching autonomous system. As the physical force is not meaningful in cyberspace, the division between cyber-attack to gather information in espionage operation and cyber-attack to alter the machine in order to patch it or physically destroy it is blurring. The attack vector is the same, intentions

677

are different and implications are different. This is also a historical moment as historically spies sent to the enemy territory usually did not have enough power to level a city to the ground but to conduct some selective sabotage operation only. They were at least a bit predictable. A hacker coming to a country in cyberspace *can do whatever s/he wants* as some policy makers do not hesitate to use words about leveling the country to the ground in emotional speeches using metaphors and constructed analogies. The logical nexus depicted in alarming academic articles with a certain policy oriented message are giving importance to vulnerabilities of critical infrastructures in relations to its imaginative enemies such as hackers, script kiddies, hacktivists, organized crime, states and terrorists[678] without ordering them on a scale of seriousness, while adding another clearly the most unpredictable actor of artificial intelligence. Terrorist is the same enemy as script kiddies – *"they already show us what they can do in cyberspace."* This is a compendium of all possibilities put at the same level of importance and marked as the highest threat to national security in every single national cyber security strategy. The *technological radical uncertainty* is what plays a role in this assessment and the artificial intelligence does not make it less complex, less uncertain and less radical.

As the meaning is repeatedly practiced in the flicking discourse on every conference, especially on places that implies discussions between *cyber experts*, they are becoming an expert by having the ability to repeat what is already generally understood as a depiction of growing threats. Meaning, which is already established as an unchallengeable *church of knowledge*, in which "priests" of cyberspace are the more respected ones, the more they reproduce already designated truths of national security. The practices of these "priests" speaking about national security in cyberspace are reproducing the discourse, which in a loop-back gives them the opportunity to become "priests" of this church of knowledge – the respect in the field is based on feelings rather than on real technical expertise; it looks like religion. It is more about the expertise, which is driven by policy as this expertise is the one, which others expect, respect as expectable and accept as the shared appropriate policy. Hearing more alarming discourse is what listeners expect, hearing less alarming would lower the attractiveness and thus

[678] A. Nicholson et al., "SCADA Security in the Light of Cyber-Warfare," *Computers & Security* 31 (2012): 418–36, doi:10.1016/j.cose.2012.02.009.

confidence of speaker's integrity as a respectful expert, but also loyal to the epistemic community of experts in policy of cyber security. The one who dares to raise important questions, such as Elon Musk who is constantly warning against artificial intelligence in the service of national security, are expelled from the democratic debate. The clear effect of Social Identity Theory. These moments of policy oriented conferences are deepening the seriousness of what have been said elsewhere by the practice of repeating statements drawing on more dramatic imaginations without a notion of technical insight to discussed events.

The content of the policy conferences is much more about repeating already adopted truths that by repeating are deepening their roots in our perception of truth. The content of these discursive practices is filled with speeches of high-rank officials, authorities, usually these (very limited amount of critical speeches) I used in empirical part, to produce the *unbeatable truths* of the *church of knowledge*. One cyber security conference in the United States culminated with speeches by all chiefs of NSA, CIA and FBI in 2014.[679] The message was clear: the evidence rises, the threat deepens, institutions must become stronger, international cooperation and sharing information is a norm. These policy moves were supported clearly by imagination of possible cyber 9/11 or cyber Pearl Harbor (mentioned almost during every speech) and question on Stuxnet was answered as understandable capability of national cyber offense.

These practices are producing content for meaning that reproduce these practices. Discourse and material practices are mutually constitutive as they are tightly bound to each other.[680] The influence link between them works in a circle rather than in a linear way; the process of reiterating truths said on "sacred grounds" by "divine enlightened experts" with special knowledge in e.g. *cyber terrorism.* It is not by accident that Richard Clark was an expert on terrorism and cyber security at once. One may rise a legitimate question, whether thinking over terrorism in White House just couple of years after 9/11 influences a perspective of ungovernable cyberspace that has grown on neoliberal principles without significant power of nation states to control the activity there. The

[679] International Conference on Cyber Security (ICCS) – http://www.iccs2016.iaasse.org/

[680] Vincent Pouillot, "'Sobjectivism': Toward a Constructivist Methodology," *International Studies Quarterly* 51, no. 2 (2007): 359–84.

technological radical uncertainty combined with unpredictability of hackers seeking the establishment of the crypto-anarchist Eden by significantly asymmetric powers pour fuel into ideas of possible terrorist attacks in cyberspace. It is crystal clear that the ideology of crypto-anarchist movement is a direct enemy to intentions of regulated cyberspace by nation state authorities. However, intermingling nation state security with international surveillance and supra-national multi-stake holder governance of the internet rises enough doubts of a nation state capability and credibility to govern the securitization of cyberspace threats, as national security issue becomes a very logical implication.

It would be understandable seeing states encouraging private business to secure glitches in systems based on lessons learnt, but we see international exercises in cyber defense on imaginative scenarios. These scenarios are drawing imaginative futures on emotional past (Cyber 9/12 Challenge by Atlantic Council) despite the fact they are driven by curiosity of filling the gap between the technical and policy part of cyber security as a national security agenda. All of these actions are carving the need as an unbeatable truth into the stone despite its basis on imaginative world. Organizing exercises based on particular experience, on for example the Ukrainian blackout, would be probably too easy as the most problematic part in Ukraine despite its better defense that some critical infrastructures have in United States[681] were absence of two level authentication. Imagination must be included in these exercises to let the competitors deal with unpredictable and unknown challenges. That finally vindicate the imagination as an appropriate approach for our preparedness. However, it leaves us in a fable rather than in the real world. It does not provide us with thoughts how to develop policy of preparedness that would react on catastrophes in the normalized manner as Aradau and Munster recommend.[682]

The *church of knowledge* developed on policy conferences and practiced on exercises is qualifying supra-national authorities in asking a question whether a particular policy have been already adopted on a national level. It is a kind of competition; the state has adopted its own national cyber security policy before the others is

[681] SANS ICS, *Analysis of the Cyber Attack on the Ukrainian Power Grid*.
[682] Aradau and Munster, *Politics of Catastrophe*.

understood as more *modern*. However, it is also a question aiming on a greater policy of internationally integrated network of state authorities in a hierarchical supra-national structures that are expected to follow a new norm – a need of national cyber defense. The threat is allegedly real as the defenses are already teased on exercises, hacking of turbines is allegedly real despite the fact that critical knowledge, hard-to-obtain, is critically needed and thus it is not generalizable as a global threat to all energy turbines.

It is a new norm to be prepared on national defense level despite the fact that every single cyber security expert dealing with everyday threats in cyberspace would say that these threats are of course real, but state can do a little to such extremely quick development of malicious technology. It is about secure technology that can be developed and finally security education at least of operators that tend to put a written password on sticky papers visible on their monitors. The Ukrainian attack was possible only due to a row of such human errors. National defense would do a little to stop it. However, that fact does not fit to the discursively constructed perceptual field of policy experts in national cyber security drawing the cyber doom in order to strengthen nation state authorities and wish to govern technology development related to cyberspace;[683] it is becoming a norm to have strong cyber defenses and a violation of global undisputable norm facilitates exceptional response – a resistance.

[683] Jerry Brito and Tate Watkins, "Paper Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," 2011, http://mercatus.org/sites/default/files/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy_0a.pdf.

3. POWER, AUTHORITY AND GOVERNANCE

On a first, horizontal, axis, an assemblage comprises two segments, one of content, the other of expression. On the one hand it is a machinic assemblage of bodies, of actions and passions, an intermingling of bodies reacting to one another; on the other hand it is a collective assemblage of enunciation, of acts and statements, of incorporeal transformations attributed to bodies. Then on a vertical axis, the assemblage has both territorial sides, or reterritorialized sides, which stabilize it, and cutting edges of deterritorialization, which carry it away.

– Deleuze and Guattari, A Thousand Plateaus[684] –

The final point I have been planning to elaborate is a specific insight into dynamics of cyberspace governance. The theoretical lens that suggests itself is the actor-network theory (ANT) and the perspective of network assemblages. As we can read throughout the literature ANT is not a theory, it is rather a perspective, a mindset how to perceive a problem. Even its first protagonist talk about ANT as follows: *"there are four things that do not work with actor-network theory: the word actor, the word network, the word theory and the hyphen! Four nails in the coffin."*[685] However, I follow several rules of ANT I could observe elsewhere. ANT provides us with a specific mindset, how to perceive what is going on in cyberspace. There are different approaches to ANT and probably every research produces its own designed approach to fit the perspective they propose with the particular research. It is also a toolkit for telling interesting stories and depicting the inner relations and interferences[686] and that is the approach I am taking in the following text.

Concept of *assemblage* was introduced to the social theory by Deleuze and Guattari with a bit cyber-punk perspective as a state of intermingled bodies in a society with all the emotional aspects (sympathies and antipathies), body alterations, splitting bodies in amalgamation, penetration, but also expansion.[687] It can be understood as expansion by technology, because Deleuze and Guattari later contended that technology makes mistake

[684] Gilles Deleuze and Felix Guattari, *A Thousand Plateaus*, vol. 52 (Minneapolis, London: University of Minnesota Press, 1989), 88.

[685] Latour, "On Recalling ANT," 15.

[686] John Law, "Actor Network Theory and Material Semiotics," in *The New Blackwell Companion to Social Theory*, ed. Bryan S. Turner (Wiley-Blackwell, 2009), 141–58.

[687] Deleuze and Guattari, *A Thousand Plateaus*, 52:90.

by being treated in isolation: *"The stirrup entails a new man-horse symbiosis that at the same time entails new weapons and new instruments."*[688]The relation plays a role in ANT as well as assemblage, the whole assemblage is a network of relations; no actor is influenced by other including technology and its dynamic development. Cyber security can be approached as a network assemblage completely, as a whole environment in one huge assemblage of states, institutions, epistemic communities and technology approached in a temporal perspective as *a chronopolitics of cyber security*.[689]

However, my perspective is to approach assemblage as antagonistic networks that can exist thanks to that negative relation (state and crypto-anarchists). Hence, the assemblage applies on these different networks as well. It is hard to distinguish strictly between them. Hackers can be hackers during the night and government paid cyber security operators at the cyber security defense center during the day. They both use the same technology and the technology develops and evolve due to the interaction between these two assemblages, so the higher assemblage of cyber security is comprised of other assemblages (states, crypto-anarchists, intelligence, corporations with technology and even artificial intelligence based on a mixture of technology and human expectation of its capabilities) that constitute the higher one: *"the properties of the component parts can never explain the relations which constitute a whole."*[690] Let's call these lower level assemblages *socio-technical dimensions* of the cyber security assemblage.

First, I was drawing on motivations of hackers and their ideology. I did it as I believe that it is important to read their final intentions rather than their current capabilities. Their intentions are causing *effects;* the capabilities are what is available to anybody if the one has the will to adopt it. Intentions matter, intentions causes *effects.* If there are uniform effects caused by the heterogeneous actors, it can be studied as a network of actors.[691] Actors, that are both human and non-human and interlinked in a

[688] Ibid.

[689] Stevens, *Cyber Security and the Politics of Time*, 181.

[690] Manuel DeLanda, *A New Philosophy of Society: Assemblage Theory and Social Complexity*, *Continuum*, vol. 40, 2006, 10, doi:10.1111/j.1467-8330.2008.00646.x.

[691] Annemarie Mol, "Actor-Network Theory: Sensitive Terms and Enduring Tensions," *Kölner Zeitschrift Für Soziologie Und Sozialpsychologie. Sonderheft* 50, no. 1986 (2010): 253–69, doi:10.1177/1745691612459060.

global networked assemblage,[692] but distinct from the other *socio-technical dimension* by having particular crypto-anarchist political agenda that drives particular technological development. The crypto-anarchist ideology is crucial for triggering the intentions as the content draws on dystopian future. The comparable tensions in inner consciousness that is well related to Kafka's writing of The Castle[693] or The Trial[694] on which Deleuze and Guattari build their perspective.[695] Kafka's writings, despite its lack of being pure cyber-punk or science fiction, is certainly a dystopian fiction, but still a fiction drawing on possible reality around us, on absurd dynamics between the state administration and the citizen. The Trial shows how absurd could be a blind following of rules in the administration and that it can lead into a tragedy, which is perceived only as a tragedy from the perspective of the victim, but certainly not from the perspective of mechanistic state administration. Kafka's message is compatible to the ideology of crypto-anarchists who see the liberation in the bright future of a body alteration (they do practice at least implanted RFID chips at crypto-anarchist institutions) and technology evolution as a tool of liberation from absurd ungovernable and hostile nation state governance. Their efforts already cause visible *effects* without central authority, but within a *network assemblage* with unexpected contingent effects practicing *actualized power*[696] that certainly fuels the *technical radical uncertainty,* of those who are dependent and materialize the *immanent power*. [697]

Second, some hackers are celebrated as heroes (Snowden, Assange) who produce the *fantasy of masterful.*[698] That inspiration, as the Pasteur in *pasteurization of France,*[699] is what drives the crypto-anarchy community in new inventions, software development and proliferation of liberation technologies. The fast development of technologies that is immediately changing the internal dynamics of technology *used by* their operators is fluid as flowing waterfall. Both, humans and non-humans are altering each other with critical

[692] Abrahamsen and Williams, "Security Beyond the State: Global Security Assemblages in International Politics."
[693] Franz Kafka, *The Castle* (OUP Oxford, 2009).
[694] Kafka, *The Trial*.
[695] Deleuze and Guattari, *A Thousand Plateaus*.
[696] Ibid.
[697] Ibid.
[698] Mol, "Actor-Network Theory: Sensitive Terms and Enduring Tensions."
[699] Bruno Latour, *Pasteurization of France* (Harvard College, 1988).

implications to social dynamics of global society. Speed of social change that have never been experienced by human. However, the technology development on the side of crypto-anarchist socio-technical dimension is capable of well-organized development of useful technologies without a central authority. The *fantasy of masterful* might look as utopia, however, the words of Edward Snowden after his revelations seems to be quite more moderate than one would expect. His continuous contention that he wanted to put attention on a bad behavior of states rather than to topple them down is enchanting his words and actions with legitimacy; in that perspective his desire could be to save the liberal democratic values of a western-type liberal nation state. However, the revelations in contrast have been lowering a liberal nation state credibility and ability to govern[700] in the eyes of citizens and have triggered a need of the same citizens to adopt liberating technologies in order to hide from authorities. This move is not what we would expect in liberal democracy, that is what we experience in the totalitarian regimes such in the communist countries of Eastern Europe. However, these fantasies of masterful about a liberated world covered by a dome of justice is a driver for the whole community to work without a need of stable shared vision, even the vision is blurred in certain objectives, but the liberation red line across it is clear. We see a networked assemblage – on both sides – of human and non-human actors driven by utopia of ultimate freedom or ultimate security. But this state of crypto-anarchist movement (on one side) is still not enough for working in an effective global cooperative network.

