SIMARGL

# D3.2 Model of cyberspace dynamics

## Work Package 3: Legal, Social Sciences and Humanities Aspects of the SIMARGL Toolkit to Detect and Counter Malware and Stegomalware

Document Dissemination Level

| | | |
|---|---|---|
| P | Public | ☒ |
| CO | Confidential, only for members of the Consortium (including the Commission Services) | ☐ |

Document Due Date: 31/10/2019
Document Submission Date: 31/10/2019

This work is performed within the SIMARGL Project – Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware – with the support of the European Commission and the Horizon 2020 Program, under Grant Agreement No 833042

Document Information

| | |
|---|---|
| **Deliverable number:** | **D3.2** |
| **Deliverable title:** | Model of cyberspace dynamics |
| **Deliverable version:** | V1.2 |
| **Work Package number:** | WP3 |
| **Work Package title:** | Legal, Social Sciences and Humanities Aspects of the SIMARGL Toolkit to Detect and Counter Malware and Stegomalware |
| **Due Date of delivery:** | 31/10/2019 |
| **Actual date of delivery:** | 31/10/2019 |
| **Dissemination level:** | PU |
| **Editor(s):** | Nikola Schmidt (IIR) |
| **Contributor(s):** | IIR, ITTI |
| **Reviewer(s):** | Michal Choras (FUH) |
| **Project name:** | Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware |
| **Project Acronym** | SIMARGL |
| **Project starting date:** | 1/5/2019 |
| **Project duration:** | 36 months |
| **Rights:** | SIMARGL Consortium |

Version History

| Version | Date | Beneficiary | Description |
|---|---|---|---|
| **1.0** | 9/10/2019 | IIR | First draft of the whole document before cutting down to more policy relevant text |
| **1.1** | 10/10/2019 | IIR | Added table of flowing perceptions between discourses |
| **1.2** | 30/10/2019 | IIR & CUING | Added Annex and rewritten core text |

# Table of Contents

# 1. Executive summary

Following the document concerning actors in cyberspace, we have developed a novel analysis of how the activity in cyberspace can be interpreted. Beside the classical alarmist perceptions based on imaginations that everything can be done in cyberspace with specific knowledge, we are proposing a perspective that the power is not necessarily in the critical knowledge of selected hackers or group of hackers or state actors or anybody that is capable to deliver a cyber attack and that can be delimited as an actor in cyberspace but in a growing networked assemblage of actors. These assemblages are specific in its ungraspable shape because their existence is not institutionalized but flow through cyberspace as each actor does something else in different contexts, for example by creating new dark ecosystem of tools, instruments, knowledge, software utilities while having a common work in IT company. Roles and interests are flowing, people are meeting sometimes in different roles online but never establish traditional institutionalized social structures. The analysis we provide is not uncovering "a new truth" or denounce the current traditional perspective of cyber super powers, however, at the same time we do challenge the perceptions of possible cyber Pear Harbours or any other doom scenarios because they are the most reductionist perceptions we can imagine behind the possibilities of a completely new technology.

The technology that enables cyberspace is changing everyday, the habits of people using them as well, our dependence on various technologies lead our preferences of certain technologies but at the same time make us blind when we need to understand what technologies can be used against our way of life. However, the new power assemblages probably do not share the way of life governments prefer but is hard to say that what a government prefers is what a society prefers. This power of preference can change the way how we live simply because people will prefer technology that is not under control of a government. Is it good or bad? It definitely challenges the role of governments and the classical social contract between us – the society – and those we elect as it challenges the common principles of democratic legitimacy. People can openly decide to use cryptocurrencies that nobody governs or a cryptocurrency Libra that Facebook wishes to introduce, however, exactly Libra shook with traditional institutions because a mere preference can significantly lower their relevance and European Central Bank recently decided to act. Here, we would like to show that the introduction of a technology that is for some "a liberation technology" can be for the democratically elected entity "a dark technology" capable to topple down traditional institutions. Thus, the focus in cyber security discourse on what cyber attack can be conducted by unlimited amount of god-like capable hacker mises the point social science scholars should put emphasis on. The possible power shift is what should be discussed, not the capabilities to conduct a single cyber attack.

The whole document shows how various discourses between various epistemic communities develop various perceptions on cyber security. The final part opens new questions that we believe should be the basis for further policy of European Union.

# 2. Introduction

## 2.1 Motivation

The motivation behind this document is to uncover the dynamics of discourse formation that later forms new social reality in an imagination of it related to cyber security. Such uncovering helps us to develop a novel argument based on power source rather than the seriousness of certain cyber attacks.

## 2.2 Intended audience

We believe that this shift of perception on cyber space form analysing consequences of certain cyber attacks on power analysis of network assemblage will help to address the problem with a completely novel policy. Policy makers tend to extinguish fires made by state actors incapability to govern technology evolution, however, the problem will only grow if policy makers do not adopt a perception that the problem is not in the technology or in selected hackers but in the power shift the

technology provides. Thus the audience for us is the policy makers that advise elected people in EU shaping cyber security policy.

### 2.3 Relation to other deliverables

The document directly builds on D3.1.

### 2.4 Structure of the deliverable

This document, though quite more theoretical, begins with literature review on critical cyber security studies to attune the reader to the way of thinking the whole document is using. The following part uses concepts from Science and Technology Studies that analyses a relation between states, technology and governability, how the production of knowledge is influenced by the consumers. The apparent distinction can be recognized in producing expertise based on request of policy makers and expertise driven by curiosity. The problem of boundary work where certain group of people within their epistemic community tend to reproduce already established knowledge for the problem of in-group status etc. Then we apply such perspective on how knowledge related to cyberspace has been developed and why all this matter in policy making related to cyber security. The next part on archaeology of discourse will use Foucault's method of discourse analysis. This clearly theoretical part has a solid position in the whole document because in visible shows how the imagination introduced in the previous document, imaginations based on cyberpunk subculture, can influence the way how we think and talk about cyber security related to national security. This part will show how discourse can materialize in power but finally the next part will show that the power of the enemy, or of those that can influence the way we live, materialized differently, not through discourse but through tools the network assemblages are using, how they flowing across each other by using these tools and how those people produce isolated worlds capable to significantly influence our way of living without capability to be influenced by elected entities possessing democratic legitimacy.

## 3. 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 inclines to post-structuralist works analyzing imaginations, their connection to the threat construction based on potentialities and pre-emptive reaction that builds on speculations. We are listing inspirational writings that significantly influenced our thinking in order to use them in further analysis; it is not meant to be an extensive literature review on critical studies in cyber security.

The social construction theory has its roots in the sociology of the 60s, when Peter Berger and Thomas Luckmann wrote their famous book *The Social Construction of Social Reality*,[1] which was later applied to the theory of international relations prevalently by Alexander Wendt[2] 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,[3] in which Giddens introduces 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

[1] Berger and Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*.

[2] Wendt, "The Agent-Structure Problem in International Relations Theory."

[3] Giddens, *The Constitution of Society*.

neorealists was that the *Anarchy is What States Make of It*.[4] It is a mind that construct the reality or explanations of the reality that is familiar to us. Following these ideas, the Copenhagen school team led by Barry Buzan then established a new methodological framework on 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*.[5] 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."*[6] The concepts are studied in the perspective of how they have been brought to the political reality within the national security discourse, which is finally exactly the point of our further research, which we are methodologically enriching using the method of Michel Foucault on discourse analysis explained in his book *The Archaeology of Knowledge*[7] (to be discussed in detail below).

When the cyber threats have become a topic, some scholars used the Copenhagen school to establish some particular key concepts related to the new security topic.[8] Helen Nissenbaum and Lene Hansen did a respectful work when they applied the 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. [9] We 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 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,[10] 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 policymakers 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 also used 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.[11] 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.[12]

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, the information age in contrast to the industrial age seems to produce

[4] Wendt, "Anarchy Is What States Make of It: The Social Construction of Power Politics."

[5] Buzan et al., *Security: A New Framework for Analysis*.

[6] Buzan et al., 25.

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

[8] Hansen and Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School."

[9] Hansen and Nissenbaum, 1157.

[10] Dunn, "The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)."

[11] Cavelty, "Cyber-Terror--Looming Threat or Phantom Menace? Th."

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

much more complex and hard-to-comprehend knowledge giving the metaphors more space to engulf more content and thus more stories or shocking narratives.[13] 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[14] which are, for example, based on (inspirational, but certainly very fictional) writings such as Alvin and Heidi Toffler.[15] 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.[16] One of such adaptation is a strategy in which *"deterrence now has to be based on prevention."*[17] 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.[18] 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 policymakers 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.[19] 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 the 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,[20] then as a scientific article in Journal of Strategic Studies[21] and then as a book, in which he uses particular events in history to underscore his argumentation.[22] 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 have 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,[23] 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

[13] Bousquet and Curtis, "Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations."

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

[15] Toffler and Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*.