Third, the language plays a crucial role in the cooperation as the adoption of particular *locutory nexus* is creating the Mind, a shared mindset within a networked community. Acquisition of language, repeated statements in shared comments or sharing the same vocabulary *attune* actors in the assemblage. Tuning people to the same frequency requires content they would believe. Crypto-anarchist movement provides enough content for that imagination. The result is clearly the *technological radical uncertainty* reflected in the production of extreme alarming discourse such as cyber terrorism. A possibility that even curiosity driven cyber security experts working for corporations running national critical infrastructures do not hesitate to take as an

[700] Jasanoff, *States of Knowledge: The Co-Production of Science and Social Order*.

option,[701] because they live in a shared inter-institutional and international consciousness sharing knowledge, opinion and beliefs.[702] They might easily become the scientific advisers to policy makers[703] as they are exactly the experts, whose expertise is accepted without doubt, but who live in the enclosed discursively constructed world counting with global terrorism as the biggest burden to a thriving civilization. It is a crystal clear example how the discourse within a particular assemblage produce a conviction of possible futures that in a loop-back facilitates policies on possibilities despite their clear authoritarian inclination in a possible future establishment of the *panopticon*. The PRISM was an understandable outcome, it is not a mistake or a contiguous error in the system, it is what was expectable when one calls for ultimate security from any possible cyber terrorist attempt. However, that development, in addition understood as legitimate, is what Baudrillard call the *Integral Reality*, where the desired future state is totalized in utopia. The same motivations apply to the ideas of artificial intelligence autonomously patching glitches in the system. In that perspective, the doom scenario seems to be the solution on what is generally call a policy against doom scenarios.

The same as seen above can thus be applied on the network of cyber security policy experts. The logic of reproduced knowledge put into the working system of visible evidence. The ability to attune to the logical nexus caught in the locutory nexus of constantly repeated statements with inner logical relations emotionally colored by constructed alarming correlations in extreme historical events produce a material existence and a *sense*. Sense that *cyber terrorism* is a plausible future and thus we have to strengthen tights of nation state power to secure the national security. In this permanent state of exception of terrorist threat discursively constructed,[704] we are drawing only the most improbable events with heavy impacts.[705] Two totally distinct worlds can exist because they are in this *tension,*[706] tension that create a relation between two; tension

[701] Based on personal interview with experts from cyber security company Alef situated in the Czech Republic and working on cyber security projects related to critical infrastructure.
[702] Barnard-Wills and Ashenden, "Securing Virtual Space: Cyber War, Cyber Terror, and Risk."
[703] Jasanoff, *The Fifth Branch: Science Advisers as Policymakers*.
[704] Ondřej Ditrych, "A Genealogy of Terrorism in States' Discourse" (Charles University, 2011).
[705] Cavelty, "Cyber-Terror--Looming Threat or Phantom Menace? Th."
[706] Mol, "Actor-Network Theory: Sensitive Terms and Enduring Tensions."

producing *agency* on both sides.[707] The relational tension and the fact of synchronized productivity of new behaviors, expressions, realities as well as territorial organizations is what produce them as a *desired elusive network assemblage*. The whole agenda can be an absolute imagination, an elusive depiction of terror based on technologies that are itself understood as a social construction – cyberspace a space that is not a mere bunch of wires, but its own interpretation, a social construction. It would not exist without our habits, our usage of it, our perception of its pros and cons, our perception of threats it *may* bring to us.

The case of Vannevar Bush[708] in the late days of WW2 was driven by a conviction that no other authority than a state has the moral obligation to secure people's lives. A lot of people today are not convinced the same way. The indeterminacy of governance[709] would serve as one example, in which governments do not follow particular ideas, but rather tend to keep its status quo. NASA achievements in human space flight in comparison to what private business has been capable to do using NASA money in the last decade is a very common argument of the liberals proposing lower power for state in the technology development. However, it was a stat who decided and funded Apollo program that produced so much spin offs to the society.

Technical invention does not need to be the same as technical change as the latter can be anti-inventive, influenced by forms of political and cultural intervention.[710] Business has proved an ability to invent technologies that states were not, but that usually do not need to cover security issues in national security perspective despite the fact it might have covered their business interests and related security. The governance indeterminacy might be a problem in centralist government, but might not in decentralized government, which supports participation if one has will to participate. The distinction between the development of open-source Linux and proprietary development of Microsoft Windows has shown that the decentralized governance of software development can meet even higher security measures than centralized meets hardly.

[707] Martin Müller, "Assemblages and Actor-Networks: Rethinking Socio-Material Power, Politics and Space," *Geography Compass* 1, no. September (January 2014): 1–20, doi:10.1111/gec3.12192.
[708] Bush, "Science - The Endless Fronties."
[709] Wynne, "Risk and Environment as Legitimatory Discourses of Technology: Reflexivity inside-Out."
[710] Andrew Barry, *Political Machines: Governing a Technological Society* (London: Athlone Press, 2001), 201.

However, these debates are not coming to an end. Microsoft, on the other hand, has been providing code to governments and recently even to NATO to let the authorities dig into the code for vulnerabilities. One would question whether such cooperation is even imaginable between authorities and decentralized open-source community.

Before the government can pursuit its objectives, it is needed to draw the problem, the threat we have to challenge, what our societies face; policy precedes construction of the threat. This is not done by objectively observable knowledge, but by proliferation of hybrids that are unknown, uncertain, ambiguous and uncontrollable. Crypto-anarchists are taking international security as given, as a result of culturally higher developed society and thus Euro-Atlantic security structures made by the alliance of nation states are understood as obsolete or even derogatory. Crypto-anarchists are such an example of an ideology driven ultra-libertarian movement rooted on anti-centralist presumptions, which are written in their constitutive writings.[711] On the other hand, states are living in their permanent state of exception, in which the security is not given and state has to look around to be prepared. These two mutually excluding perspectives are the clash between crypto-anarchists believing in liberating technologies and nation states following tradition of nation state security driven by social contract. If nation states are working on cyber defenses due to well successful materialization of imaginations of cyber policy experts, which mutually constitute themselves in a relation to the drawn enemy in crypto-anarchists, states are becoming *effect rather than an exercise of power*.[712] If we follow the experience with open-source and proprietary software, we might devise that it would be more decentralized network of people accepting encryption standards than states and their intelligence who will win the battle over security and privacy in the long term. Deleuze and Guattari make the distinction between *puissance*, the immanent power, and *pouvoir*, the actualized power,[713] the question is not whether states are more or less powerful, it is about the form of power that is activated. States have power to act immediately, but the assemblages of crypto-anarchists and all other moderate liberals using their technologies are fulfilling the principle of *actualized power,* which is proving

[711] Barlow, "A Declaration of the Independence of Cyberspace."

[712] Timothy Mitchell, "Society, Economy, and the State Effect," in *State/culture: State-Formation after the Cultural Turn* (Ithaka: Cornell University Press, 1999), 76–97.

[713] Deleuze and Guattari, *A Thousand Plateaus*.

its success by the proliferation of liberating technologies, services, ideas and principles as being the best security for a citizen.

There was a network called Arpanet at the beginning,[714] there is one cyberspace according to current national cyber security strategies today, but according to the diversified technology development there cannot be one cyberspace in the future. It is a statement that helps application of the same norms on all communication networks in order to secure *cyberspace*, an undisputable norm. As I pointed out already in the chapter about *Construction of security crises under technological radical uncertainty* the co-production process introduced by Sheila Jasanoff[715] can be applied to several different technology development strains. The difference in state driven cyber security technology development securing critical infrastructures and liberation driven technology development of crypto-anarchist movement can evolve in a non-conflicting mode or, if some of these liberating technologies are exploited by criminals, an adoption of a new policy focused on adopting some preventive counter-measures lowering privacy of citizens. The latter is what we are observing across the whole developed and liberal world, the mirroring of national cyber security strategies including the lowering of peoples' privacies is approached as a good habit. In that perspective, securing the whole cyberspace as one global network seems to be an unachievable idea as there is simply no one cyberspace and as these intentions lead to authoritarian rule. It is about a will of the governance over global communication technology development habits and standards. Shaping the ideas of appropriate technology development cannot be understood as Latour's ideal of modern, but as an authoritarian wish to control curiosity that drive inventions. States are losing their power over the governance of technology development, so they are shaping the threat through imaginative discourse, but that also lowers their credibility of governance in a nation state model by integrating supra-national bodies with objectives in cooperative construction of the panopticon. All of this in seek of global security; totalized security. I would understand it as a suicide of the nation state governance model.

[714] Ryan, *A History of the Internet and the Digital Future*.
[715] Jasanoff, *States of Knowledge: The Co-Production of Science and Social Order*.

The will to secure a nation state by supra-national bodies that will beat global security assemblages cannot strengthen the principle of a nation state in a global political arena. On the other hand, the decentralized regulation misdirects responsibility,[716] the assemblages and multi-stakeholder governance in case of global militarization of cyberspace would probably not be able to solve what a national security agenda is seeking for. However, there are only two options of further development, a super-authority that was already proposed at ITU Dubai Conference in 2012[717] and failed to be adopted, or a way we are experiencing right now, the multi-stakeholder governance, in which no state has power to shape cyberspace enough to meet required security measures. The result is that even the West tend to extremely securitize cyberspace to strengthen its power – to use cyberspace to its advantage,[718] but which resonates within citizens as an authoritarian rule.[719] Citizens, which are more than ever interconnected in global assemblages, are identifying with these global ideas rather than being linked to a national identity.

The political implications of the networks are very clear as Barry put it in difference between *politics* and *the political*.[720] The former is understood as institutionalized politics comprising of political parties, institutions, parliaments and states – the exercise of immanent power in *Deleuze and Guattari's puissance*, while the latter is understood as a way how a particular political agenda is established through artefacts, activities or practices that become objects of contestation[721] - the exercise of actualized power in *Deleuze and Guattari's pouvoir.* Power in the eyes of Foucault "*…is exerted rather than owned; it is not the acquired or preserved privilege of the dominant class, but the overall effect of its strategic positioning."*[722] Foucault revealed the fundamental fluidity of power that *"passes through individuals. It is not applied to*

[716] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).
[717] ITU, "Forging the Future," in *Panel Proceedings at the ITU Telecom World 2012* (Dubai 14–18 October 2012, 2012), http://world2012.itu.int/summary1.
[718] US-DoD, "Department Of Defense Strategy For Operating In Cyberspace," 2011, http://www.defense.gov/news/d20110714cyber.pdf.
[719] Barlow, "A Declaration of the Independence of Cyberspace."
[720] Barry, *Political Machines: Governing a Technological Society*, 201.
[721] Ibid., 6.
[722] Deleuze, *Foucault.*

them.''[723] It is an individual who practice power based on beliefs within the social structure s/he well know and is oriented in. Power is not only centralized as it should have been taking the words of Vannevar Bush, power is more decentralized, networked and practiced as a repetition of *fantasies of masterful.* It is happening with no regard whether the state's centralized *immanent power* is exercised, because the *actualized power* is slowly materialized through crypto-anarchists developments of e.g. state independent global currency that, if used, only people's belief in it can seriously shake with the global economy. A move, that no politician would even imagine in the first decades after the World War Two. Power is not about what is it, but about what it does[724] that implies a creation of *regime of practice*,[725] which we observe around in the building of international project concerning national cyber security agendas along with the opposite liberation process that is materializing its actualized power slowly, but smoothly.

On the one hand, we have observed a will, a political agenda, an interest, a real operation to fulfil absurd utopia of global surveillance megastructure not far from Foucault's *panopticon* to preserve ultimate security from terrorist, which is itself an absurd utopia, maybe a formation of forecasted dystopia. However, it has successfully facilitated an investment of billions of dollars in a construction of it, of a real *panopticon*. On the other hand, the ideal of *nearly perfect assurance against tampering*, a vision from The Crypto Anarchist Manifesto[726] is seeking for an opposite utopia of *oligopticon*, where *"they see much too little to feed the megalomania of the inspector or the paranoia of the inspected, but what they see, they see it well."*[727] Both developments are strictly antagonistic, but fulfilling itself at the same time. No *oligopticon* would be possible in minds of people, it would never materialize into usable technology that is changing the world so quickly, if we were not observed the construction of *panopticon* in the massive global surveillance hydra. It would not be present in their intentions, in the *causes and effects* the network assemblage of crypto-anarchists produces the liberating technology

[723] Michel Foucault, *Society Must Be Defended: Lectures at the Colle`ge de France 1975–1976* (New York: Picador, 2003), 29.

[724] Foucault, *Society Must Be Defended: Lectures at the Colle`ge de France 1975–1976*.

[725] Michel Foucault, "Questions of Method," in *The Foucault Effect: Studies in Governmentality* (Chicago: The University of Chicago Press, 1991), 75.

[726] May, "The Crypto Anarchist Manifesto."

[727] Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory*, 181.

out of and against a will of centralized power in sovereign state. Nevertheless, they will continue this practice, if the tendency to create more powerful state beating imaginative cyber terrorist, preparing for imaginative cyber war, but burning its credibility by stealing privacy of citizens to secure global cyberspace persists. In the light of Snowden revelations, it seems like an exercise of authoritarian rule despite its liberal democratic foundations[728] and that so motivates the crypto-anarchists to continue and empower ultra-libertarians and thus corporations on a global scale. The critical distinction to the ideal model of panopticon and to what we have observed with PRISM is the fact that panopticon should have a sovereign, but the situation in cyberspace is, and in near future will be, quite different. The crypto-anarchists and ultra-libertarians seek decentralized government, the nation states introduced corporations to surveillance and thus cannot stop it and finally DARPA thinks about autonomous artificial intelligence patching glitches in cyberspace. This is not an environment, in which one sovereign can persist or emerge. However, it is a mutually constitutive process of multiple actors driven by contrastive imaginative discourses that will not preserve the international system as it is today.

This process I perceive as very dangerous to open minded liberal global democratic society, but at the same time the will along with the inability to reach the utopia of panopticon by a nation state may lead into a hybridized global governance or a central solution for particular policies on a global scale. After all, the global state is by some well-respected scholars understood as inevitable.[729]

[728] Bauman et al., "After Snowden: Rethinking the Impact of Surveillance."