[16] Cebrowski and Garstka, "Network-Centric Warfare : Its Origin and Future."

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

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

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

[20] Rid, "Think Again: Cyberwar."

[21] Rid, "Cyber War Will Not Take Place," April 20, 2012.

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

[23] Stone, "Cyber War Will Take Place!"

a man over a man", which does not need to include lethality.[24] Cyber war thus can be violent, but does not need to be as lethal as conventional war. That violence is enough to call it war. Bernard Brodie argues in context with the Cold War that the principal problem of strategists is the question "will the idea work"?[25] 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 our opinion – unanswered. We 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 a cool head, Thomas Rid is proposing a 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 the Atlantic Council in Washington D.C. contributed with an interesting categorization of responsibility scale for a nation state in a case of a cyber-attack,[26] he has also been productive in the application of military strategies into cyberspace.[27] 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."*[28] Such an approach is exactly what Gartzke and others criticize. Moreover, to demonstrate that link Healey created analogue models called Cyber Pearl Harbor and 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".[29] Lawson criticized this boom of doom scenarios after the Estonia 2007 cyber-attack a 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 puts through the idea of fortification, centralization and control-oriented policy in order to develop the suggested "internet control switch".[30]

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.[31] And if they do, it is highly possible that attacks causing blackout will be easily repaired and energy quickly restarted.[32] This in fact happened in December 2015 in Ukraine two years after Gartzke wrote his article and is the point of our further analysis in the empirical part. Gartzke also shifts 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[33] and that cyber-attacks are extremely unlikely to be decisive.[34]

---

[24] Arendt, "On Violence."

[25] Brodie, *War and Politics*, 452.

[26] Healey, "The Spectrum of National Responsibility for Cybera."

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

[28] Rattray and Healey, 97.

[29] Cavelty, *Cyber-Security and Threat Politics: US Efforts To*.

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

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

[32] Gartzke, 57.

[33] Gartzke, 63.

[34] Gartzke, 68.

If we come back to imaginations, they have been very inspirationally analyzed by Robert Kaiser in the article Birth of Cyber War.[35] 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 in 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 possesses 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.[36] 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 thought.[37] 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',[38] which they drew on Ulrich Beck's theorization of uncertainty.[39] According to Aradau and Munster *"imagination creates the future as a new epistemic 'reality' by mediating between the senses and understanding,"*[40] towards policy of normalized reaction. The point is not to produce politics of fear, but rather through politics of catastrophe[41] be prepared for events on which we react with normalized reactions. Possessing knowledge is what dissolves the catastrophe as the event is anticipated, thus they talk about a possible anticipator regime created through fear and pleasure. Fear, that reacts on unknowns and pleasures produced through theatrical exercises producing knowns.[42] Under that perspective, imaginations are perceived as a needed preventive and predictive models[43] and thus even science fiction writers aside the governmental officials are understood as "*indispensable to the pursuit of knowledge and the problematization of the unknown*."[44] However, as we will show later it is hard to balance between a 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*.[45] As Stevens perceives 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."*[46] According to Stevens, the *catastrophic*

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

[36] Kaiser, 17.

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

[38] Aradau and Munster, 6–7.

[39] Beck, "Risk Society: Towards a New Modernity."

[40] Aradau and Munster, *Politics of Catastrophe*, 84.

[41] Aradau and Munster, 112–13.

[42] Aradau and Munster, 85.

[43] Aradau and Munster, 68.

[44] Aradau and Munster, 69.

[45] Stevens, "Apocalyptic Visions : Cyber War and the Politics of Time."

[46] Stevens, 2.

*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 discursive practices, which we are using later in this 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.[47] 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,[48] 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."[49] 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 a different light.

The next important contribution to the critical perception that influenced significant 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.[50] We are using this division to analyze each discourse. The point of Myriam is that each group of people approached 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 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?"*[51]

Rod Deibert in a reaction to the Snowden revelations[52] 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 the norm of free speech by the Western world is jeopardized two folds. First, by the West through its unveiled massive surveillance hydra, however, second, by the new South with its authoritarian regimes, which never asked a question of 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.[53] 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

[47] Stevens, 8–9.

[48] Stevens, *Cyber Security and the Politics of Time*.

[49] Stevens, 160.

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

[51] Cavelty, 150–51.

[52] Deibert, "The Geopolitics of Cyberspace after Snowden."

[53] Deibert, 12.

of future development. Such a situation awaits analysis from a perspective of the related actors and our 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 trying to shape 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 states focused on their historical evolution and a problem-solving one focused on an analysis of how the current institutional architecture should work smoothly.[54] Despite the fact that we are trying to provide a reader with a particular insight which should help to narrow the current cyber security policy with a cool head, our central aim is exactly the first one, a critical approach describing the historical evolution and the genealogy of current state. The text is not trying to solve how particular institutions should operate, but trying to explain – and thus understand – how the current policy architecture to solve cyber security issues came about and what does it mean for world politics. We are rather providing a specific reading with possible implications of current policy that produce *hypersecuritization* effects. To be concrete, we are 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."*[55]

The main argument of this document 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 the 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 the form of a growing resistance within ultra-libertarian world and crypto-anarchist movement. The analysis 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 not exactly our concern here. We are not going to denounce that moves; our 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 research. We are not doing that deliberately and if you find such a discussion inside, please understand it as a comment, which we could not be silent about. The core of the analysis focuses on a discourse formation, its co-production, consequent power materialization and finally the debate of its possible implications on world politics.

We are using one prevalent epistemological approach based on Foucault's method of knowledge production. The aim is to unveil the dynamics between cyber-technologically related knowledge production for policymakers 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.

---

[54] Cox, "Social Forces, States and World Orders: Beyond International Relations Theory," 129.

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

# 4. Construction of security crises under technological radical uncertainty

## 4.1 Theoretical and conceptual framework from STS

Science and Technology Studies (STS) is a discipline closely related to a centuries or millennia long debate concerning the philosophy of science. Its relation to the philosophy of science is the assessment of how particular knowledge has been produced within a particular scientific community. The three steps in the modern historical development of the philosophy of science in the 20th Century can be considered important. First, the logical positivism, which has 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 the 20s within the Vienna Circle and the Berlin Society for Empirical Philosophy.[56] 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.[57] The only cognitively meaningful knowledge was by the logical positivist 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 lasted 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.[58] 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 of observations and thus later more radical to positivism, the social construction.[59] 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*[60] 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 the 60s with a revolutionary perspective of a paradigm as a response to logical positivism.[61] In his thought, the efforts to develop scientific knowledge is dependent on a viewpoint of a particular researcher. The research then develops 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 paradigms to the examined phenomena researchers conduct a revolutionary science, which should be to Kuhn the most desired approach of any researcher. During the process of analysis 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

---

[56] The Prehistory of Science and Technology Studies In Sismondo, *An Introduction to Science and Technology Studies*.

[57] Russell, *Mysticism and Logic: And Other Essays*.

[58] Durkheim, *The Rules of Sociological Method*.

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

[60] Latour, *Politics of Nature: How to Bring the Sciences Into Democracy*.

[61] Kuhn, *The Structure of Scientific Revolutions*.

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.

In the same decade of 60s, 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 World War II, which won thanks to extremely successful technological innovations that led to the invention of the nuclear bomb, but then sparked resistance in anti-nuclear and environmentalist movement of the 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 do not constitute the context, but also content of science.[62] Later on, scholars added to this claim that government policies and programs create expert authority to particular scientific disciplines.[63] 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 becomes *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 of 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.[64] As 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"*[65] 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.[66] 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 research in their research proposals in order to conform the so-called applicable science, thus they are forced to use analogical reasoning, they need to manipulate with concepts using analogy and metaphors[67] 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 and they are therefore 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.[68] 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.

---

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

[63] Wynne, *Risk Management and Hazardous Waste: Implementation and the Dialectics of Credibility*; Hilgartner, *Science on Stage: Expert Advice as Public Drama*.

[64] Latour and Woolgar, *Laboratory Life*.

[65] Knorr-Cetina and Mulkay, *Observed: Perspectives on the Social Study of Science*.

[66] Woolgar, *Knowledge and Reflexivity: New Frontiers in the Sociology of Knowledge.*

[67] Knorr-Cetina, *The Manufacture of Knowledge: An Essay on the Constructivist and Contextual Nature of Science*.

[68] Latour, *Science in Action: How to Follow Scientists and Engineers Through Society*.

Additionally, if these scientific facts are socially constructed they should also be contestable, they should also have a value oriented assessment of 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."*[69]

As the whole document aims on a question of how the uncertainty of new technology implications in society gave birth to cyber as a national security agenda, relations between technology and society, interpretation or social construction of its consequences and the dynamics of 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.[70] Similar concerns inspired scholars introducing concepts like *ethno-epistemic assemblage*,[71] where both, science and society, are co-constructed, or differently said mutually constituted. As ideas of scientists develop technologies that have a 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 in which they are used, understood, treated and finally governed. In the automotive 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 a 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[72] producing also a web of responsibility. In cyber security discourse, especially from the one on the national security level, policymakers 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. States then force operators to run particular technologies in accordance with standards and specific law that mark their systems as critical to the national security – thus the birth of the term *critical infrastructure*. All of this has been done the whole world over to different extents without witnessing serious attacks that have been disturbing critical infrastructures. There are examples of "huge" cyber-attacks 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 the Ukrainian blackout.[73]

## 4.2 States, technology and the governability

Foucault, as will be shown below, is used as a theoretical-methodological lens through which we can perceive the formation of discourse leading to the birth of the cyber security agenda in discourse. Concepts used by the actors of discursive practices are analyzed and deconstructed in their historical evolution, however, a particular conceptual framework is taken from the sociological approach of science and technology (STS), especially sociology of its governance. In the end of the document, we combine three pillars in the analysis. First, the sociology of technology governance as a conceptual framework that provides us with analytical tool in approaching, second, the 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 a crucial role in construction of threats when combined with the social aspect, especially the presumptive (e.g. hackers') intentions based on opportunities. As the grasp or definition of the needed corpus of knowledge is hard to

[69] Hacking, *THE SOCIAL CONSTRUCTION OF WHAT ?*, 6.

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

[71] Irwin and Michael, *Science, Social Theory and Public Knowledge*.

[72] Wetmore, "Redefining Risks and Redistributing Responsibilities: Building Networks to Increase Automobile Safety."

[73] SANS ICS, *Analysis of the Cyber Attack on the Ukrainian Power Grid*.

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*.[74]

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 continues to deepen, it is impossible to purify the needed knowledge. The idea of compact knowledge regarding particular discipline has become utopia. As Ezrahi put it at the beginning of the 90s, the employment of science and technology in support of liberal democracy had become debatable by the end of 20th century.[75] However, it was brave argumentation especially at the end of Iron Curtain that according to general consensus in 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 the late 40s and early 50s, when the national US policy strongly focused on technology development as national security policy in a reaction to 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 the 50s,[76] 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 – destruction.[77] As Sheila Jasanoff put it, science and technology permeate the culture and politics of modernity.[78]

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 to constructed security discourse and 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[79] are becoming very questionable policy approaches, because any artificial intelligence cannot make a choice from 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.* [80] 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.[81] Governance of science and technology development is not only about the bureaucracies that help scientists and technology researchers 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 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

[74] Latour, *We Have Never Been Modern*.

[75] Ezrahi, *The Descent of Icarus: Science and the Transformation of Contemporary Democracy*.

[76] Merelman, "Technological Cultures and Liberal Democracy in the United States."

[77] Applebaum, "Mark Zuckerberg Should Spend $45 Billion on Undoing Facebook's Damage to Democracies."

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

[79] Kumar, "DARPA Challenges Hackers to Create Automated Hacking System — WIN $2 Million."

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

[81] Veeramachaneni and Arnaldo, "AI 2 : Training a Big Data Machine to Defend."

significance of *decentralized networks of power assemblages*. Every attempt to regulate this decentralized network assemblage is easily answered by technology developments 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.[82] This uncertainty produces 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[83] 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 cyberspace by adopting strict laws regulating its usage.[84] However, technological characteristics and the pace of the technological development of communication technologies will probably lead into a deeper inability to control the flow of information and proliferation of what we call liberating technologies; the technological answer to regulations. As a reaction, some undemocratic countries, for example, started to pour disinformation into the political debate in newly studied hybrid warfare rather than keep a mere blocking of undesirable information.[85]

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.[86] 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.[87] 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 a 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[88] just after World War II as a response to president Roosevelt, technology brought us a victory over Nazism by 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 military research, that scientific research is the main driver for further well-being of American people, the main driver of employment and for security. He certainly helped with the rise of the optimism in the technology determinism as a driver of post-war national security policy, which was quickly spread to Europe through the Marshall plan. However, during this time some had argued conversely. This opposite way of thinking is known today as

---

[82] Jasanoff, *Designs on Nature: Science and Democracy in Europe and the United States*.

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

[84] Endeshaw, "Internet Regulation in China: The Never-ending Cat and Mouse Game1"; Murray, *The Regulation of Cyberspace: Control in the Online Environment*.

[85] Schmidt, "Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War."

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

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

[88] Bush, *Science - The Endless Frontier*.

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.[89] Since we have been witnessing an 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."*[90]

The 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 by the relation between concepts *scientific governance* and *scientific democracy*.[91]

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

## 4.3 Policy makers and the relevant knowledge

When the capability to govern sociotechnical development seems to be decentralized and ungovernable by a 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*.[92] What kind of knowledge had been produced in that time? To what subject was the knowledge related? And who profited from the new norm establishment?

In sociotechnical areas *legitimate knowledge* is related to hereafter mentioned concept of *boundary work*[93] where the idea of production of a *good science* can be found and thus the particular actor is

[89] Mumford, *The Myth of the Machine: The Pentagon of Power*.

[90] Jasanoff, *Designs on Nature: Science and Democracy in Europe and the United States*, 14.

[91] Irwin, "Constructing the Scientific Citizen: Science and Democracy in the Biosciences."

[92] Lewis, "Jaywalking: How the Car Industry Outlawed Crossing the Road"; Stromberg, "The Forgotten History of How Automakers Invented the Crime of 'Jaywalking.'"

[93] Gieryn, *Cultural Boundaries of Science: Credibility on the Line*.

given a legitimacy to interpret, manipulate, evaluate, reproduce and implement knowledge on solutions of problems, which might 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 an institution, the legitimate knowledge for risk assessment can be possessed by *epistemic communities*[94] 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[95] and criticized.[96] The fact that the experience is detached from expertise produces two different perspectives and thus knowledge that leads to decision-making under conditions of *radical uncertainty*.[97] However, delivery of knowledge to policymakers by specialist possessing specific expertise has been studied as successful stories, e.g. AIDS,[98] 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 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.[99] His enemy was a scientist paid by oil companies Robert Kehoe to sow doubt. Despite 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 the unhealthy way of civilization development where logic of naturally renewable sources would be certainly long-lasting with less impact on the environment then non-renewable energy sources (in their ideal form).

In that perspective, a *relevant knowledge* for policymakers 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 is usual in basic research. The story between world saviors and oil companies has not finished yet as the continuous questioning of the raising evidence of need for renewables is still underway and include nicely calculable bunch of self-convincing evidences.[100] 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 argued acquiring the specific knowledge in cyber security is a daunting task.[101] 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 attention. As Nissenbaum argued elsewhere, we have observed a shift from hackers as wise geeks to

[94] Kastenhofer, "Risk Assessment of Emerging Technologies and Post-Normal Science."

[95] Collins and Evans, "The Third Wave of Science Studies: Studies of Expertise and Experience."

[96] Jasanoff, "Breaking the Waves in Science Studies: Comment on H.M. Collins and Robert Evans, `The Third Wave of Science Studies'"; Wynne, "Seasick on the Third Wave? Subverting the Hegemony of Propositionalism."

[97] Irwin, *Expertise in Law and Regulation*.·

[98] Epstein, *Impure Science: AIDS, Activism and the Politics of Knowledge*.

[99] Settle and Patterson, "Lead in Albacore: Guide to Lead Pollution in Americans."

[100] Lomborg, "Don't Be Fooled - Elon Musk's Electric Cars Aren't about to Save the Planet."

[101] Nissenbaum, "Where Computer Security Meets National Security."

hackers as terrorists,[102] clear securitization, which is a move that Deibert understands as unsecurutizable.[103] Such move encircles all activities of hackers as being equal to terrorist intentions, at least for a selected audience.

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 policymakers as in the success story of Patterson, but favors the threat that politics based on doomy imaginative scenarios plays 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 require a scientific answer within a cultural boundary of expected scientific facts. One of the reasons why we depend on these imaginations is the so-called *attribution problem,* which is today understood as an unbeatable characteristic of all cyber-related events. The attribution problem, which poses an almost unanswerable question about whom has been behind the attack, is fairly irresolvable in the current technological setting of the Internet. However, one of the obstacles behind the 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.[104] 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 and as Gatzke argued, these examples show us that even serious cyber-attacks 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 the 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*.

## 4.4 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 environments (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.

[102] Nissenbaum, "Hackers and the Contested Ontology of Cyberspace."

[103] Deibert, "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace."

[104] Firestone, "In Cyberspace, Anonymity and Privacy Are Not the Same."