[729] Alexander Wendt, "Why a World State Is Inevitable," *European Journal of International Relations* 9, no. 4 (2003): 491–542, doi:10.1177/1354066103940001.

CONCLUSION

The whole dissertation has been divided into three parts. The first anchored the theoretical and methodological approach. The second was about three archaeologies of cyber security discourses and the third was about the discussion concerning the implication of observed dynamics; both preceded by the theoretical chapter focused strictly on the theoretical perspective of the empirical part.

The part about the discourse archaeologies had the objective to draw three different images of cyber security as they are perceived by their respective actors. Geeks focus on computer security and have developed their own ideology of crypto-anarchism as an ultimate challenge of one's liberation from alleged state oppression practices. Law enforcement and espionage discourses are producing particular evidence that cyber security has become a serious problem that will certainly be on the increase in the near future. However, the third national defense discourse embodies these two images together, the evidence of cyber crime/espionage and the utopist crypto-anarchist Eden as a lair of possible cyber terrorists, to draw a near future of cyber doom. I did not show only the process of discourse formation; my goal was also to show how these images of fiction form into a national security discourse. How particular sub-culture that is adherent to the geek community, how these fictitious writings have established the foundation of near future imaginations in national security discourse that is confirmed by evidence in cyber crime conducted seemingly by the same people. It is hard to prove a causal link, but that was not intended. My intentions were to show how some inspirations, at least the vocabulary, have been taken from cyberpunk subculture. The dystopian visions of fictitious writings have been proved to be very similar to the doom scenarios shown by the authorities. The politics of national cyber security does not build on evidence threatening national security, it currently much more elaborates on imaginations as the policy is focused on preventive actions that should help nation states to avoid doom scenarios.

That approach seems to react directly on several sources. First, it has been drawn on dystopian future of cyberpunk by taking over the semiosis of this subculture. Second,

on visions of supernatural capabilities of geeks. Third, on ideology of crypto-anarchists that have particular objectives in toppling down states. Semiosis provides language and vocabulary, but it comes from a certain dystopian visions, which are culturally bound in cyberpunk literature and work as a subconscious pillar for imaginations of the real during formation of a nation state security discourse. Geeks are proving their capabilities by being involved in a massive global transfer of crime to cyberspace that is and will be still one step in advance from the law enforcement. That sort of evidence then forms visions, a perceptual field of possible cyber doom giving a birth of cyber as a national security agenda.

The discussion part then elaborates on these observations I made in the archaeology of three discourses. I used several theoretical perspectives to discuss the implications emanating from that imaginations.

Drawing on Bruno Latour perspective *we have never been modern*, I demonstrated how the alleged reality of cyber security threat cannot be liberated from cultural bounds and thus become modern. Beliefs play a significant role in policy making, beliefs made on formed imaginations of possible futures that can fulfil; they can, because hackers possess supernatural capabilities and they *will* do it because they have formed a movement of crypto-anarchists, which carved their objectives into their manifesto. Policy makers are carving these images of futures into a stone that has become an undisputable truth; a church of knowledge, however, a knowledge that forgot to translate its content to observe that cultural boundary. We can very clearly observe a creation of policy driven education programs directly focused on cyber security as a national security concern driven by these imaginations as a vindication of their opening. If combined with discussions concerning two types of expertise in science and technology studies: the curiosity driven expertise and the policy driven expertise, we are able to expect an emergence of self-confirming inner universe of cyber security policy despite the lack of evidence of burning cities or flooded valleys from opened dams. Palpable Latour's proliferation of hybrids, in which the cultural is mixed with natural; they are co-produced. The final knowledge cannot be detached from cultural interpretations and it is becoming institutionalized as a pure expertise reacting on *alleged* objective facts.

These developments have become possible due to what I called *technological radical uncertainty*. As geeks within their crypto-anarchy movement are patiently developing technologies making them more supernatural (technologies such as Bitcoin that has the potency to lower states' regulation power) other *possible* technologies in the hands of hackers are understood as tools for future cyber terrorists and nation states are not able to do anything with it. The inability of states to regulate development and export of certain technologies (proved on encryption technologies) gives an opportunity to the national cyber security discourse to self-confirm the possible future doom scenarios. However, in contrast to Y2K event in the end of the millennium, current imaginations do not have a judgement day in 31st December. Thanks to the lack of the judgement day, a lot of privacy lowering policies could be adopted. The continuous tendency to take over cyberspace by nation state that is losing its credibility in the light of being caught in the biggest surveillance operation ever can produce only one reaction – a resistance. This fact will give the imaginations opportunity to thrive.

Assessment of this process led me to think about future governability of cyberspace. While states possess the immanent power (*puissance)* to act, regulate by law or make surveillance legal, the geeks possess the actualized power *(pouvoir)* in developing liberating technologies on state regulation. The vision of online reputation stated in crypto-anarchist manifesto is not a hype, but has apparently fulfilled in a row of online services. Taxis regulated by law are not preferred as company Uber provided both the driver and the client with a tool based on online reputation. And other examples were used to show how these visions are making their way to our lives with no regard on state intervention. The proliferation of hybrids in global network assemblages are becoming more important at the same moment when liberal democratic states were caught in the biggest massive surveillance ever. I was arguing along with Sheila Jasanoff's perspective that states are not only losing their capability to govern technological development but also the credibility to govern it. If combined with such extreme exploitation of technology against its own citizens, when liberal democratic states switched in espionage tactics from high degree of certainty about a small amount of data to high degree of uncertainty about a large amount of data, we would arrive into a dystopian world depicted by George Orwell or Franz Kafka.

On the one hand we have geeks, which are working actively on liberating technologies that are lowering the ability of a nation state to govern not only the cyberspace, but in overall. On the other hand, we have nation states that are harshly building so called cyber defenses in space that does not have borders in order to secure a nation state from imaginative threats but being caught in unprecedented spy operation against its own citizens; in operation that shows how national security is no longer national, but supranational and privatized by incorporating massive online businesses. These two processes are at the same time mutually constitutive and antagonistic. If states continue in building cyber defenses against imaginative threats and continue carve their rationale in church of knowledge driven by undisputable and unquestionable policy requirements, we will observe more liberating technologies proliferation to our lives and lowering of a nation state immanent power. The rationale of crypto-anarchist objective is receiving credibility by each such a blow to the credibility of a liberal democracy nation state. The result might be a hybridized global governance, in which states do not play a significant role, even in delivering security.

The key message is that by preserving the current status quo – a situation, in which the most credible governance model of liberal democratic nation states respects massive surveillance on their own citizens in order to preserve security against dystopian fictions similar to science fiction writings – will lead to much less governable future, an decentralized panopticon nobody understand, nobody govern and nobody control. Ideas such as adding artificial intelligence as an actor to solve socially constructed hyperinsecurity will cause exactly the opposite to security and as Michel Foucault said:

> (…) the last man, when radiation has finally reduced his last enemy to ashes, will sit down behind some rickety table and begin the trial of the individual responsible. I can't help but dream about a kind of criticism that would not try to judge but to bring an oeuvre, a book, a sentence, an idea to life; it would light fires, watch the grass grow, listen to the wind, and catch the sea-foam in the breeze and scatter it."[730]

[730] Foucault, "The Masked Philosopher," 326.

BIBLIOGRAPHY

Aaviksoo, J. "Cyberspace: A New Security Dimension at Our Fingertips." *CSIS Statesmen's Forum*, 2007.

Abraham, John. *Science, Politics and the Pharmaceutical Industry: Controversy and Bias in Drug Regulation*. London and New York: UCL Press and St. Martin's Press, 1995.

Abrahamsen, Rita, and Michael C. Williams. "Security Beyond the State: Global Security Assemblages in International Politics." *International Political Sociology* 3, no. 1 (March 2009): 1–17. doi:10.1111/j.1749-5687.2008.00060.x.

Adler, Emanuel, and PM Peter M. Haas. "Epistemic Communities, World Order, and the Creation of a Reflective Research Program." *International Organization* 46, no. 01 (1992): 367. doi:10.1017/S0020818300001533.

Alexander, Keith B., Emily Goldman, and Michael Warner. "Defending America in Cyberspace." *National Interest*, 2013, 18–24.

Ampère, A M, and C A Sainte-Beuve. *Essai Sur La Philosophie Des Sciences; Ou, Exposition Analytique D'une Classification Naturelle de Toutes Les Connaissances Humaines*. Essai Sur La Philosophie Des Sciences; Ou, Exposition Analytique D'une Classification Naturelle de Toutes Les Connaissances Humaines. Bachelier, 1838.

Anderson, Ben. "Security and the Future: Anticipating the Event of Terror." *Geoforum* 41, no. 2 (2010): 227–35.

Anonymous. "Message to Scientology." *YouTube*, January 21, 2012. https://www.youtube.com/watch?v=JCbKv9yiLiQ.

Applebaum, Anne. "Mark Zuckerberg Should Spend $45 Billion on Undoing Facebook's Damage to Democracies." *The Washington Post*, 2016. https://www.washingtonpost.com/opinions/mark-zuckerberg-could-spend-45-billion-on-undoing-facebooks-damage/2015/12/10/4b7d1ba0-9e91-11e5-a3c5-c77f2cc5a43c_story.html.

Aradau, Claudia. *Critical Security Methods: New Frameworks for Analysis*. Oxon: Routledge, 2015.

Aradau, Claudia, and Rens van Munster. *Politics of Catastrophe*. London and New York: Routledge, 2011.

Arendt, Hannah. "On Violence." In *Crises of the Republic*, 105–98. San Diego, New York, London: Harcourt Brace Jovanovich, 1972.

Arquilla, John, and David Ronfeldt. "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (1993): 141–65. http://www.tandfonline.com/doi/abs/10.1080/01495939308402915.

ASP. "NATO Article 5: Collective Security in the Cyber Era." *American Security Project*, September 30, 2015. http://www.americansecurityproject.org/rethinking-nato-article-5-challenges-to-collective-security-in-the-cyber-era/.

Atlantic Council. "About the Cyber 9/12 Student Challenge." Accessed April 22, 2016. http://www.atlanticcouncil.org/programs/brent-scowcroft-center/cyber-statecraft/cyber-9-12/about-the-cyber-9-12-student-challenge.

———. "Exclusive Interview with Estonian President Ilves on Cyber Security," 2013. http://www.atlanticcouncil.org/blogs/new-atlanticist/exclusive-interview-with-estonian-president-ilves-on-cyber-security.

Austin, Greg. "What the US Gets Wrong About Chinese Cyberespionage." *The Diplomat*, May 22, 2015. http://thediplomat.com/2015/05/what-the-us-gets-wrong-about-chinese-cyberespionage/.

"BAE Homepage," 2016. http://www.baesystems.com/en/cybersecurity/feature/it-s-not-just-security---it-s-defence-.

Baldor, Lolita C. "Carter: NATO Must Bolster Cyberdefense before Addressing Cyberwarfare." *U.S. News*, June 24, 2015. http://www.usnews.com/news/world/articles/2015/06/24/carter-nato-must-bolster-cyber-defense.

Balzacq, Thierry. "The Three Faces of Securitization: Political Agency, Audience and Context." *European Journal of International Relations* 11, no. 2 (2005): 171–201. doi:10.1177/1354066105052960.

Barabási, A L. *Linked: The New Science of Networks*. Cambridge, Massachusetts: Perseus Publishing, 2002.

Barlow, John Perry. "A Declaration of the Independence of Cyberspace." Davos, Switzerland: Electronic Frontier Foundation, 1996. https://www.eff.org/cyberspace-independence.

Barnard-Wills, D., and D. Ashenden. "Securing Virtual Space: Cyber War, Cyber Terror, and Risk." *Space and Culture* 15, no. 2 (2012): 110–23. doi:10.1177/1206331211430016.

Barnett, Michael, and Raymond Duvall. *Power in International Politics*. *International Organization*. Vol. 59, 2005. doi:10.1017/S0020818305050010.

Barry, Andrew. *Political Machines: Governing a Technological Society*. London: Athlone Press, 2001.

Barša, P, and O Císař. *Levice v Postrevoluční Době: Občanská Společnost a Nová Sociální Hnutí v Radikální Politické Teorii 20. Století*. Politika a Společnost. Brno: Centrum pro studium demokracie a kultury, 2004.

Batey, Angus. "The Spies behind Your Screen." *The Telegraph*, November 24, 2011. http://www.telegraph.co.uk/technology/8899353/The-spies-behind-your-screen.html.

Baudrillard, J, and M Poster. *Selected Writings*. Stanford University Press, 2001.

Baudrillard, Jean. *Simulations*. New York, NY, USA: Columbia University, 1983.

———. *The Consumer Society: Myths and Structures*. London: SAGE Publications, 1998.

Bauman, Zygmunt. *Liquid Modernity*. *Contemporary Sociology*. Vol. 30, 2000. doi:10.2307/3089803.

———. *Umění Života*. Praha: Academia, 2010.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B J Walker. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8, no. 2 (2014): 121–44. doi:10.1111/ips.12048.

Bauman, Zygmunt, and T May. *Thinking Sociologically*. Blackwell Publishers, 2001.

Bayuk, Jennifer L., Jason Healey, and Paul Rohmeyer. *Cyber Security Policy Guidebook*. Somerset, NJ, USA: Wiley, 2012.

BBC. "Estonia Fines Man for 'Cyber War.'" *BBC News*, January 25, 2008. http://news.bbc.co.uk/2/hi/technology/7208511.stm.

———. "MP3 Sites Accused of Music 'Hijack.'" *BBC News*, July 12, 2000. http://news.bbc.co.uk/2/hi/americas/829668.stm.

BBC News. "More than 100 Arrests, as FBI Uncovers Cyber Crime Ring." *BBC*, October 2, 2010. http://www.bbc.co.uk/news/world-us-canada-11457611.

———. "The Ransomware That Knows Where You Live." *BBC*, April 8, 2016. http://www.bbc.com/news/technology-35996408.

Beck, Ulrich. "Risk Society: Towards a New Modernity." London: SAGE, 1992.

Benson, Pan. "Panetta: Cyber Threat Is Pre 9/11 Moment." *Cnn.com*, October 12, 2012. http://security.blogs.cnn.com/2012/10/12/panetta-cyber-threat-is-pre-911-moment/.

Berger, Peter L, and Thomas Luckmann. *The Social Construction of Reality: A Treatise in the Sociology of*

Knowledge. *New York*. Vol. First Irvi, 1966. doi:10.2307/323448.