Maybe this statement is not precise and fair, as physics does currently have serious problems on where to evolve as string theory has brought a perspective of an uncountable amount of solutions related to an uncountable amount of events and particles or that the standard model is hardly compatible with quantum physics.[105] We might have had some shortcomings in medicine before the first heart transplantation, but we have solved it and already pose knowledge on how to successfully transplant a heart; we already poses a compact knowledge that works in a practical way to achieve a clear objective – to transplant a heart, but the objective is clearly a 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[106] which brings quite serious problems to its governability. When it comes to cyberspace there is also an ongoing debate over whether it supposes to be governed by governments or left to self-governability.[107] This debate is quite huge and will be elaborated on later; however, one point is important here. As cyberspace is fluidly changing so quickly, the ability to govern is significantly limited. It is not only about the complexity, but also 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[108] followed by particular nations, but they may not be able to govern cyberspace completely, especially branches of cyberspace that belongs to and are governed by people seeking ultimate liberty in cyber anarchism[109] 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 the future shape of cyberspace. That requirement exceeds the inability of governance, it becomes utopia.

The technical capability of individual people can seriously exceed the capability of state employed experts that super-empowers them as well.[110] When we come back to threat analysis in cyberspace in this perspective, the ability to assess threats coming from particular sub-disciplines of computer science do not critically require all other knowledge in a wide compact manner, but a critical amount of certain knowledge. Young hackers, so called *script kiddies* were able to cause a lot of damage,[111] but also probably whole armies of hackers were able to cause larger damage to national infrastructure.[112] One may raise a question what is damage in cyberspace as there is 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.[113] In summary, what is important on the digital world of computers is its quick change that gathering comprehensive and compact expertise in a

[105] Smolin, *The Trouble With Physics: The Rise of String Theory, The Fall of a Science, and What Comes Next*.

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

[107] Deibert and Rohozinski, "Liberation vs. Control: The Future of Cyberspace"; Deibert and Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls"; Netanel, "Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory."

[108] EU, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace."

[109] Halpin, "The Philosophy of Anonymous: Ontological Politics without Identity."

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

[111] Calce and Silverman, *Mafiaboy: How I Cracked the Internet and Why It's Still Broken*.

[112] Kampmark, "CYBER WARFARE BETWEEN ESTONIA AND RUSSIA."

[113] 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.

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 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,[114] but some particular successful occurrences are available in the literature.[115] However, these boundaries are being attacked by policymakers to produce deliberately value-oriented results or otherwise, the result by the *epistemic authority* was excessively absorbed as unchallengeable scientific *truth* by policymakers. Boundaries can be raised around the whole organizations that possess unchallengeable authority to assess particular problems even though the whole organization does not harbor experts with appropriate expertise. Moreover, the expertise appropriateness can be devised from conformity. Sometimes experts are not willing to contribute to the political process, but despite that policymakers 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;[116] 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.[117] 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.[118]

Erwing Goffman's sociological concept of *framing*[119] is used in a context with STS as *collective action frames* where particular actors mobilize and counter-mobilize ideas and meanings[120] 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 at 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 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 a fluidly changing cyber realm of mutually constitutive iterative process between habits of users and technology evolution, but also in

---

[114] Irwin and Wynne, *Misunderstanding Science*.

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

[116] Waterton and Wynne, "Knowledge and Political Order in the European Environment Agency."

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

[118] Lynch, "Circumscribing Expertise: Membership Categories in Courtroom Testimony."

[119] Goffmann, *Frame Analysis: An Essay on the Organization of Experience*.

[120] Roth, Dunsby, and Bero, "Framing Processes in Public Commentary on US Federal Tobacco Control Regulation."

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 the 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 differences between governmental research driven by risk and scientific research driven by curiosity.[121] She elaborated this criticism of advisory boards serving policymakers, which are in fact policymakers themselves.[122] 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 events in recent history.[123] Emotions and fears drive nation states into a state of fluid post-modern non-governability.

Experts driven by policy rather than curiosity have shared interests – to introduce the world to a threat they are capable of dealing 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 a 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 as such are powered by adopting knowledge, they previously created through grouping the *best* experts in the field.

The *boundary* within such cyber related institutions serve to construct 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.

## 5. Archaeology, genealogy and the rules of discourse

Based on Foucauldian perspective this 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 document we study the evolution of cyber security, the genealogy of discourse that gave the birth to cyber security as a national security agenda. Taking Foucault's approach means that we 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? We will define some starting points of its origin to unveil present materialization rather than to describe the

[121] Jasanoff, "Technologies of Humiliation: Citizen Participation in Governing Science."

[122] Jasanoff, *The Fifth Branch: Science Advisers as Policy- Makers*.

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

discourse production as an historical period. We use Foucault's archaeological approach to study the discourse and how this discourse has formed a new material world – new institutions, new technologies, and new authorities. This perspective helps us to analyze statements of particular politicians or statesmen having a significant impact on further policy development; discourses as practices, as *"the general system of the formation and transformation of statements."*[124]

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 artefacts 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.[125]

The methodological procedure of the analysis 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*. The objective is to use Foucault's approach to formation of new concepts and use them in further reading of discourse.

## 5.1 Formation of new concepts through successive series of statements

Being able to advance from the beginning, we will describe the methodological approach in layers. On the first layer, we 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. We focus on the *formation of new concepts*[126] 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 the *church of knowledge* that is the foundation of security assessment and thus the new political agenda. What do we mean with the concept the *church of knowledge we* currently introduced? When we talked about the circulation of discourse within a 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.[127] Foucault wanted to have read his books as a flow of experience and they particularly have a specific language, in which Foucault consequently uses adjectives in series to precisely depict his current experience of thought. When we 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, we 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[128] or experience[129] are critical.

Foucault distinguishes between two kinds of knowledge that are distinguishable in the French language. The distinction between *connaissance* and *savoire*.[130] In the former meaning, knowledge means knowing a thing, to understand that the 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 of how to

---

[124] Foucault, *The Archeology of Knowledge*, 130.

[125] Wickman and Kendall, *Using Foucault's Methods*, 26.

[126] Foucault, *The Archeology of Knowledge*, 62–71.

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

[128] 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.

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

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

use a wheel and anticipate the consequences, it provides him/her with power.[131] In our context, it is a political power of 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 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"*[132] 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."* [133] 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. The 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 advantages 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 themselves as mutual enemies, 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 speculative expectations that stands only thanks to preserving beliefs in potentialities, thus we call that corpus of newly emerged knowledge a *church of knowledge.*

Their usage in a *successive series* is strengthening relevancy of the emerging *church of knowledge* to the adoption of the current political agenda. A s*uccessive series* consequently legitimizes its adoption as unquestionably needed. Then, the series needs to be easily comprehensible to the audience, so they are put in the *successive order* that further evolves 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 we discuss particular moments, where new reasoning of newly adopted concepts within new fields of knowledge is taken for granted, the emergence of the *field of concomitance* evolves into new *statements* based on presumptive experiences of those who face the threats on a professional level. Then the *field of concomitance* transforms into the *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 to *fields of memory*; to 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, we are talking about the shift from *computer security*

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

[132] Foucault, *The Archeology of Knowledge*, 64.

[133] Ibid.

to *cyber security* covering very probably the same problem, but with new evolved meaning including national security concerns, a new *field of concomitance*. We 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*.[134] 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 behavior.[135] 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*.

## 5.2 Creation of field of truth and the logical slide

On the second layer, we elaborate on a 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 a new one. In the words of our case, how 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,* we 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 other statements that cannot be challenged as they have already established their position in new reasoning, new logic, new belief, and new undisputable concern. In particular, applying cyber security discourse to conventional waring. The whole discourse over cyber war depicts cyber war as something inevitable. It builds on assumption that conflicts have happened in past and will happen in the 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 policymakers 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 into our everyday lives and are uncontrollable by state authorities.

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*.

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 scenarios on their capabilities. Production of a technical knowledge under the curtain of such a cultural cloud produce a 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

[134] Ibid., 56–58.

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

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 the real technological consequences of particular technical vulnerability; it is a vulnerability in *cyber systems,* vulnerability that can be possibly exploited by hackers, which thus becomes cyber terrorism and thus a threat to national security. As we mentioned before, these two environments do not need to be in 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.[136] 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 for 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 policymakers point on these newly emerged experts as holders of the *relevant knowledge*. Nobody questions too much, as questioning is threatening the solid foundation of the 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.[137] However, it is based on their authority and 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 at 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 questions. Powerful policymakers 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 with Cox, there are two approaches, the "critical" that question the current policy and the "problem-solving" that needs smooth operations of institutions. [138]

## 5.3 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 *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;[139]

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

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

[138] Cox, "Social Forces, States and World Orders: Beyond International Relations Theory," 129.

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

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),[140] repeating these correlative statements within a group of involved people tighten relations between them and pointing out any outer critics as being deaf and blind without any self-criticism. In the end, cycles of these iterations help strengthen these tight relations and strong tight relations deepen beliefs of colleagues' expertise. Imaginations that were at the beginning a piece of a possible scenario on which the national 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 to the 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.[141] It is thought, that one event can bring us back to the *stone age*, thus it is not desirable to be prepared for that event, but it is broadly believed that we must act pre-emptively to cease the inevitable apocalypse. It is about social construction of the possible event in the future by correlating it with a well-known emotionally bound event in the past by discourse as there is no other evidence or source to this claim. SIT also provides interesting relation with Foucault's method while the process of strengthening ties can be strengthened with Foucault's concept of discipline.[142] 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 humans, *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 humans who *speak, create, construct, repeat and correlate*,[143] 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 a pupil, it is a policeman who is right with his argument against a jaywalker and there is no doubt that the higher authority can use the role, the position as a means of power.

## 5.4 Truths are growing from an underground to the surface of emergence

The fourth layer analyzes the *surface of emergence*, places before they are institutionalized or forum where the discourse takes place, where it gains its reasoning and credibility; where proper

[140] 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.

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

[142] Foucault, *Discipline & Punish: The Birth of the Prison*.

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

solutions are given to raised threats.[144] These surfaces might be different for different discourses. In our case, the 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 outcome of this document 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 policymakers to anchor particular interests rather than support public interest, we would be able to identify how these surfaces of emergence in discourse play a 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.

## 5.5 Materialization of power

The fifth layer identifies how *surfaces of emergence* form into *institutions*. How creation of places of visibility have been formed from discourse into the 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 policymakers constructed a new field of knowledge emanating from *technological radical uncertainty*. The use of the genealogical method 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 as to what it might do to urbanism. Who is right, cars or pedestrians? Do we really lower the number of causalities while significantly enlarging car usage? What is appropriate, a habit, that had been already established by discourse of those who blamed walkers by inappropriately 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 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 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

[144] Wickman and Kendall, *Using Foucault's Methods*, 26.

cooperation without establishing a global authority? The conference in Dubai in 2012[145] was exactly that attempt in establishing one super-authority over the Internet that failed. Paradoxically, the West with its liberal ideas would transfer powers to one body within the United Nations and drop current multi-stakeholder governance of the Internet, but the fear that such body would be exploited by authoritarian states that found their way forward how to control the Internet in their territory, led to support of the current multi-stakeholder model.[146]

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;[147] 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 on 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 existing actions, or on those which may arise in the present or in the future'; it is 'a set of actions upon other actions'."*[148]

## 5.6 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 out 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 needs to be said here that the analysis does not want to judge, it supposes to be critical per se or critical with a 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."[149]

---

[145] World Conference on International Telecommunications (WCIT) 2012.

[146] Deibert, "The Geopolitics of Cyberspace after Snowden."

[147] Michel Foucault and Duccio Trombadori, *Remarks on Marx: Conversations with Duccio Trombadori* (Semiotext(e), 1991), 112–113.

[148] Gilles Deleuze, *Foucault* (Paris: Editions de minuit, 1986).

[149] Michel Foucault, "The Masked Philosopher," in *Politics, Philosophy, Culture. Interviews and Other Writings 1977-1984*, ed. Lawrence D. Kritzman (New York: Routledge, 1988), 326.

When we are able to analytically grasp the process of how 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 history to seek for the processes that precede the current state of the policy in cyber security. It is very possible that the genealogical approach will find the subjects of discourse, those who 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, we see a great opportunity to take the same position as Foucault took. One may raise a question, where is the truth? How does this analysis contribute to a concern about whether we are standing in front of cyber war or not? The point is not to answer this question. The purpose of this analysis 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 and over the whole of 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 analysis 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 have been imagined, thus expected and then probably constructed based on our *technological radical uncertainty*.[150]

We have already been 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.[151] Genealogy is about the 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.[152] 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, the authority to alter it, evolve it in an intended direction without being criticized or suspicious of preserving the power.[153] Those 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 the 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 possessing corrective ion engines, be understood as a kinetic weapon thanks to its maneuverability. It is therefore called a dual-use technology.[154] A pure discursive attribute. There is a normative layer of using a knife, we all know that a knife is a weapon as well as an irreplaceable tool in a kitchen and it is up to the user who usually understand the consequences as to how the tool will be used. In the case of satellites and their maneuverability, which can be used to lower the orbital debris by deorbiting retired satellites or to

[150] Ibid., 95.

[151] Wickman and Kendall, *Using Foucault's Methods*, 24.

[152] Ibid., 29.

[153] Ibid., 47.

[154] 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.

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 to 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.[155] We all have knifes, but there is no carnage in the 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 potentialities is not a preparation on possible catastrophe, it is a legitimation of particular policy applications.*

Michel Foucault in one of his texts mentioned 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 a much more solid and traditional social status and its kind.[156] 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 materialized their *truth* in semantic delimitation of such truth to possible negative outcomes when no measures were taken.[157] 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 for 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 an 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."*[158] Including science fiction literature, in particular cyberpunk literature, is – to our opinion – an eyes-opening approach as the literature contains 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. 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."*[159]

## 6. Knowledge and the context of its formation

The whole idea of perceptions flow between discourses is based on the following table showing how cyberpunk subculture is constitutive of the possible imaginations but forgotten, while cyber-

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

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

[157] 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.

[158] 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.

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

crime is producing enormous amount of evidence to underscore the cyberpunk imaginations as possibilities and how cyber-war withing national security perspective uses the imaginations supported by the cyber crime evidence to develop threat politics on the national level, however, not on the evidence which suppose to be used for national security policy development. This is the core idea of our research, which is not necessary showing the *truth* but provides a critical insight into the policy making. This idea is not necessary explaining all the dynamics in cyberspace but has an ambition to provide a perspective how discourse materialize into power without proper evidence.

<table>
<tr><th></th><th>CYBER-PUNK</th><th>CYBER-CRIME</th><th>CYBER-WAR</th></tr>
<tr><td>Function</td><td>constitutive</td><td>evidentiary</td><td>imaginative</td></tr>
<tr><td>Founding policy</td><td>idealism</td><td>realism</td><td>threat politics</td></tr>
<tr><td>Effects</td><td>forgotten</td><td>exploding</td><td>overemphasized</td></tr>
<tr><td rowspan="3">Discursive influence</td><td colspan="2">>>> hacker becomes criminal >>></td><td></td></tr>
<tr><td></td><td colspan="2">>>> evidence transfer >>></td></tr>
<tr><td colspan="3">>>> hacker implies terrorist >>></td></tr>
<tr><td>Resulting role</td><td>hero</td><td>criminal</td><td>terrorist</td></tr>
</table>

Table 1 – Perceptions flow between the three discourse currents

## 6.1 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, we would agree. Bruno Latour came up with the idea in his masterpiece[160] to show how networks of knowledge are deepening the complexity of knowledge, so the purification process is becoming harder and harder. Let us introduce the idea, before we apply it to the whole work. Bruno Latour is talking about two distinct processes that are needed to develop a *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 has been out there since ages ago and what is culturally created is, for Bruno Latour, the key for a *modern critical stance.* Differing nature from human also reveals a discourse *"that is independent of both reference and society."*[161]

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, drives them to the inability to distinct what is science and what is culture. This has 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.

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

[160] Latour, *We Have Never Been Modern*.

[161] Latour, 10–11.

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 resonates in the discourse, by the creation of new *fields of truths* that emerged as *churches of knowledge* nobody dares to argue. The War on Terror after 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 let terrorists continue to 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.[162] Similar cultural processes can be distinguished within reaction on the development after the optimistic technological determinism despite the fact that they are thematically far from themselves. It was an argumentation on what role the technology can play in our lives and the subsequent debate of its societal impacts.

In that perspective, we argue that it is not the critically analyzed and unveiled intention, but the cultural cloud over technologies that drives the policy of cyber threats. Cyber is the problem, they said, not the intentions. Intentions are taken for 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 for 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. Policymakers should stop talking about undisputable cyber terrorist intentions in the near future, when no statistics of cyber terrorism is available, and start working on more mature technologies with the communities. The 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 policymakers and the technical one, where 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 terrorists will have a 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 of 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.[163] Technologies are still insecure and we have not observed one significant cyber terrorist attack and if there is a sophisticated cyber-attack against an 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.[164] This has not changed too much in recent history, cyber doom was a question since the invention of the 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;

[162] Hodges and Nilep, *Discourse, War and Terrorism*.

[163] Stohl, "Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?"

[164] Barnard-Wills and Ashenden, "Securing Virtual Space: Cyber War, Cyber Terror, and Risk."

however, how this is possible 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.[165] A genius example as weather forecast cannot be based on pure facts, which are then put into a calculation model that produces a 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 television news once had to provide insight into the future weather. The causal link is dependent on an enormous number of variables. Each increase needed computing capacities 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, a weather forecast must include a bit of *beliefs* about the weather and some general *knowledge* of weather development.[166] Weather forecasting started as a discipline based on beliefs of one's observation without 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 and looks like a fractal. Beliefs of experts become relevant, it is authority with a final word and will never be eradicated from the forecast process as we cannot reach absolute certainty. In fact, we have a threshold of preciseness that is needed for our personal planning; hence, absolute certainty is not needed and the subjective interpretation of incomplete data is a desirable solution. The cultural layer will never be unbounded.