Betz, David J., and Tim Stevens. "Analogical Reasoning and Cyber Security." *Security Dialogue* 44 (April 2013): 147–64. doi:10.1177/0967010613478323.

"BITCOIN MEETUP | Hivemind - Síla Decentralizované Mysli," 2016. https://www.facebook.com/events/555520327962033/.

"Bitlegal Tracks the Evolving Regulatory Landscape of Cryptocurrency, Digital Assets and Distributed Ledger Technology around the World." *Bitlegal.io*. Accessed March 26, 2016. http://bitlegal.io/.

Blanchette, J F. *Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents*. MIT Press, 2012.

Bloor, Robin. "Large-Scale DOS Attack Menace Continues to Grow." *The Register*, June 11, 2007. http://www.theregister.co.uk/2007/06/11/dos_security_cyberwarfare/.

Boas, Richard. "Sinister New Site 'Assassination Market' Enables Users to Contribute Bitcoins for Murder of US Officials." *Coindesk.com*, 2013. http://www.coindesk.com/sinister-new-site-assassination-market-enables-users-contribute-bitcoins-murder-us-officials/.

Booth, Ken. "Security and Self: Reflections of a Fallen Realist." In *Critical Security Studies: Concepts and Cases*, edited by Keith C. Krause and Michael C. Williams, 1997.

Bousquet, Antoine, and Simon Curtis. "Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations." *Cambridge Review of International Affairs* 24, no. 1 (2011): 43–62. doi:10.1080/09557571.2011.558054.

Bowman, M E. "Is International Law Ready for the Information Age." *Fordham Int'l LJ* 19, no. 5 (1995): 1935.

Brito, Jerry, and Tate Watkins. "Paper Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," 2011. http://mercatus.org/sites/default/files/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy_0a.pdf.

Brodie, Bernard. *War and Politics*. London: Cassell, 1972.

Broersma, Matthew. "NATO Set To Ratify Cyber-Defence Declaration At Summit." *Tech Week Europe*, September 1, 2014. http://www.techweekeurope.co.uk/workspace/nato-cyber-151717.

Bronk, Christopher, Cody Monk, and John Villasenor. "The Dark Side of Cyber Finance." *Survival* 54, no. 2 (November 14, 2012): 129–42. doi:10.1080/00396338.2012.672794.

Bronk, Christopher, and Eneken Tikk-Ringas. "The Cyber Attack on Saudi Aramco." *Survival* 55 (May 19, 2013): 81–96. doi:10.1080/00396338.2013.784468.

Brooke, Heather. "Inside the Secret World of Hackers." *The Guardian*, August 24, 2011. https://www.theguardian.com/technology/2011/aug/24/inside-secret-world-of-hackers.

Bumiller, Elisabeth, and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." *New York Times*, October 11, 2012. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

Bush, Vannevar. "Science - The Endless Fronties." *Transactions of the Kansas Academy of Science* 48, no. 3 (1945): 231–64.

Bussel, Jennifer. "Cyberspace." *The Encyclopædia Britannica*, 2016. http://www.britannica.com/topic/cyberspace.

Buzan, Barry, Ole Wæver, J de Wilde, and Jaap De Wilde. *Security: A New Framework for Analysis*. *National Bureau of Economic Research Working Paper Series*. Lynne Rienner Publishers, 1998.

Calce, Michael, and Craig Silverman. *Mafiaboy: How I Cracked the Internet and Why It's Still Broken*. Viking, 2008.

Carneggie Mellon University. “CERT Software Engineering Institute.” Accessed April 28, 2016. www.cert.org.

Castillo, Michael del. “European Parliament Member: Everyone Should ‘Get Some Bitcoins.’” *Coindesk*, April 22, 2016. http://www.coindesk.com/european-parliament-member-blockchain-get-some-bitcoins/.

Cavelty, Myriam Dunn. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London and New York: Taylor & Francis, 2007.

———. “Cyber-Terror—looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate.” *Journal of Information Technology & Politics* 4, no. 1 (2008): 19–36. doi:10.1300/J516v04n01_03.

———. “The Militarisation of Cyberspace: Why Less May Be Better.” In *4th International Conference on Cyber Conflict*, edited by Christian Czosseck, Rain Ottis, and Katharina Ziolkowski, 141–53. Tallin: NATO CCD COE, 2012.

Cavelty, Myriam Dunn, V. Mauer, and S.F. SF Krishna-Hensel. *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*. Ashgate Publishing, Limited, 2007.

CCDCOE. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Edited by Michael N. Schmitt. New York: Cambridge University Press, 2013.

Cebrowski, Arthur K. “The State of Transformation. Presentation to Center for Naval Analyses on 20th November in Crystal City.” 2002.

Cebrowski, Arthur K., and John J. Garstka. “Network-Centric Warfare : Its Origin and Future.” *US Naval Institute Proceedings*, no. January (1998): 28–35.

Center for Strategic and International Studies. “Net Losses: Estimating the Global Cost of Cybercrime.” *Mcafee*, no. June (2014). http://www.mcafee.com/kr/resources/reports/rp-economic-impact-cybercrime2.pdf.

Chen, Adrian. “Hacker Plot to ‘Kill Facebook’ Is All a Terrible Misunderstanding.” *Gawker*, October 8, 2011. http://gawker.com/5829659/hacker-plot-to-kill-facebook-is-all-a-terrible-misunderstanding.

Chilton, Paul Anthony. *Security Metaphors: Cold War Discourse from Containment to Common House*. Peter Lang GmbH, 1996.

Choucri, N. *Cyberpolitics in International Relations*. Cambridge, Massachusetts and London, England: MIT Press, 2012.

Clarke, Richard. “Threats to US National Security: Proposed Partnership Initiatives towards Preventing Cyber Terrorist Attacks.” *DePaul Business Law Journal* 12 (1999): 33–44.

Clarke, Richard, and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins, 2012.

Clinch, Matt. “Bitcoin Recognized by Germany as ‘Private Money.’” *Cnbc.com*, August 19, 2013. http://www.cnbc.com/id/100971898.

“CloudFlare.” Accessed March 29, 2016. https://www.cloudflare.com/.

Clynes, M., and N. Kline. “Cyborgs and Space.” *Astronautics*, no. September (1960): 26–27, 74–75.

Cohen, Julie E. “Cyberspace As/and Space.” *Columbia Law Review* 107:210, no. 1 (2007): 210–56.

Collier, Jamie. “NATO’s Role in the Cyber Domain Is Unclear.” *Cyber Security Intelligence*, November 6, 2015. https://www.cybersecurityintelligence.com/blog/natos-role-in-the-cyber-domain-is-unclear-775.html.

Collins, Harold Maurice, and Robert John Evans. “The Third Wave of Science Studies: Studies of Expertise and Experience.” *Social Studies of Science* 32, no. 2 (2002): 235–96. doi:10.1177/0306312702032002003.

Collins, Harry, and Trevor Pinch. *The Golem at Large: What You Should Know About Technology*. Cambridge

University Press, 2002.

Collins, Sean, and Stephen McCombie. "Stuxnet: The Emergence of a New Cyber Weapon and Its Implications." *Journal of Policing, Intelligence and Counter Terrorism* 7 (April 2012): 80–91. doi:10.1080/18335330.2012.653198.

Committee on Armed Services. "U.S. Senate Committee on Armed Services Hearing to Consider the Nomination of Hon. Leon E. Panetta to Be Secretary of Defense." Washington D.C., June 9, 2011.

Conroy, Julie. *Citadel and Gozi and Zeus, Oh My!* AITE group, 2013. http://www.emc.com/collateral/white-papers/citadel-gozi-zeus-oh-my-wp.pdf.

Cornwell, Rupert. "US Declares Cyber War on China: Chinese Military Hackers Charged with Trying to Steal Secrets from Companies Including Nuclear Energy Firm." *Independent*, May 19, 2014. http://www.independent.co.uk/life-style/gadgets-and-tech/us-charges-chinese-military-hackers-with-cyber-espionage-bid-to-gain-advantage-in-nuclear-power-9397661.html.

Cox, Robert W. "Social Forces, States and World Orders: Beyond International Relations Theory." *Millenium* 10, no. 2 (1981): 126–55.

Crilly, Bob. "FBI Finds Method to Hack Gunman's iPhone without Apple's Help." *Telegraph.co.uk*, March 29, 2016. http://www.telegraph.co.uk/technology/2016/03/29/fbi-finds-method-to-hack-gunmans-iphone-without-apples-help0/.

Cuhadar, Esra, and Bruce Dayton. "The Social Psychology of Identity and Inter-Group Conflict: From Theory to Practice." *International Studies Perspectives* 12, no. 3 (2011): 273–93. doi:10.1111/j.1528-3585.2011.00433.x.

Culler, Johnathan D. *Ferdinand de Saussure*. Cornell Paperbacks : Linguistics, Literary Criticism. Cornell University Press, 1986.

Czosseck, C., and K. Geers. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Ios Press, 2009.

Dahlberg, Lincoln. "Democracy via Cyberspace." *New Media & Society* 3, no. 2 (2001): 157–77. doi:10.1177/14614440122226038.

"DEF CON," 2016. https://www.defcon.org/.

Deibert, R. J. "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace." *Millennium - Journal of International Studies* 32, no. 3 (2003): 501–30. doi:10.1177/03058298030320030801.

Deibert, Ron. "The Geopolitics of Cyberspace after Snowden." *Current History* 114, no. 768 (2015): 9–15.

Deibert, Ronald J., and Masashi Crete-Nishihata. "Global Governance and the Spread of Cyberspace Controls." *Global Governance* 18, no. 3 (2012): 339–61.

Deibert, Ronald, and Rafal Rohozinski. "Liberation vs. Control: The Future of Cyberspace." *Journal of Democracy* 21, no. 4 (2010): 43–57. doi:10.1353/jod.2010.0010.

DeLanda, Manuel. *A New Philosophy of Society: Assemblage Theory and Social Complexity*. *Continuum*. Vol. 40, 2006. doi:10.1111/j.1467-8330.2008.00646.x.

Deleuze, Gilles. *Foucault*. Paris: Editions de minuit, 1986.

Deleuze, Gilles, and Felix Guattari. *A Thousand Plateaus*. Vol. 52. Minneapolis, London: University of Minnesota Press, 1989.

———. *Anti-Edipus. Capitalism and Schizophrenia*. *SubStance*. Minneapolis: University of Minnesota Press, 1983. doi:10.2307/3684887.

Denning, Dorothy E. "Afterword to 'The Future of Cryptography.'" In *Crypto Anarchy, Cyberstates and Pirate Utopias*, edited by Peter Ludlow, 103. Cambridge, Massachusetts and London, England: MIT Press, 2001.

———. “Hacktivism: An Emerging Threat to Diplomacy.” *Foreign Service Journal* 77, no. September (2000): 43–49.

———. “The Future of Cryptography.” In *Crypto Anarchy, Cyberstates and Pirate Utopias*, edited by Peter Ludlow, 85–101. Cambridge, Massachusetts and London, England: MIT Press, 2001.

Ditrych, Ondřej. “A Genealogy of Terrorism in States’ Discourse.” Charles University, 2011.

Dougherty, Jon E. “It’s Time to Negotiate a Cyber War Treaty before the World Is Thrown back to the Stone Age.” *Cyber War News*, September 28, 2018. http://www.cyberwar.news/2015-09-28-its-time-to-negotiate-a-cyber-war-treaty-before-the-world-is-thrown-back-to-the-stone-age.html.

Dumont, Clayton W. *The Promise of Poststructuralist Sociology: Marginalized Peoples and the Problem of Knowledge*. State University of New York Press, 2008.

Dunn Cavelty, Myriam. “From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse.” *International Studies Review* 15, no. 1 (2013): 105–22. doi:10.1111/misr.12023.

Dunn, Myriam. “The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP).” *International Journal of Critical Infrastructures* 1, no. 2/3 (2005): 258. doi:10.1504/IJCIS.2005.006122.

Durkheim, Emile. *The Rules of Sociological Method*. New York: Free Press, 1950.

DW. “Cyber Attacks, Energy Security and Terrorism – A NATO Perspective on Emerging Security Challenges in the 21st Century.” *Deutsche Welle*, April 10, 2014. http://www.dw.com/en/cyber-attacks-energy-security-and-terrorism-a-nato-perspective-on-emerging-security-challenges-in-the-21st-century/a-17533087.

———. “NATO Moves to Apply Armed Conflict Law to Cyber Warfare.” *Deutsche Welle*, July 2, 2014. http://www.dw.com/en/nato-moves-to-apply-armed-conflict-law-to-cyber-warfare/a-17754359.

Egan, Paul. “State on High Cyber Alert after Anonymous Threat.” *Detroit Free Press*, January 22, 2016. http://www.freep.com/story/news/local/michigan/flint-water-crisis/2016/01/22/activist-hacker-group-anonymous-starts-flint-campaign/79157780/.

Eiriksson, Jonas Matthias, and José Manuel Retsloff. “Librarians in the ’ Information Age ’: Promoter of Change or Provider of Stability? Deconstructing Reality.” Royal School of Library and Information Science, 2006. http://www.biblioteksskonsulenterne.dk/filer/Librarians in the information age Promoter of change or Provider of stability.pdf.

Elias, Herlander. *Cyberpunk 2.0. Fiction and Contemporary*, 2009.

Elmer-Dewitt, Philip. “Computers: The 414 Gang Strikes Again.” *TIME*, August 29, 1983. http://content.time.com/time/magazine/article/0,9171,949797,00.html.

Endeshaw, Assafa. “Internet Regulation in China: The Never-ending Cat and Mouse game1.” *Information & Communications Technology Law* 13, no. 1 (2004): 41–57. doi:10.1080/1360083042000190634.

ENISA. *An Evaluation Framework for National Cyber Security Strategies*. ENISA, 2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1.

———. *National Cyber Security Strategies - Practical Guide on Development and Execution*. ENISA, 2012. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide.

Epstein, Charlotte. *The Power of Words in International Relations: Birth of an Anti-Whaling Discourse*. Cambridge University Press, 2008.

Epstein, Steven. *Impure Science: AIDS, Activism and the Politics of Knowledge*. Berkeley: University of California Press, 1996.

Etzioni, Amitai. *NSA: National Security vs. Individual Rights*. *Intelligence and National Security*. Vol. 00, 2014.

doi:10.1080/02684527.2013.867221.

EU. "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace." Brussels, 2013. http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

Europol. "The Internet Organised Crime Threat Assessment (IOCTA)," 2015. https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.

Ezrahi, Yaron. *The Descent of Icarus: Science and the Transformation of Contemporary Democracy*. Cambridge: Harvard University Press, 1990.

Falkenrath, Richard A. "From Bullets to Megabytes." *New York Times, The (NY)*. Accessed January 1, 2028. http://www.nytimes.com/2011/01/27/opinion/27falkenrath.html?_r=1.

Farivar, Cyrus. "A Brief Examination of Media Coverage of Cyberattacks (2007 - 2009)." *Cryptology and Information Security Series, The Virtual Battlefield: Perspectives on Cyber Warfare* 3 (2009).

Farwell, James P., and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." *Survival (00396338)* 53 (2011): 23–40. doi:10.1080/00396338.2011.555586.

FBI. "FBI — Manhattan U.S. Attorney Charges 37 Defendants Involved in Global Bank Fraud Schemes That Used 'Zeus Trojan' and Other Malware to Steal Millions of Dollars from U.S. Bank Accounts." *Fbi.gov*, 2013. http://www.fbi.gov/newyork/press-releases/2010/nyfo093010.htm.

Fielding, James. "EXCLUSIVE: Cyber Hackers Are GREATER Threat to UK Security than Nuclear Weapons." *Express*, October 25, 2015. http://www.express.co.uk/news/uk/614417/cybercrime-UK-talktalk-hack-security-computer-systems-online-safe.

Finkle, Jim. "Bangladesh Bank Hackers Compromised SWIFT Software, Warning Issued." *Reuters*, April 25, 2016. http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR.

Firestone, Adam. "In Cyberspace, Anonymity and Privacy Are Not the Same." *Securityweek*, September 26, 2014. http://www.securityweek.com/cyberspace-anonymity-and-privacy-are-not-same.

Foucault, M. *Discipline & Punish: The Birth of the Prison*. Vintage. Knopf Doubleday Publishing Group, 2012.

Foucault, Michel. *Power/Knowledge: Selected Interviews and Other Writings*. Edited by Colin Gordon. *New York*. Vol. 23. Pantheon Books, 1980.

———. "Questions of Method." In *The Foucault Effect: Studies in Governmentality*, 73–86. Chicago: The University of Chicago Press, 1991.

———. *Society Must Be Defended: Lectures at the Colle`ge de France 1975–1976*. New York: Picador, 2003.

———. *The Archeology of Knowledge*. London: Tavistock, 1972. doi:10.1177/053901847000900108.

———. "The Masked Philosopher." In *Politics, Philosophy, Culture. Interviews and Other Writings 1977-1984*, edited by Lawrence D. Kritzman. New York: Routledge, 1988.

———. "The Order of Discourse." In *Untying the Text: A Post-Structuralist Reader*, edited by Robert Young, 48–78. London and New York: Routledge, 1981.

Foucault, Michel, and Duccio Trombadori. *Remarks on Marx: Conversations with Duccio Trombadori*. Semiotext(e), 1991.

Fox News. "A Brief History of the LulzSec Hackers," June 21, 2011. http://www.foxnews.com/tech/2011/06/21/brief-history-lulzsec-hackers.html.

Fox-Brewster, Thomas. "FBI 'Most Wanted' Cybercrime Kingpin Linked To Russian Espionage On US Government." *Forbes2*, August 5, 2015. http://www.forbes.com/sites/thomasbrewster/2015/08/05/gameover-zeus-surveillance-links/.

Fukuyama, Francis. *Our Post Human Future: Consequences of Biotechnology Revolution*. New York: Farrar, Straus and Giroux, 2002.

Gable, Kelly A. "Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent." *Vanderbilt Journal of Transnational Law* 43 (2010): 57–118.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2 (2013): 41–73. http://belfercenter.ksg.harvard.edu/files/IS3802_pp041-073.pdf.

Geers, Keneth. *Strategic Cyber Security*. Tallinn: NATO CCD COE Publication, 2011.

Gewirtz, David. "Could Cyberwar Knock Us back to the Stone Age?" *ZDNet*, August 3, 2015. http://www.zdnet.com/article/could-cyberwar-knock-us-back-to-the-stone-age/.

Gibson, William. "Burning Chrome." *Omni*. Omni, July 1982. http://www.voidspace.org.uk/cyberpunk/burning_chrome.shtml#burning.

———. *Neuromancer*. New York: Ace Books, 1984.

Giddens, Anthony. *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Polity Press, 1991.

———. *The Constitution of Society*. Polity Press, 1984.

Gieryn, Thomas. *Cultural Boundaries of Science: Credibility on the Line*. Chicago: The University of Chicago Press, 1999.

Globa Cyber Security Capacity Centre. *Cyber Security Capability Maturity Model*. University of Oxford, 2014. http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM Version 1_2_0.pdf.

Goffmann, Erwing. *Frame Analysis: An Essay on the Organization of Experience*. Cambridge, Massachusetts: Harvard University Press, 1974.

Go-Gulf Blog. "Online Piracy in Numbers – Facts and Statistics [Infographic]," 2011. http://www.go-gulf.com/blog/online-piracy/.

Gomez, Miguel Alberto. "Operation Red October Fuels Debate over Cyber Espionage." *Eastasiaforum.org*, 2013. http://www.eastasiaforum.org/2013/02/07/operation-red-october-fuels-debate-over-cyber-espionage/.

Gompert, David C., and Martin Libicki. "Waging Cyber War the American Way." *Survival* 57, no. 4 (2015): 7–28. doi:10.1080/00396338.2015.1068551.

Goodwin, Cristin Flynn, and J. Paul Nicholas. *Developing a National Strategy for Cybersecurity*. Microsoft, 2013. http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf.

Gorman, Siobhan, and Jennifer Valentino-devries. "New Details Show Broader NSA Surveillance Reach." *The Wall Street Journal*, August 20, 2013. http://www.wsj.com/articles/SB10001424127887324108204579022874091732470.

GReAT. "The 'Red October' Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies - Securelist." *Kaspersky Lab Report*, 2013. http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies.

Green, James A. *Cyber Warfare*. Abingdon, UK: Routledge, 2015.

Green, Ruth. "Cyber-Attacks Rival Terrorism Threat, Says Former Head of NATO Rasmussen." *Ibanet*, October 21, . http://www.ibanet.org/Article/Detail.aspx?ArticleUid=d4ffe859-ed9d-4f83-8ecc-919dac460e9f.

Greenberg, Andy, and Gwern Branwen. "Bitcoin's Creator Satoshi Nakamoto Is Probably This Unknown Australian Genius." *Wired.com*, 2015. http://www.wired.com/2015/12/bitcoins-creator-satoshi-nakamoto-is-probably-this-unknown-australian-genius/.

Gros, Frédéric, Francois Ewald, and Alessandro Fontana. *The Courage of the Truth (The Government of Self and Others II) LECTURES AT THE COLLÈGE DE FRANCE 1983–1984*. Palgrave Macmillan, 2008.

Guitton, Clement, and Elaine Korzak. "The Sophistication Criterion for Attribution." *The RUSI Journal* 158 (August 2013): 62–68. doi:10.1080/03071847.2013.826509.

Hacking, Ian. *THE SOCIAL CONSTRUCTION OF WHAT ?* Cambridge, Massachusetts and London, England: Harvard University Press, 1999.

Hagmann, J., and Myriam Dunn Cavelty. "National Risk Registers: Security Scientism and the Propagation of Permanent Insecurity." *Security Dialogue* 43, no. 1 (2012): 79–96. doi:10.1177/0967010611430436.

Halpin, Harry. "The Philosophy of Anonymous: Ontological Politics without Identity." *Radical Philosophy* 176 (2012): 19–28.

Hansen, Lene, and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53, no. 4 (2009): 1155–75. doi:10.1111/j.1468-2478.2009.00572.x.

Healey, Jason. "The Spectrum of National Responsibility for Cyberattacks." *Brown Journal of World Affairs* 18 (2011): 57–70.

HEG. "Česko Je Podle Sobotky v Evropě Vzorem v Kybernetické Bezpečnosti. Hrozba Hackerských Útoků Ale Stoupá." *Hospodářské Noviny*, 2016. http://domaci.ihned.cz/c1-65206270-cesko-je-podle-sobotky-v-evrope-vzorem-v-kyberneticke-bezpecnosti-hrozba-hackerskych-utoku-ale-stoupa.

Held, D. *Democracy and the Global Order: From the Modern State to Cosmopolitan Governance*. Political Science. Stanford University Press, 1995.

Hilgartner, Stephen. *Science on Stage: Expert Advice as Public Drama*. Stanford: Stanford University Press, 2000.

Hill, Kashmir. "The Terrifying Search Engine That Finds Internet-Connected Cameras, Traffic Lights, Medical Devices, Baby Monitors And Power Plants." *Forbes*, September 23, 2013. http://www.forbes.com/sites/kashmirhill/2013/09/04/shodan-terrifying-search-engine/#4100e5a5174c.

Hodges, A, and C Nilep. *Discourse, War and Terrorism*. Discourse Approaches to Politics, Society and Culture. John Benjamins Publishing Company, 2007.

Hughes, Rex. "A Treaty for Cyberspace." *International Affairs* 86 (2010): 523–41. doi:10.1111/j.1468-2346.2010.00894.x.

Hutchinson, Jonathan. "Megaupload Founder Goes From Arrest to Cult Hero." *New York Times*, July 3, 2012. http://www.nytimes.com/2012/07/04/technology/megaupload-founder-goes-from-arrest-to-cult-hero.html.

Hyatt, Michael S. *The Millennium Bug: How to Survive the Coming Chaos*. Regnery, 1998.

———. *The Y2K Personal Survival Guide: Everything You Need to Know to Get from This Side of the Crisis to the Other*. Regnery Pub., 1999.

Iamme986. "Tech Geek." *Urban Dictionary*, 2010. http://www.urbandictionary.com/define.php?term=tech+geek.

Inkster, Nigel. "China in Cyberspace." *Survival* 52, no. 4 (November 15, 2010): 55–66. doi:10.1080/00396338.2010.506820.

Irwin, Alan. "Constructing the Scientific Citizen: Science and Democracy in the Biosciences." *Public Understanding of Science* 10, no. 1 (2001): 1–18. doi:10.1088/0963-6625/10/1/301.

———. *Expertise in Law and Regulation*. Ashgate, 2004.

Irwin, Alan, and Mike Michael. *Science, Social Theory and Public Knowledge*. Maidenhead, U.K.: Open

University Press, 2003.

Irwin, Alan, and Brian Wynne. *Misunderstanding Science*. Cambridge: Cambridge University Press, 2004. doi:10.1017/CBO9780511563737.

ITU. "Forging the Future." In *Panel Proceedings at the ITU Telecom World 2012*. Dubai 14–18 October 2012, 2012. http://world2012.itu.int/summary1.

———. *National Cybersecurity Strategy Guide*. International Telecommunication Union, 2011. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

———. "National Strategies," 2016. http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx.

Jackson, R. *Writing the War on Terrorism: Language, Politics and Counter-Terrorism*. New Approaches to Conflict Analysis. Manchester University Press, 2005.

Jackson, Richard. "Genealogy , Ideology , and Counter-Terrorism : Writing Wars on Terrorism from Ronald Reagan to George W . Bush Jr 1." *Studies in Language and Capitalism* 1, no. 1 (2006): 163–93. doi:ideologie; terrorismus; reagan; bush; krieg.

Jajodia, Sushil, Paulo Shakarian, V.S. Subrahmanian, Vipin Swarup, and Cliff Wang. *Cyber Warfare: Building the Scientific Foundation*. Springer, n.d.

Jasanoff, Sheila. "Breaking the Waves in Science Studies: Comment on H.M. Collins and Robert Evans, `The Third Wave of Science Studies'." *Social Studies of Science* 33, no. 3 (2003): 389–400. doi:10.1177/03063127030333004.

———. *Designs on Nature: Science and Democracy in Europe and the United States*. New Jersey: Princeton University Press, 2005. doi:10.1163/156848409X12526657425587.

———. *States of Knowledge: The Co-Production of Science and Social Order*. Routledge, 2004.

———. "Technologies of Humiliation: Citizen Participation in Governing Science." *Minerva* 41, no. 3 (2003): 223–44. doi:10.2307/41821248.

———. *The Fifth Branch: Science Advisers as Policy- Makers*. Cambridge, Massachusetts: Harvard University Press, 1990.

———. *The Fifth Branch: Science Advisers as Policymakers*. Cambridge, Massachusetts: Harvard University Press, 1990.

Jirásek, Petr, Luděk Novák, and Josef Požár. *Cyber Security Glossary*. 3rd ed. Praha: AFCEA and NCKB, 2015. http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf.

Johnson, Barnabas D. "The Cybernetics of Society: The Governance of Self and Civilization." Accessed March 19, 2016. http://www.jurlandia.org/cybsoc.htm.

Kafka, Franz. *The Castle*. OUP Oxford, 2009.

———. *The Trial*. Courier Corporation, 2012.

Kaiser, Robert. "The Birth of Cyberwar." *Political Geography* 46 (2015): 11–20.

Kampmark, Binoy. "Cyber Warfare Between Estonia And Russia." *Contemporary Review* 289 (2007): 288–93.

Karaganis, Joe. "Chapter 1 : Rethinking Piracy." In *Media Piracy in Emerging Economies*, 1–74. SSRC Press, 2011.

Kaspersky Lab. "Equation Group : Questions and Answers," 2015. http://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf.

———. "Kaspersky Security Bulletin 2015: Overall Statistics for 2015," 2015. https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf.

Kastenhofer, K. "Risk Assessment of Emerging Technologies and Post-Normal Science." *Science, Technology & Human Values* 36, no. 3 (2011): 307–33. doi:10.1177/0162243910385787.

Keany, Francis. "Australia Not Prepared for Cyber War; Response to Threats 'Slow and Fragmented', Report Warns." *ABC News*, January 19, 2016. http://www.abc.net.au/news/2016-01-19/australia-not-prepared-for-cyber-warfare-experts-warn/7097796.

Kellner, Douglas. *Media Culture: Cultural Studies, Identity and Politics between the Modern and the Postmodern*. London and New York: Routledge, 1995.

Kelly, Brian B. "Investigating in a Centralized Cybersecurity Infrastructure: Why 'Hacktivism' can and Should Influence Cybersecurity Reform." *Boston University Law Review* 92, no. 5 (2012): 1663–1711.