The inability to detach the cultural bound from science is in Latour's early work understood in accordance to the impossibility to avoid the 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."*[167] 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.[168] The existence is not possible without non-modern existence, without culture; seeking for scientific truths has been performed, but never achieved[169] 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. The 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 that cannot not be understood as a critical perspective and that completely denies the processes of cyber policy formation. The critical

[165] Latour, *Science in Action: How to Follow Scientists and Engineers Through Society*, 181–82.

[166] Latour, 182.

[167] Latour, *We Have Never Been Modern*, 51.

[168] Latour, 86.

[169] Latour, 144.

perspective we proposed primarily shows how the particular cultural content plays a significant role in the cyber policy formation.

## 6.2 Technological radical uncertainty and its risk measurement

Baudrillard understands *radical uncertainty* in relation to media production, to the production of vast numbers 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*.[170] Deeping of this uncertainty looks very similar to the Latour's vertical axis between essence and existence, a post-modern existence, which enlightens another Baudrillard's argument with irreparability of this uncertainty by the *excess of available information*.[171] What kind of knowledge is deepened by repeated depicted threats of possible cyber doom? Only beliefs that are culturally binding us together in the victim of the others who cause the situation. The same process is well studied in critical studies of terrorism.

We have been working throughout this document with a concept we 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.[172] The idea of an objective should (but does not need to) precede the idea of a 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 the 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 particular technologies[173] and it is this discourse that shapes our reflecting of technology if its application missed its intended objectives.

However, how to make a decision over particular technological developments when democratic decisions can lead to technological paralysis and expert decisions to popular opposition?[174] Policymakers tend to overcome responsibility by changing the mind of the 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 the risk we take while adopting a particular policy. Nevertheless, will we be able to judge such policy of imaginative threats one day? One of the biggest troubles in taking a critical perspective on cyber security discourse is the absence of a judgement day. The day we had in the case of Y2K, so these who were intensively working on spreading panic worldwide could apologize as happened in Y2K case. The circle of repeating adopted truths imprinted to rationality of adopted policy creates conviction of acceptability of taken policy and mediates public concern related to the taken policy. Social construction of both, the scientific facts and the related policy emerge.[175] They exist in their own world of knowledge*. It is a combination of constructed analogies on national security levels based on empirical evidence in cyber crime and mystified by geeky culture with a 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

[170] Baudrillard and Poster, *Selected Writings*, 210.

[171] Baudrillard and Poster, 210.

[172] Latour and Woolgar, *Laboratory Life*.

[173] Wynne, "Risk and Environment as Legitimatory Discourses of Technology: Reflexivity inside-Out."

[174] Collins and Evans, "The Third Wave of Science Studies: Studies of Expertise and Experience."

[175] Irwin, "Constructing the Scientific Citizen: Science and Democracy in the Biosciences."

policymakers who produce the discourse. Experts' impressions are taken as knowledge, the same dynamics we discussed with weather forecasts, applies to the 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 have had since their beginning a special aura of being understood by special people only; geeks, 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 in a strictly different direction than expertise driven by curiosity, states cannot be a 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 in order to find a job in cyber-security institutions. Their expertise is devised much more from the loyalty to the nation state, especially in the 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,[176] 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 does 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.[177] The resonation of the Challenger and Columbia disasters is visible in currently adopted in the no-failure policy of NASA that burdens its technological development in order to achieve some meaningful results in human space flight.[178] 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 Latour's perfect modernity of socially detached facts about nature.[179] It is simply not possible to cover all the variables. The effectiveness of such an institution is based on resonation within the 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 for the positive impact to nature and thus the undisputable impact of human survivability. If authorities propose subsidies of better isolated windows leading to energy savings, they would be welcomed with a 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[180] of natural and social knowledge and perceiving 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 layers of reflection. The U.S. Department of Homeland Security approaches the security of critical infrastructures 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.[181] 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

[176] Love, "As a Hacker, I Know How Much Power Some Teenagers Have - We Need to Start Building Bridges with Them, and Fast."

[177] Collins and Pinch, *The Golem at Large: What You Should Know About Technology*.

[178] Zubrin, "The Case For Mars."

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

[180] Jasanoff.

[181] Based on an interview with Michele Markoff, deputy coordinator of cyber issues. July 2013.

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 corporate 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 a green light and the other a red light within huge corporations? Knowledge-making is thus an 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.[182] Nevertheless, the point is that consent between actors is productive, while conflict consumes time to explain why each actor prefers a particular position. And here we come to the point. The idea that the state is enforcing policies only to serve people would be naïve. It is the most common clash in democratic societies, the clash between liberty of the individual and security of the social. Whereas policy of individual liberty lowers the power of the state, policy of national security strengthens the power of the state. The policy approach by DHS strengthens both and reduces 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 seem 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.[183] Morale gives a hint here, but nothing more; however, morale could be understood also as expertise to protect things, species or human dignity[184] 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 not all about the problem of the 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.[185] When it comes to expertise required for immediate security concerns, experts might be under pressure to produce results that will go smoothly through the policy intended to be adopted as soon as possible.[186] 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 could expect more culturally influenced policy as the call for preventive action drew on doom consequences rises on its relevancy by adopting correlative analogies as facts. The desirable policy would be to draw these analogies as well-balanced to develop secure technologies, but to avoid filling the discursive space with only one possible threat.

## 6.3 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;[187] 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 resonance in the U.S. nation, using the name of the harbor in order to deepen attention on security threats from

[182] Jasanoff, *States of Knowledge: The Co-Production of Science and Social Order*, 3.

[183] Jasanoff, *The Fifth Branch: Science Advisers as Policymakers*.

[184] Fukuyama, *Our Post Human Future: Consequences of Biotechnology Revolution*.

[185] Abraham, *Science, Politics and the Pharmaceutical Industry: Controversy and Bias in Drug Regulation*.

[186] Nowotny, "Democratising Expertise and Socially Robust Knowledge."

[187] McDonald, "Securitization and the Construction of Security."

cyberspace adds a sign to whatever one says. No real threat, rather real fear based on a 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,[188] 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.*[189] Our perspective is that the *church of knowledge* produced by *cyber experts* in the field is a process narrowing this contingency. The *meaningful* claim in the field is then much more related to other comparable statements of cyber security discourse, which in the repeating circles produces unbeatable *dictums* of truth. *Meaningful* statements are not related to reality out there they are 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. We do not want to show that the discursive practices are the only explanation of cyber security politics production. We would rather answer the classical criticism of post-structuralist approaches[190] by adding the explanation of 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 the current national cyber security agenda is giving vindications to particular political moves. Explanations of these moves aside from what seems to be ordinary action by a nation state in order to deliver security is our research objective. Unveiling powers of discourse as implications to particular events might be criticized as a detour from an epistemological perspective, but this move was taken also to avoid criticism that the discourse analysis equals to *"relativism, nihilism, nominalism, solipsism or subjectivism"*[191] 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 we 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.

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 sues 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 and reactivation of unimportant historical events or emotionally 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.

## 6.4 Corpus of knowledge and the beginning of beliefs

For Michel Foucault, the perceptual field is a corpus of knowledge that presupposes the way of looking at things.[192] Before we can practice any skills in the same way, someone has to put all the

[188] Culler, *Ferdinand de Saussure*, 138.

[189] Epstein, *The Power of Words in International Relations: Birth of an Anti-Whaling Discourse*.

[190] Dumont, *The Promise of Poststructuralist Sociology: Marginalized Peoples and the Problem of Knowledge*.

[191] Dumont, 3.

[192] Foucault, *The Archeology of Knowledge*, 36.

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 forecasting, building a rocket, governing a state, all of these skills require 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. The 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.

We were 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 later, 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 at each cyber security conference around the world are shockingly, vigorously and ferociously explaining how extreme a threat this is while there are no burning cities around, what drives these people to believe the others? Fourth, along this panic there are still people who would like to answer questions with a bitter but sober tone[193] 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 we 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 the possibility to narrow it to a sober approach? Sixth, if there is still a driver despite statements such as the one from the 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?

## 7. 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 us to a development of the poniżej depicted figure of a perceptual field concerning cyber security as a national security agenda. Let us explain the whole logic. We will summarize the core of our argument in the following paragraphs.

[193] These feelings are coming from personal interviews with particular people. We 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 us 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.