Kim, Andrew, Daryl Sng, and Soyeon Yu. "The Stateless Currency and the State: An Examination of the Feasibility of a State Attack on Bitcoin," 2014, 1–32. http://randomwalker.info/teaching/spring-2014-privacy-technologies/state-attack.pdf.

Kirsch, Cassandra M. "Science Fiction No More: Cyber Warfare And The United States." *Denver Journal of International Law & Policy* 40 (2012): 620–47.

Kiviat, Trevor I. "Beyond Bitcoin: Issues in Regulating Blockchain Transactions." *Duke Law Journal* 65, no. 3 (2015): 569–608.

Klimburg, Alexander. *National Cyber Security - Framework Manual*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012.

Knorr-Cetina, K. D. *The Manufacture of Knowledge: An Essay on the Constructivist and Contextual Nature of Science*. Oxford: Pergamon Press, 1981.

Knorr-Cetina, K. D., and M. J. Mulkay. *Observed: Perspectives on the Social Study of Science*. London: SAGE, 1983.

Koepsell, David R. *The Ontology of Cyberspace: Philosophy, Law, and the Future of Intellectual Property*. Open Court Publishing, 2003.

Kramer, Andrew E., and Nicole Perloth. "Expert Issues a Cyberwar Warning." *New York Times*, June 3, 2012. http://www.nytimes.com/2012/06/04/technology/cyberweapon-warning-from-kaspersky-a-computer-security-expert.html.

Kramer, Franklin D. "Cyberpower and National Security." *American Foreign Policy Interests* 35 (January 2013): 45–58. doi:10.1080/10803920.2013.757960.

Kruse, Peter. "Complete ZeuS Sourcecode Has Been Leaked to the Masses." *CSIS*, 2011. http://www.csis.dk/en/csis/blog/3229.

Kuchler, Hannah. "FireEye Bulks up for 'cyber Arms Race.'" *Financial Times*, January 20, 2016. http://www.ft.com/cms/s/0/35b30470-bfb0-11e5-846f-79b0e3d20eaf.html#axzz46jzMnJpC.

Kuehl, Daniel. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 35:24–42. Potomac Books, 2013.

Kuhn, Thomas. *The Structure of Scientific Revolutions*. *The Philosophical Review*. 2nd ed. Vol. II. Chicago: The University of Chicago Press, 1972. http://www.jstor.org/stable/2183664.

Kumar, Mohit. "DARPA Challenges Hackers to Create Automated Hacking System — WIN $2 Million." *The Hacker News*, 2016. http://thehackernews.com/2016/07/hacking-artificial-intelligence.html.

Kutiš, Robert. "Bitcoin - Light at the End of the Tunnel for Cyber-Libertarians." *HeinOnline* 8, no. 2 (2014): 214–21.

Lachow, Irving. "Active Cyber Defense - A Framework for Policymakers," 2013. http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf.

Lake, David a. "Why 'isms' Are Evil: Theory, Epistemology, and Academic Sects as Impediments to Understanding and Progress." *International Studies Quarterly* 55, no. 2 (2011): 465–80. doi:10.1111/j.1468-2478.2011.00661.x.

Lamont, Tom. "Alan Moore – Meet the Man behind the Protest Mask." *The Guardian*, November 26, 2011. http://www.theguardian.com/books/2011/nov/27/alan-moore-v-vendetta-mask-protest.

Larsson, Linus. "Charges Filed against the Pirate Bay Four." *ComputerSweden.idg.se*, January 31, 2008. http://computersweden.idg.se/2.2683/1.143146.

Latour, Bruno. "On Recalling ANT." In *Actor Network Theory and after*, edited by John Hassard and John Law, 15–25. Oxford: Blackwell and the Sociological Review, 1999.

———. *Pasteurization of France*. Harvard College, 1988.

———. *Politics of Nature: How to Bring the Sciences Into Democracy*. Cambridge: Harvard University Press., 2004.

———. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Clarendon Lectures in Management Studies. OUP Oxford, 2005.

———. *Science in Action: How to Follow Scientists and Engineers Through Society*. Harvard University Press, 1987.

———. *We Have Never Been Modern*. Cambridge, Massachusetts: Harvard University Press, 1993.

Latour, Bruno, and Steve Woolgar. *Laboratory Life*. Princenton: Princeton University Press, 1979.

Law, John. "Actor Network Theory and Material Semiotics." In *The New Blackwell Companion to Social Theory*, edited by Bryan S. Turner, 141–58. Wiley-Blackwell, 2009.

Lawson, S. "BEYOND CYBER-DOOM: Cyberattack Scenarios and the Evidence of History." *Mercatus Center George Mason University*, 2011. http://www.voafanti.com/gate/big5/mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf.

Lawson, Sean. "Articulation, Antagonism, and Intercalation in Western Military Imaginaries." *Security Dialogue* 42, no. 1 (2011): 39–56. doi:10.1177/0967010610393775.

Lee, Timothy B. "Everything You Need to Know about the NSA and Tor in One FAQ," October 4, 2014. https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/everything-you-need-to-know-about-the-nsa-and-tor-in-one-faq/.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

Levy, Steven. *Heroes of the Computer Revolution*. Anchor Press/Doubleday, 1984.

Lewis, Aidan. "Jaywalking: How the Car Industry Outlawed Crossing the Road." *BBC*, February 12, 2014. http://www.bbc.com/news/magazine-26073797.

Leyden, John. "Did Hacktivists Really Just Expose Half of Turkey's Entire Population to ID Theft? Entire Citizen Database? Probably Not." *The Register*, April 4, 2016. http://www.theregister.co.uk/2016/04/04/turkey_megaleak/.

Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999.

Libicki, Martin. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press, 2007.

Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35, no. 3 (November 10, 2012): 401–28. doi:10.1080/01402390.2012.663252.

Liscouski, Bob, and William J.S. Elliot. "Final Report on the August 14, 2003 Blackout in the United States

and Canada: Causes and Recommendations," 2004. https://reports.energy.gov/BlackoutFinal-Web.pdf.

Little, R. *The Balance of Power in International Relations: Metaphors, Myths and Models*. Cambridge University Press, 2007.

Ljungqvist, Alexander P, and William J. Jr. Wilhelm. "IPO Pricing in the Dot-Com Bubble." *The Journal of Finance* LVIII, no. 2 (2002): 723–52.

Lomas, Natasha. "WhatsApp Completes End-to-End Encryption Rollout." *Techcrunch*, April 5, 2016. http://techcrunch.com/2016/04/05/whatsapp-completes-end-to-end-encryption-rollout/.

Lomborg, Bjørn. "Don't Be Fooled - Elon Musk's Electric Cars Aren't about to Save the Planet." *The Telegraph*, April 6, 2016. http://www.telegraph.co.uk/opinion/2016/04/06/dont-be-fooled---elon-musks-electric-cars-arent-about-to-save-th/.

Lord, Jim. "My Y2K Apology." *GWU Website*. Accessed August 17, 2015. http://www.gwu.edu/~y2k/categories/jimlord_apology.html.

Love, Lauri. "As a Hacker, I Know How Much Power Some Teenagers Have - We Need to Start Building Bridges with Them, and Fast." *Independent*, May 9, 2016. http://www.independent.co.uk/voices/as-a-hacker-i-know-how-much-power-some-teenagers-have-we-need-to-start-building-bridges-with-them-a7020331.html.

Lucas, Edward. *The Snowden Operation*, 2014.

Lucas, Edward, and Peter Pomerantsev. *Defending and Ultimately Defeating Russia's Disinformation Techniques. Recommendatins. A Report by CEPA's Information Warfare Project in Partnership with the Legatum Institute*. Center for European Policy Analysis, 2016.

Ludlow, Peter. *Crypto Anarchy, Cyberstates, and Pirate Utopias*. Cambridge, Massachusetts and London, England: MIT Press, 2001. doi:10.1108/146366902320942995.

Lustick, I. *Trapped in the War on Terror*. University of Pennsylvania Press, Incorporated, 2006.

Lynch, Michael. "Circumscribing Expertise: Membership Categories in Courtroom Testimony." In *States of Knowledge: The Co-Production of Science and Social Order*, 161–80. London: Routledge, 2004.

Mandiant. "APT1 Exposing One of China's Cyber Espionage Units." *Report*, 2013, 1–76. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Manson, George Patterson. "Cyberwar: The United States and China Prepare For the Next Generation of Conflict." *Comparative Strategy* 30, no. 2 (November 14, 2011): 121–33. doi:10.1080/01495933.2011.561730.

Mark, Chris. "Case Study: The Compromise of RSA Security and the Rise of Cyber-Espionage." *PoliceOne*, July 22, 2012. http://www.policeone.com/police-products/communications/articles/5827608-Case-study-The-compromise-of-RSA-Security-and-the-rise-of-cyber-espionage/.

Marks, Michael P. *Metaphors in International Relations Theory*. New York: Palgrave Macmillan, 2011.

May, Timothy C. "The Crypto Anarchist Manifesto." In *Crypto Anarchy, Cyberstates, and Pirate Utopias*, edited by Peter Ludlow, 61–63. Cambridge, Massachusetts and London, England: MIT Press, 2001.

McAfee. *Virtual Criminology Report 2009: Virtually Here: The Age of Cyber Warfare*. Santa Clara, CA, USA: McAfee, 2009. www.mcafee.com.

McAfee Labs. "McAfee Labs Threats Report," 2015. www.mcafee.com/us/mcafee-labs.aspx.

McDonald, Matt. "Securitization and the Construction of Security." *European Journal of International Relations* 14, no. 4 (2008): 563–87. doi:10.1177/1354066108097553.

McGraw, Gary. "Cyber War Is Inevitable (Unless We Build Security In)." *Journal of Strategic Studies* 36 (February 2013): 109–19. doi:10.1080/01402390.2012.742013.

Melnitzky, Alexander. "Defending America Against Chinese Cyber Espionage Through The Use Of Active Defenses." *Cardozo Journal of International & Comparative Law* 20 (2012): 537–70.

Melzer, Nils. "Cyberwarfare and International Law," 2011. http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

Merelman, Richard M. "Technological Cultures and Liberal Democracy in the United States." *Science, Technology, & Human Values* 25, no. 2 (2000): 167–94. doi:10.1177/016224390002500202.

Meserve, Jeanne. "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid." *Cnn.com*, 2007. http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html?iref=topnews.

Metz, Cade. "Google Made a Chatbot That Debates the Meaning of Life." *Wired*, June 26, 2015. http://www.wired.com/2015/06/google-made-chatbot-debates-meaning-life/.

Mitchell, Timothy. "Society, Economy, and the State Effect." In *State/culture: State-Formation after the Cultural Turn*, 76–97. Ithaka: Cornell University Press, 1999.

Mol, Annemarie. "Actor-Network Theory: Sensitive Terms and Enduring Tensions." *Kölner Zeitschrift Für Soziologie Und Sozialpsychologie. Sonderheft* 50, no. 1986 (2010): 253–69. doi:10.1177/1745691612459060.

Monbiot, George. *Neoliberalism – the Ideology at the Root of All Our Problems*. Verso, 2016. http://www.theguardian.com/books/2016/apr/15/neoliberalism-ideology-problem-george-monbiot.

Moore, David, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver. "Inside the Slammer Worm." *Security & Privacy, IEEE* 1, no. 4 (2003): 33–39.

Morgan, Steve. "Cyber Crime Costs Projected To Reach $2 Trillion by 2019." *Forbes*, January 17, 2016. http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6900f7df3bb0.

Morgus, Robert. "NATO Tries to Define Cyber War." *Real Clear World*, October 20, 2014. http://www.realclearworld.com/articles/2014/10/20/nato_tries_to_define_cyber_war_110755.html.

Morrison, Aimée Hope. "An Impossible Future: John Perry Barlow's 'Declaration of the Independence of Cyberspace.'" *New Media & Society* 11, no. 1–2 (2009): 53–71. doi:10.1177/1461444808100161.

Mukherjee, Sangeeta. "Anonymous Threatens To Shut Down Internet On March 31 – April Fool Hoax Or Real Threat?" *IB Times*, March 31, 2012. http://www.ibtimes.com/anonymous-threatens-shut-down-internet-march-31-april-fool-hoax-or-real-threat-432468.

Müller, Martin. "Assemblages and Actor-Networks: Rethinking Socio-Material Power, Politics and Space." *Geography Compass* 1, no. September (January 2014): 1–20. doi:10.1111/gec3.12192.

Mumford, Lewis. *The Myth of the Machine: The Pentagon of Power*. Harcourt, Brace & World, 1970.

Murray, A. *The Regulation of Cyberspace: Control in the Online Environment*. Oxon: Taylor & Francis, 2007.

Nadeau, François. "Examining the Effects of Anti-Space Weaponization Arguments in the Media: Some Experimental Findings from Canada." *Space Policy* 29, no. 1 (February 4, 2013): 67–75. doi:10.1016/j.spacepol.2012.11.004.

Nakamoto, Satoshi. "Bitcoin : A Peer-to-Peer Electronic Cash System," 2008, 1–9.

Nakashima, Ellen. "CIA Web Site Hacked." *The Washington Post*, June 15, 2011. https://www.washingtonpost.com/national/national-security/cia-web-site-hacked/2011/06/15/AGGNphWH_story.html.

Nakashima, Ellen, and Steven Mufson. "Hackers Have Attacked Foreign Utilities, CIA Analyst Says." *The Washington Post*, January 19, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/01/18/AR2008011803277.html.

NASA. "Scientific Consensus: Earth's Climate Is Warming," 2016. http://climate.nasa.gov/scientific-consensus/.

National Academy of Sciences (NAS). *Computer Science and Telecommunications Board. Computers at Risk: Safe Computing in the Information Age.* Washington D.C.: National Academies Press, 1991.

NATO. "Active Engagement, Modern Defence." In *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted at the NATO Lisbon Summit*. Brussels: NATO Public Diplomacy Division, 2010. http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf.

———. "Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization." Lisbon, 2010. http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf.

———. "Wales Summit Declaration." Press Release 120, September 5, 2014. http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

NATO Review. "Cyberattack, NATO and Angry Birds." *Nato.int*, 2013. http://www.nato.int/docu/review/2013/Cyber/Cyber-attacks-NATO-angry-birds/CS/index.htm.

NCTA. "How Google Tracks Traffic." *National Cable & Telecommunications Association*, 2014. https://www.ncta.com/platform/broadband-internet/how-google-tracks-traffic/.

Netanel, Neil Weinstock. "Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory." *California Law Review* 88, no. 2 (2000): 397. doi:10.2307/3481227.

Nicholson, A., S. Webber, S. Dyer, T. Patel, and H. Janicke. "SCADA Security in the Light of Cyber-Warfare." *Computers & Security* 31 (2012): 418–36. doi:10.1016/j.cose.2012.02.009.

Nicolas Falliere, Liam O Murchu, and and Eric Chien. "W32.Stuxnet Dossier." Cupertino, 2012. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Nicoll, Alexander. "Stuxnet: Targeting Iran's Nuclear Programme." *Strategic Comments* 17 (2011): 1–3. doi:10.1080/13567888.2011.575612.

Nissenbaum, Helen. "Hackers and the Contested Ontology of Cyberspace." *New Media & Society* 6, no. 2 (2004): 195–217. doi:10.1177/1461444804041445.

———. "Where Computer Security Meets National Security." *Ethics and Information Technology* 7, no. 2 (2005): 61–73. doi:10.1007/s10676-005-4582-3.

Nolan, Steve. "Revealed: Google and Facebook DID Allow NSA Access to Data and Were in Talks to Set up 'Spying Rooms' despite Denials by Zuckerberg and Page over PRISM Project." *Daily Mail*, June 8, 2013. http://www.dailymail.co.uk/news/article-2337863/PRISM-Google-Facebook-DID-allow-NSA-access-data-talks-set-spying-rooms-despite-denials-Zuckerberg-Page-controversial-project.html.

Norton, Quinn. "2011: The Year Anonymous Took On Cops, Dictators and Existential Dread." *Wired*, January 11, 2012. http://www.wired.com/2012/01/anonymous-dicators-existential-dread/all/1.

Nowotny, Helga. "Democratising Expertise and Socially Robust Knowledge." *Science and Public Policy*, 2003. doi:10.3152/147154303781780461.

O'Leary, Timothy. "Foucault, Experience, Literature." *Foucault Studies*, no. 5 (2008): 5–25. http://cjas.dk/index.php/foucault-studies/article/viewPDFInterstitial/1422/1526.

Olssen, Mark. *MICHEL FOUCAULT - Materialism and Education*. *America*, 1999.

Orwell, George. *1984: A Novel*. New American Library, 1949.

Paganini, Pierluigi. "DB with Records of 50 Million Turkish Citizens Leaked Online. Are They Recycled Data?" *Security Affairs*, April 4, 2016. http://securityaffairs.co/wordpress/45981/data-breach/db-50-million-turkish-citizens.html.

Palermo, Elizabeth. "10 Worst Data Breaches of All Time." *Tom's Guide*, February 6, 2015. http://www.tomsguide.com/us/biggest-data-breaches,news-19083.html.

"Panic Postponed." *The Economist*, January 6, 2000. http://www.economist.com/node/327829.

"Paralelni Polis," 2016. https://www.paralelnipolis.cz/en/.

Parker, B. *Introduction to Globalization and Business: Relationships and Responsibilities*. SAGE Publications, 2005.

Partnership for Peace Consortium. "Hybrid Conflicts as an Emerging Security Challenge: Policy Considerations for International Security." PfPC Emerging Security Challenges Working Group Policy Paper No. 3, 2015.

Perrow, Charles. *Normal Accidents: Living with High-Risk Technologies*. Princenton: Princeton University Press, 1984.

Perthes, Volker. "Europe and the Arab Spring." *Survival* 53, no. 6 (November 15, 2011): 73–84. doi:10.1080/00396338.2011.636273.

Peters, Sara. "Questions Remain On How Cyberattack Caused Ukraine Blackout." *Information Week. Dark Reading.*, January 5, 2016. http://www.darkreading.com/attacks-breaches/questions-remain-on-how-cyberattack-caused-ukraine-blackout-/d/d-id/1323749.

Peterson, Dale. "Offensive Cyber Weapons: Construction, Development, and Employment." *Journal of Strategic Studies* 36, no. 1 (February 2013): 120–24. doi:10.1080/01402390.2012.742014.

"Petya Ransomware Encryption System Cracked." *BBC News*, April 11, 2016. http://www.bbc.com/news/technology-36014810.

Pfanner, Eric, and James Kanter. "Google Tries to Calm Europe Over Book Deal - The New York Times," September 7, 2009. http://www.nytimes.com/2009/09/08/technology/internet/08books.html.

Pickrell, Ryan. "A Dangerous Game: Responding to Chinese Cyber Activities." *The Diplomat*, September 29, 2015. http://thediplomat.com/2015/09/a-dangerous-game-responding-to-chinese-cyber-activities/.

Plassaras, Nicholas A. "Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF." *Chicago Journal of International Law* 14 (2013): 377–407.

Plato. *Alcibiades I & II*. 1st World Library Literary Society, 2004.

Pomerantsev, Peter, and Michael Weiss. "The Menace of Unreality : How the Kremlin Weaponizes Information , Culture and Money." New York, 2014.

Pouillot, Vincent. "'Sobjectivism': Toward a Constructivist Methodology." *International Studies Quarterly* 51, no. 2 (2007): 359–84.

Poulsen, Kevin. "Did Hackers Cause the 2003 Northeast Blackout? Umm, No." *Wired.com*, 2008. https://www.wired.com/2008/05/did-hackers-cau/.

———. "Slammer Worm Crashed Ohio Nuke Plant Net • The Register." *Theregister.co.uk*, 2003. http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke/.

Puglisi, William C. Hannas James Mulvenon Anna B. *Chinese Industrial Espionage*. Routledge, 2013.

Quentson, Andrew. "Panama Papers Scandal Shows How Bitcoin Could Stop Corruption." *Bitcoin.com*, April 4, 2016. https://news.bitcoin.com/panama-papers-bitcoin-stop-corruption/.

Ranger, Steve. "The New Art of War: How Trolls, Hackers and Spies Are Rewriting the Rules of Conflict." *Techrepublic.com*, 2016. http://www.techrepublic.com/article/the-new-art-of-war-how-trolls-hackers-and-spies-are-rewriting-the-rules-of-conflict/.

Rashid, Fahmida Y. "Inside The Aftermath Of The Saudi Aramco Breach." *Information Week. Dark Reading.*, August 8, 2015. http://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-

aramco-breach/d/d-id/1321676.

Rasmussen, Anders Fogh. "NATO's Next War—in Cyberspace," April 28, 2016. http://www.wsj.com/articles/SB10001424127887323855804578508894129031084.

Rathmell, Andrew. "Towards Postmodern Intelligence." *Intelligence and National Security* 17, no. 3 (2002): 87–104. doi:10.1080/02684520412331306560.

Rattray, Gregory, and Jason Healey. "Categorizing and Understanding Offensive Cyber Capabilities and Their Use." In *Proceedings of a Workshop on Deterring CyberAttacks : Informing Strategies and Developing Options for U. S. Policy*, edited by John D. Steinbruner. Washington, DC, USA: National Academies Press, 2010.

Reid, Edna Ferguson. *Why 2K?—A Chronological Study of the (Y2K) Millen- Nium Bug: Why, When and How Did Y2K Become a Critical Issue for Businesses?* Singapore: Universal, 1999.

Reid, Fergal, and Martin Harrigan. "An Analysis of Anonymity in the Bitcoin System." In *Security and Privacy in Social Networks*, 1–28, 2013. doi:10.1007/978-1-4614-4139-7_10.

Reuters. "Kim Dotcom Raid Illegal, New Zealand Court Rules." *The Telegraph*, June 28, 2012. http://www.telegraph.co.uk/technology/news/9361759/Kim-Dotcom-raid-illegal-New-Zealand-court-rules.html.

Reveron, D.S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Georgetown University Press, 2012. http://books.google.cz/books?id=v576FVMpdcAC.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (April 20, 2012): 5–32.

———. *Cyber War Will Not Take Place*. Hurst, 2013.

———. "Think Again: Cyberwar," 2012. http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=0,0.

Ring, Tim. "NATO Members to Get Cyber War Protection." *SC Magazine*, September 2, 2014. http://www.scmagazineuk.com/nato-members-to-get-cyber-war-protection/article/369026/.

Robertson, Jordan. "Three Things You Should Know About the Syrian Electronic Army." *Bloomberg*, March 24, 2014. http://www.bloomberg.com/news/articles/2014-03-24/three-things-you-should-know-about-the-syrian-electronic-army.

Rogin, Josh. "NSA Chief: Cybercrime Constitutes the 'greatest Transfer of Wealth in History.'" *Foreign Policy*, July 9, 2012. http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/?wp_login_redirect=0.

Roosth, Sophia, and Susan Silbey. "Science and Technology Studies: From Controversies to Posthumanist Social Theory." In *The New Blackwell Companion to Social Theory*, edited by Bryan S. Turner, 451–74, 2009.

Rosenau, James N., and J. P. Singh. *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, 2002.

Roth, Andrew L, Joshua Dunsby, and Lisa a Bero. "Framing Processes in Public Commentary on US Federal Tobacco Control Regulation." *Social Studies of Science* 33, no. 1 (2003): 7–44. doi:10.1177/0306312703033001038.

Russell, Bertrand. *Mysticism and Logic: And Other Essays*. Longmans, Green and Company, 1919.

Rustad, Michael, and Lori E. Eisenschmidt. "Commercial Law of Internet Security, The." *High Technology Law Journal* 10, no. 2 (1995): 213. doi:10.15779/Z38QX0H.

Ryan, J. *A History of the Internet and the Digital Future*. London: Reaktion Books, 2010.

Samadashvili, Salome. "Muzzling the Bear Muzzling the Bear. Strategic Defence for Russia's Undeclared Information War on Europe." Brussels, 2015.

Samuel, Alexandra Whitney; Aw. *Hacktivism and the Future of Political Participation*. Harvard University, 2004. doi:10.4324/9780203485415.

Sanger, D E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. Crown Publishing Group, 2012.

SANS ICS. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. SANS ICS, E-ISAC, Electricity Information and Analysis Center, 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Schmidt, Nikola. "A Sociological Approach to Cyberspace Conceptualization and Implications for International Security." In *Perspectives on Cybersecurity*, edited by Jakub Drmola, 70–77. Brno: Muni Press, 2015.

———. "Critical Comments on Current Research Agenda in Cyber Security." *Defense and Strategy* 14, no. 1 (2014): 29–38. doi:10.3849/1802-7199.14.2014.01.029-038.

———. "Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War." *Defense and Strategy* 14, no. 2 (2014): 73–86. doi:10.3849/1802-7199.14.2014.02.073-086.

———. "Super-Empowering of Non-State Actors in Cyberspace." In *World International Studies Committee 2014*, 5. Frankfurt: Goethe Universitat, 2014.

Schmitt, Michael N. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." *Harv. Int'l L.J. Online* 54 (2012). http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/.

"Security Snapshot Reveals Massive Personal Data Loss." *BBC News*, April 12, 2016. http://www.bbc.com/news/technology-36024570.

Settle, D M, and C C Patterson. "Lead in Albacore: Guide to Lead Pollution in Americans." *Science (New York, N.Y.)* 207, no. 4436 (1980): 1167–76. doi:10.1126/science.6986654.

Shackelford, Scott J. "Estonia Three Years Later: A Progress Report On Combating Cyber Attacks." *Journal of Internet Law* 13 (2010): 22–29.

———. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal of International Law* 27 (2009): 192–251.

Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. *Introduction to Cyber-Warfare*. *Introduction to Cyber-Warfare*, 2013. doi:10.1016/B978-0-12-407814-7.00010-5.

Shea, Jamie. "New Security Challenges And Nato's Future." *Turkish Policy Quarterly* 10 (2011): 53–59.

Shirky, Clay. "The Political Power of Social Media." *Foreign Affairs* 9, no. 1 (2010): 1–7.

"Should Governments Be Able to Look at Your Data When It Is Abroad? | The Economist." *The Economist*, 2015. http://www.economist.com/news/business-and-finance/21663902-test-case-set-determine-whether-fbi-can-access-microsofts-foreign-data-should.

Shu, Catherine. "Meet Telegram, A Secure Messaging App From The Founders Of VK, Russia's Largest Social Network." *Techcrunch.com*, October 27, 2013. http://techcrunch.com/2013/10/27/meet-telegram-a-secure-messaging-app-from-the-founders-of-vk-russias-largest-social-network/.

Singel, Ryan. "Richard Clarke's Cyberwar: File Under Fiction." *Wired.com*, 2013. http://www.wired.com/2010/04/cyberwar-richard-clarke/.

Sismondo, Serge. *An Introduction to Science and Technology Studies*. Wiley-Blackwell, 2010.

Smith, George. "An Electronic Pearl Harbor? Not Likely." *Issues in Science and Technology* 15, no. 1 (1998): 68–73.

Smith, Graham. "Hacking Group Anonymous Could Shut down the Entire U.S. Power Grid, Head of National Security Warns." *Daily Mail*, February 22, 2012. http://www.dailymail.co.uk/news/article-2104832/Hacking-group-Anonymous-shut-entire-U-S-power-grid-head-national-security-warns.html.

Smolin, Lee. *The Trouble With Physics: The Rise of String Theory, The Fall of a Science, and What Comes Next*. Houghton Mifflin Harcourt, 2007.

Snegovaya, Maria. "Putin's Information Warfare in Ukraine," no. September (2015): 28.

Snowden, Edward. "An Open Letter to the People of Brazil." *Pastebin*, December 17, 2013. http://pastebin.com/2ybz27UE.

Spafford, E. H. "Crisis and Aftermath." *Communications of the ACM* 32, no. 6 (1989): 678–87. doi:10.1145/63526.63527.

Stempel, Jonathan. "Google Defeats Authors in U.S. Book-Scanning Lawsuit." *Reuters.com*, November 14, 2013. http://www.reuters.com/article/us-google-books-idUSBRE9AD0TT20131114.

Stevens, Tim. "Apocalyptic Visions : Cyber War and the Politics of Time." *Available at SSRN*, 2013, 1–28. doi:10.2139/ssrn.2256370.

———. *Cyber Security and the Politics of Time*. Cambridge University Press, 2015.

Stohl, Michael. "Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?" *Crime, Law and Social Change* 46, no. 4–5 (2006): 223–38. doi:10.1007/s10611-007-9061-9.

Stoll, Cliff. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Doubleday, 1989.

Stone, John. "Cyber War Will Take Place!" *Journal of Strategic Studies* 36, no. 1 (November 10, 2013): 101–8. doi:10.1080/01402390.2012.730485.