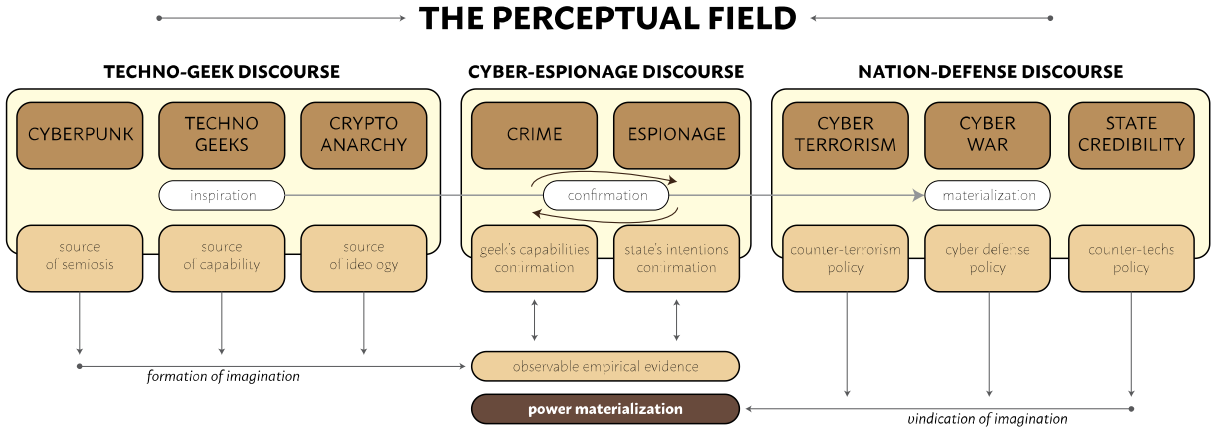



*Figure 1 - The Perceptual Field of Cyber Security as a National Security Agenda*

In that table, we showed the reason to choose three discourses, however, we 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 point is to put them into relation with each other and show the perspective of national cyber security discourse formation. We propose this perspective for your critical consideration.

## 7.1 Techno-Geek Discourse

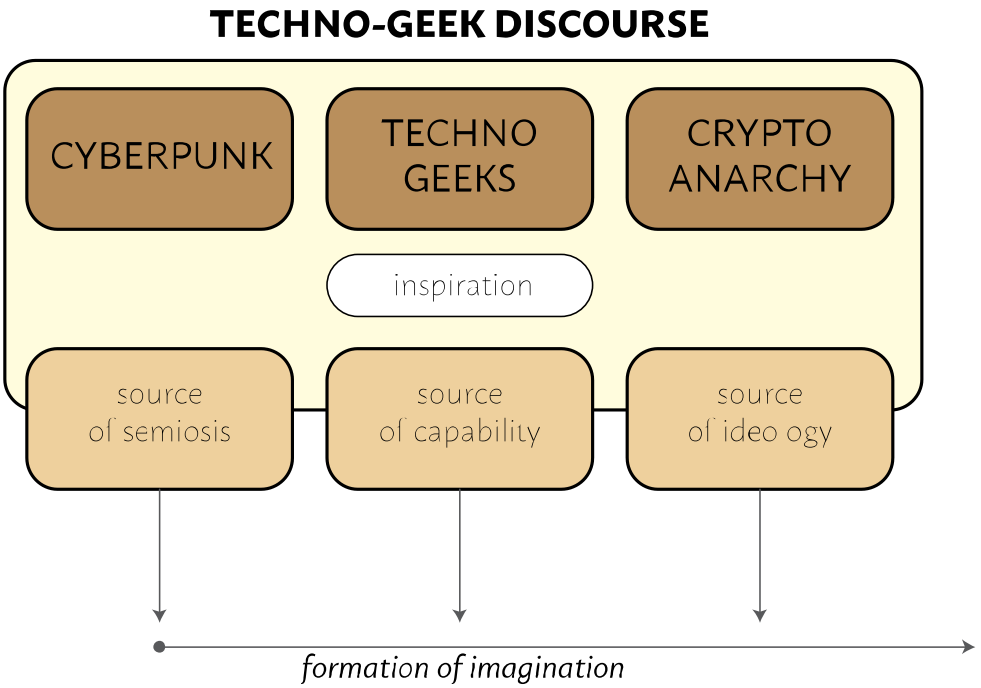



*Figure 2 - Techno-geek discourse structure*

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 the rising power of technologies as we discussed in the deliverable D3.1. 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, it is not too much complicated to find a list of such relation, the most visible would be the recently reopened case concerning addiction of US population on pain killers.

The relation between the individual and the corporate, the ability of the individual to stand against the powerful entity driven by neoliberal global capitalist ideas flattering our lives is very close to

Baudrillard's[194] simulations or Bauman's post-modern writings about a liquid society.[195] 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 *cyber security.* We proposed an answer. Cyber-punk, driven by curiosity of how to *steer* systems, is upgrading a mere computer security paradigm with a *man* and *intentions*. Who would talk about computer security without a man? Are computers our adversary? Fortunately, not yet, but as shown in the example of DARPA's artificial intelligence patching exploits autonomously online we may be adding one more actor very soon and that actor will again empower others by providing a new tool for continuous development. The addition of a man's intentions was needed to construct a rationale. A man, that possesses power – *the power of a man over a man*[196] is what stimulates insecurity feelings. However, what comes nest with artificial intelligence is beyond our imagination.

Geek, a man that is able to disentangle every system causing fascination and fear of his/her capabilities to others, is a real entity in our world that is driven by cyber-punk dystopian visions of a dark future he/she can avoid. Geeks exist, they are not in literature, they are a significant part of cyberspace development. Laughing to faces of mere earthlings by running global search engines of pirated data or of vulnerabilities of critical infrastructures. The demonstrations of capabilities of the search engine Shodan[197] are the moments when mere earthlings are hardly taking a breath. The capability of a man-geek is visible everywhere. The whole world of invisible viruses and malwares deployable without our awareness is feeding our imaginations regarding 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 our perception of their capabilities.

Finally, what drives the political agenda of geeks, the man rising from a dystopian world of cyber-punk, is the ideology behind the movement of those people. The ability to stand against the system is coming from the capabilities geeks possess and from the will the movement stimulates. 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[198] what the agenda is and it is clearly observable how the technology development of particular technologies within this epistemic community have been developed in accordance to it in the last two decades. We also briefly mentioned other ideologies such as ultra-libertarians, sometimes called anarcho-capitalists; however, we approached those as renegades from the crypto-anarchy movement, as those who decided to take the liberating technologies and make a 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 show much more how the liberating technologies can be so powerful and how they can liberate people from states when used massively. They also fulfill 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 we currently mentioned.

The techno-geek discourse is then encircling these three constitutive pillars. Whose perspective to take? Geeks or policymakers on behalf of governments? We 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 are driven by the ideology of crypto-anarchism (not all

[194] Baudrillard, *The Consumer Society: Myths and Structures*; Baudrillard and Poster, *Selected Writings*; Baudrillard, *Simulations*.

[195] Bauman and May, *Thinking Sociologically*; Bauman, *Liquid Modernity*.

[196] Arendt, "On Violence."

[197] Hill, "The Terrifying Search Engine That Finds Internet-Connected Cameras, Traffic Lights, Medical Devices, Baby Monitors And Power Plants."

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

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 policymakers, but also services such as AirBnB or Uber are showing how the ultra-libertarian agenda seeks a world without a super-authority, a nation state is not a complete fiction, but at least a fulfilling fiction that is proliferating 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 deepens 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 a 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 a global epistemic community;[199] 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 a 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, at 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[200]) 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 in the case of DHS. The conflictual policies will produce only a deeper conflict and will give power to rising resistance.

At the same time, classical work by Albert Laszlo Barabasi, Wired, showed that the ideal decentralization is not possible as all distributed networks, whether social, technical or galactic, tend to build centers. AirBNB begun as a principal representative of so-called shared economy, however, it shifted to the most ugly capitalist projection of global power ignoring legal regimes on national level. Lime, Uber and others followed the suit. Nation states was not even unable to contribute to the development of the technology, nor governed its development but is also almost incapable to regulate its usage, while the society is slowly changing, rents prices in historical centers multiplied, whole residential areas changed into tourist business sectors without local authorities having a clue how to influence the change. This may fade away but at least the last years showed how capitalist agenda of technological geeks can share with states. Libra cryptocurrency still awaits and the situation is simply only about whether Facebook is courageous enough to go into that legal fight or not but finally, all of this will depend mainly on the customers and whether they want to use the service. Here, our point is

[199] Adler and Haas, "Epistemic Communities, World Order, and the Creation of a Reflective Research Program."

[200] Rid, *Cyber War Will Not Take Place*, 2013, 26–32.

that such a power shift, such a degradation of power of an elected authority, might be more serious than all imaginations of possible cyber attack on a power plant.

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 these *weary giants of flesh and steel*[201], in fact by nation states,[202] which crypto-anarchists are so keenly willing to topple down. In that perspective provided by Morrison[203] their visions are utopic, but are as well visible throughout popular journalism or personal websites of respected geeks who behave in line of crypto-anarchism.

The political agenda behind the crypto-anarchists and crypto-capitalist is the substance that should be studied. The power of bigger elected entity, such as European Union, is critical in regulating the shift from crypto-anarchists through crypto-capitalist to global corporations and its materialization of power.