Stromberg, Joseph. "The Forgotten History of How Automakers Invented the Crime Of 'jaywalking.'" *VOX*, January 15, 2015. http://www.vox.com/2015/1/15/7551873/jaywalking-history.

Sullivan, Gail. "Russian Hackers Steal More than 1 Billion Passwords. Security Firm Seizes Opportunity." *The Washington Post*, August 6, 2014. https://www.washingtonpost.com/news/morning-mix/wp/2014/08/06/russian-hackers-steal-a-billion-passwords-security-firm-seizes-opportunity/.

Symantec. "Internet Security Threat Report." Vol. 20, 2015. https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

Tabansky, Lior, and Isaac Ben Israel. "Striking with Bits? The IDF and Cyber-Warfare." In *Cybersecurity in Israel*. SpringerBriefs in Cybersecurity. Cham: Springer International Publishing, 2015. doi:10.1007/978-3-319-18986-4.

Telegram.org. "FAQ Telegram Security," 2016. https://core.telegram.org/techfaq#q-how-are-mtproto-messages-authenticated.

The~Economist. "All Eyes on the Sharing Economy." *9th March*, 2013.

———. "Digital Dilemmas," January 23, 2003. http://www.economist.com/node/1534303.

———. "Going Dark," January 17, 2015. http://www.economist.com/news/leaders/21639506-just-threat-terrorism-increasing-ability-western-security-agencies-defeat.

———. "Hackers Inc." *12th July*, 2014.

———. "Hacking the Banks," August 28, 2014. http://www.economist.com/news/business-and-finance/21614181-who-lies-behind-latest-cyber-attacks-jp-morgan-chase-hacking-banks.

———. "Imperial Ambitions," April 9, 2016. http://www.economist.com/news/leaders/21696521-mark-zuckerberg-prepares-fight-dominance-next-era-computing-imperial-ambitions.

———. "Leak of the Century: The Lesson of the Panama Papers," April 9, 2016. http://www.economist.com/news/leaders/21696532-more-should-be-done-make-offshore-tax-

havens-less-murky-lesson-panama-papers.

———. "Over to the Dark Side." *10th June*, 2013.

———. "Taking a Bite at the Apple," 2016. http://www.economist.com/news/science-and-technology/21693564-fbis-legal-battle-maker-iphones-escalation.

———. "The Great Chain of Being Sure about Things," October 31, 2015. http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable.

———. "The Terrorist in the Data." *28th November*, 2015.

———. "The Trust Machine," October 31, 2015. http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine.

———. "Uber Is Now More Popular than Taxis or Car Rental with Business People." *22nd January*, 2015.

———. "Unfriended." *12th December*, 2015.

———. "Winning the Battle, Losing the War," November 7, 2014. http://www.economist.com/news/business-and-finance/21631360-fbi-try-close-down-silk-road-again-winning-battle-losing-war.

TheWhiteHouse. "International Strategy for Cyberspace," 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

———. "The National Strategy to Secure Cyberspace." Washington, DC., 2003.

Thies, Wallace J. *Why NATO Endures*. Cambridge University Press, 2009. http://www.cambridge.org/cz/academic/subjects/politics-international-relations/international-relations-and-international-organisations/why-nato-endures.

Toffler, Alvin, and Heidi Toffler. *War and Anti-War: Survival at the Dawn of the 21st Century*. Boston, MA: Little Brown & Co., 1993.

Tothova Jordan, Klara. "NATO Must Boost Its Cyber Defense Capabilities Now." *Defense One*, September 11, 2014. http://www.defenseone.com/ideas/2014/09/nato-must-boost-its-cyber-defense-capabilities-now/93836/?oref=d-channelriver.

Trifonas, Peter Pericles. *Barthes and the Empire of Signs*. *Barthes and the Empire of Signs*. Totem Books, 2001.

Tung, Liam. "Microsoft Signs Deal to Let NATO Check Its Products for Backdoors." *Zdnet.com*, September 25, 2015. http://www.zdnet.com/article/microsoft-signs-deal-to-let-nato-check-its-products-for-backdoors/.

Unauthored. "Biggest Cybertheft in History Hits Banks." *WND*, February 16, 2015. http://www.wnd.com/2015/02/biggest-cyber-theft-in-history-hits-banks/.

Unknown. "Tom Cruise Scientology Video." *YouTube*, January 17, 2008.

———. "User Guide for Zeus Malware." *Pastehtml*. Accessed April 12, 2016. http://pastehtml.com/view/1ego60e.html.

USCC. "The National Security Implications of Investments and Products From the People's Republic of China in the Telecommunications Sector," 2011. http://www.uscc.gov/sites/default/files/Research/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf.

US-DoD. "Department Of Defense Strategy For Operating In Cyberspace," 2011. http://www.defense.gov/news/d20110714cyber.pdf.

VAN EETEN, MICHEL, ALBERT NIEUWENHUIJS, ERIC LUIIJF, MARIEKE KLAVER, and EDITE CRUZ. "The

State and the Threat of Cascading Failure Across Critical Infrastructures: The Implications of Empirical Evidence From Media Incident Reports." *Public Administration* 89, no. 2 (2011): 381–400. doi:10.1111/j.1467-9299.2011.01926.x.

Vanca, David. "Richard A. Clarke and Robert K. Knake's 'Cyber War: The Next Threat to National Security and What to Do About It,'" 2013. http://georgetownsecuritystudiesreview.org/2013/12/10/richard-a-clarke-and-robert-k-knakes-cyber-war-the-next-threat-to-national-security-and-what-to-do-about-it-harper-collins-2010/.

Vaseashta, A, P Susmann, and E Braman. *Cyber Security and Resiliency Policy Framework*. EBSCO Ebook Academic Collection. IOS Press, 2014.

Veeramachaneni, Kalyan, and Ignacio Arnaldo. "AI 2 : Training a Big Data Machine to Defend," n.d.

Verizon. *2012 Data Breach Investigations Report*. Verizon, 2012. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.

Volz, Dustin. "U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage." *Reuters*, February 25, 2016. http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K.

Wakefield, Jane. "Hello, I Am BBCTechbot. How Can I Help?" *BBC News*, April 12, 2016. http://www.bbc.com/news/technology-36024160.

———. "Whodunnit? The Mystery of the Sony Pictures Hack." *BBC.co.uk*, December 18, 2014. http://www.bbc.com/news/technology-30530361.

Warner, Michael. "Cybersecurity: A Pre-History." *Intelligence and National Security* 27, no. February 2015 (2012): 781–99. doi:10.1080/02684527.2012.708530.

Waterton, Claire, and Brian Wynne. "Knowledge and Political Order in the European Environment Agency." In *States of Knowledge: The Co-Production of Science and Social Order*, edited by Sheila Jasanoff, 87–108. London: Routledge, 2004.

Weathers, Cliff. "NSA's Massive Cyber-Spying Efforts Called 'Superhuman.'" *AlterNet*, February 17, 2015. http://www.alternet.org/civil-liberties/nsas-superhuman-cybersurveillance-network-exposed.

Wendt, Alexander. "Anarchy Is What States Make of It: The Social Construction of Power Politics." *International Organization* 46, no. 02 (March 1992): 391. doi:10.1017/S0020818300027764.

———. "The Agent-Structure Problem in International Relations Theory." *International Organization* 41, no. 3 (1987): 335–70. http://journals.cambridge.org/production/action/cjoGetFulltext?fulltextid=4309572.

———. "Why a World State Is Inevitable." *European Journal of International Relations* 9, no. 4 (2003): 491–542. doi:10.1177/135406610394001.

Westwood, Sallie. *Imagining Cities: Scripts, Signs, Memory*, 1997. doi:10.4324/9780203397350.

Wetmore, Jameson M. "Redefining Risks and Redistributing Responsibilities: Building Networks to Increase Automobile Safety." *Science, Technology, & Human Values* 29, no. 3 (2004): 377–405. doi:10.1177/0162243904264486.

White House. "National Presidential Directive 54." Washington D.C.: White House, 2008. http://fas.org/irp/offdocs/nspd/nspd-54.pdf.

Wickman, Gary, and Gavin Kendall. *Using Foucault's Methods*. London: Sage Publications, 1999.

Wiener, N. *The Human Use of Human Beings: Cybernetics and Society*. Da Capo Press, Incorporated, 1988.

Williams, Rhiannon. "Cyber Crime Costs Global Economy $445 Bn Annually." *The Telegraph*, June 9, 2014. http://www.telegraph.co.uk/technology/internet-security/10886640/Cyber-crime-costs-global-economy-445-bn-annually.html.

Windrem, Robert. "Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets." *NBC News*, July 30, 2015. http://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211.

Wishart, Ian. "NATO Tests Cyber-Defense Firepower to Combat Internet Terror." *Bloomberg*, November 20, 2015. http://www.bloomberg.com/news/articles/2015-11-20/nato-tests-cyber-defense-firepower-amid-fears-of-internet-terror.

Wistinghausen, Christian von. "Certification and Licensing of Encryption Software in the Russian Federation." *Rus Soft*, October 31, 2001. http://russoft.org/docs/?doc=88.

Wodak, Ruth. *The Politics of Fear*. SAGE Publications, 2015.

Wood, Jessica A. "The Darknet: A Digital Copyright Revolution." *Richmond Journal of Law and Technology* 16, no. 4 (2009): 1.

Woolgar, Steve. *Knowledge and Reflexivity: New Frontiers in the Sociology of Knowledge.* Thousand Oaks, CA, US: Sage Publications Inc., 1988.

Wyatt, Sally. "Danger! Metaphors at Work in Economics, Geophysiology, and the Internet." *Science, Technology, & Human Values* 29, no. 2 (2004): 242–61. doi:10.1177/0162243903261947.

Wynne, B. "Risk and Environment as Legitimatory Discourses of Technology: Reflexivity inside-Out." *Current Sociology* 50, no. 3 (2002): 459–77. doi:10.1177/0011392102050003010.

Wynne, Brian. *Risk Management and Hazardous Waste: Implementation and the Dialectics of Credibility*. London: Springer-Verlag, 1987.

———. "Seasick on the Third Wave? Subverting the Hegemony of Propositionalism." *Social Studies of Science* 33, no. 3 (2003): 401–17. doi:10.1177/03063127030333005.

Zeller, Mark. "Common Questions and Answers Addressing the Aurora Vulnerability." In *DistribuTECH Conference*. San Diego, CA, 2011. https://cdn.selinc.com/assets/Literature/Publications/Technical Papers/6467_CommonQuestions_MZ_20101209_Web.pdf.

Zetter, Kim. "FBI Fears Bitcoin's Popularity with Criminals." *Wired*, May 9, 2012. http://www.wired.com/2012/05/fbi-fears-bitcoin/.

———. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Zubrin, Robert. "The Case For Mars," 2012. doi:10.1016/0019-1035(85)90164-2.

ABSTRAKT

Tato dizertace studuje, jak se z kybernetické bezpečnosti stala agenda národní bezpečnosti a diskutuje implikace těchto procesů na mezinárodní bezpečnost. Práce je rozdělena do tří částí. První část rozebírá teoretický a metodologický přístup. Druhá část rozebírá tři různé diskurzy spojené s kybernetickou bezpečností, diskurz technologických nadšenců (techno-geek), diskurz kybernetické kriminality a špionáže a diskurz kybernetické národní obrany za pomocí metody známé z díla Michela Foucaulta Archeologie vědění. Třetí část následně diskutuje implikace zjištěné v empirické části za pomocí několika teoretických přístupů. Konkrétně z pohledu disciplíny studující vědu a technologii z perspektivy společenských věd (Science and Technology Studies – STS), z pohledu teorie ANT (actor-network theory) a síťových asambláží. Kritická část výzkumu se orientuje na různé pohledy konstitutivních funkcí jednotlivých diskurzů. Zatímco technologičtí nadšenci jsou vnímáni jako zdroj použitého jazyka tvořícího významové znaky (semiosis), následně kryptoanarchistickou ideologii ovlivněnou kyberpunkovou subkulturou, diskurz kriminality a špionáže je studován jako zdroj empirické evidence dovedností technologických nadšenců (geeks). Když jsou tyto dva světy zkombinovány, vzniká přehnaná imaginace na straně národních států, které primárně vnímají snahy technologických nadšenců se vyhnout zákonu vývojem tzv. osvobozujících technologií (liberating technologies), které jsou též používány k organizaci globálních kriminálních gangů. Důsledek těchto procesů je vznik přehnaných imaginací budoucnosti národní bezpečnosti bez ohledu na nedostatek empirických dat potvrzujících realizovatelnost katastrofických scénářů. Kybernetická bezpečnost jako národně bezpečnostní agenda byla schopna vytvořit oblast znalostí, které nejsou dokladem možnosti naplnění katastrofických scénářů, nýbrž součástí sociální konstrukce celé imaginace potenciální katastrofické budoucnosti. Expertíza, která vzniká na politický popud, daleko spíše odpovídá na tuto potenciální imaginaci namísto toho, aby doložila naplnění hrozeb vyplývající z technologických možností komunikačních technologií. Práce argumentuje tím, že nedůsledné oddělování imaginací stojících na kulturním základě namísto základu technicistně faktickým, způsobuje vznik nereálných scénářů vývoje národní bezpečnosti implikující žádost vzniku národní obrany kybernetické bezpečnosti. Nicméně důsledky jsou dalekosáhlejší v tom, že samotná iniciativa na straně států implikuje další iniciativu na straně technologických nadšenců (geeks), kteří vyvíjí další osvobozující technologie, jenž národní státy nejsou schopny efektivně regulovat. V důsledku toho vzniká organizovaná rezistence, kterou národní státy začínají vnímat jako potenciální líheň kybernetického terorismu čistě z důvodu jejich dovedností, ale bez ohledu na jejich zájmy. Nicméně tyto katastrofické zájmy pro národní státy jsou vidět v zájmech krypto-anarchistických hnutí. Následující vývoj má však zásadní dopady na vnímání charakteru liberálně demokratického státu západního typu. A to především po událostech, kdy globální sledování všech dostupných lidí v kyberprostoru tyto hodnoty přímo popírá, neboť nejen, že tyto operace přispívají ke vzniku utopického panoptikonu, ale též proto, že národní státy ztratily možnost tyto operace efektivně řídit. V případě, že státy nebudou schopny reagovat a regulovat vznik nových technologií efektivně a s respektem ze strany vzdorujících technologických nadšenců, je pravděpodobné, že svět se bude ubírat směrem hybridního vládnutí, do světa vlády tzv. oligoptikonu, ve kterém státy nebudou hrát roli suverénního globálního aktéra.