## 7.2 Crime-Espionage Discourse

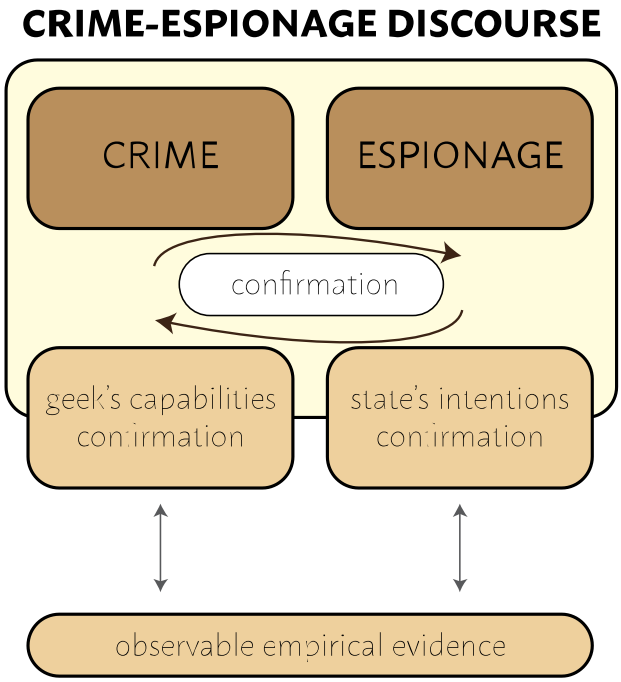



*Figure 3 - Crime-Espionage Discourse structure*

The measurement of cyber crime impacts is tricky as you could see in the empirical part. However, there is a consensus of rising events, e.g. in the 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 continuous grow. Cyber crime is a strong argument for those who think that states should possess more power in cyberspace and should be able to tackle 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 words enchanted by emotions – *lords of cyberspace* or switching the words giving the name a different and more dark connotation, like the move from the term *CryptoNet* to *Darknet.*

[201] Barlow, "A Declaration of the Independence of Cyberspace."

[202] Morrison, "An Impossible Future: John Perry Barlow's 'Declaration of the Independence of Cyberspace.'"

[203] Morrison.

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 policymakers. However, one of the most recent examples in Bangladesh, in which hackers were close to stealing almost a billion dollars, shows how these actions are taking place due to incapability of particular computer security administrators and thanks to specific knowledge of the attackers.[204] 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 produces evidence, which is evaluated in financial loses that vary from real amounts of money stolen to very debatable economical loses due to software piracy (projected profit loss), it provides policymakers a confirmation concerning the *real* capabilities of hackers. Regardless for specifics of particular attacks. The one from Bangladesh is not confirming a 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 the mountains down to the cities with mined gold; on the other hand, it raises 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 systems. Criminals are exploiting the state of unpreparedness on the side of banks due to lack of empirical evidences, which banks can use to secure them. It is expectable that banking systems will be significantly more secure in the near future. Nevertheless, state authorities see these criminals as rising empires that threaten our liberties.

Cyber crime produces evidence that can easily support the imagined knights or lords of cyberspace in their empires of dystopian cyberpunk lairs. A "*few clicks*"[205] are the only thing 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 the 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 understands the security of our computers better than the anti-virus companies? One may ask this question while reading advertisements all around the world wide web. They have also become anti-malware, Internet security, cyber defense or cyber security experts. The rising 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 multiplying proof of a newly emerging global crisis. Sometimes even interactive suggestive tools of live numbers about online theft, today stopped attacks or current ransoms 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 give the rationale to build more robust cyber defenses. However, one may raise a question why states are not inviting these companies to cyber defense operations when they are making contracts with these companies to secure systems running critical infrastructures? 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 of why states do not tend to defend critical systems using these companies, but settle contracts with companies experienced in national defense

[204] Finkle, "Bangladesh Bank Hackers Compromised SWIFT Software, Warning Issued."

[205] The~Economist, "Hacking the Banks."

(BAE)[206] 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, we discussed that some cyber espionage attempts or successful operations do not need to be treated as nation driven espionage. We 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. States thus understand attacks 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 raises the perception of these attacks to 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 proving state driven espionage is simply impugnable. The repeated attacks on critical systems, the fact that geeks operate search engines 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 policymakers that states will be able, and are currently willing, to steal all of 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 establishing new national security institutions that are clearly a materialization of power in the hands of a nation state. The fact that states are not able to deal with certain rising cyber crime threats to citizens (ransomware as an example) is leaving state security administrations in a position of need to socially construct or discursively bend the criminal reality into the perspective of rising threats to a nation state in the shape of 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 the international surveillance monster, which does not follow interests we would expect from a liberal democratic nation state.[207]

At this same time, the liberal West was caught in the middle of the shockingly massive surveillance operation PRISM, which disputes the principle of social contract in the eyes of citizens supporting a liberal democratic political system. Results of such revelations would be nothing more 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,[208] the more important results is a *lower credibility* of a liberal democratic nation state as a principal authority at the international level finally empowering decentralized networks and corporations. 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, the Panama Papers and similar unveiling of nation states corruption of elites or even nation states intentional behavior violating principles of liberal democracies are certainly part of this decadence.

---

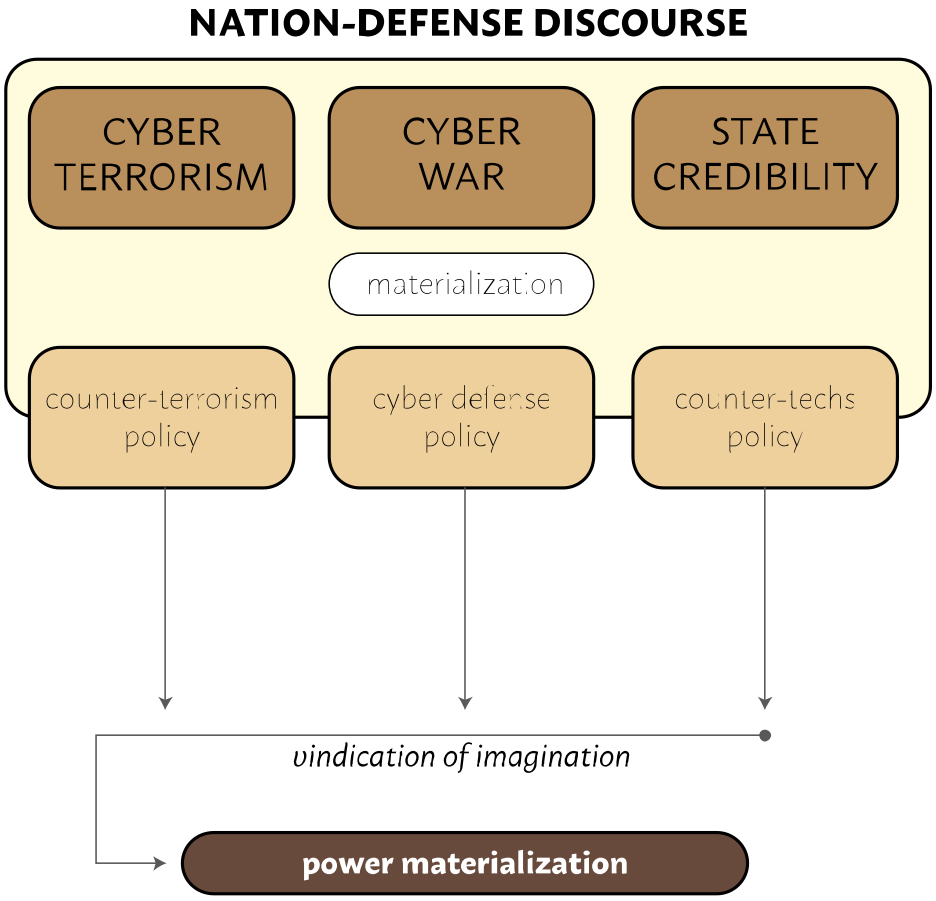
[206] "BAE Homepage."

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

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

However, crime has to become espionage to raise the argument of a needed new power in the 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 a world without governments would be more secure and these are certainly coming from places such as Silicon Valley, where all the giants of cyberspace, giants that found a way 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 produces a 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 the geek community. This process shows lowering confidence in 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 that citizens allegedly cannot deal with and *national cyber defense* is the key in their eyes but they are wrong.

## 7.3 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 hampered 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 the Vannevar Bush recommendation after 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 the Cyber Grand Challenge in Las Vegas, just days before the DEF CON,[209] 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 a 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 we do not perceive a development of possible hostile artificial intelligence as a harmonization of policies, especially when such systems can be completely decentralized and will need to gather information globally to create distinction between 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 the cyberpunk movie *the 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 at patching the autonomous system. As the physical force is not meaningful in cyberspace, the division between a cyber-attack to gather information in espionage operations and a cyber-attack to alter the machine in order to patch it or physically destroy it is blurring. The attack vector is the same, intentions 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 policymakers 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[210] without ordering them on a scale of seriousness, while adding another, clearly the most unpredictable actor of artificial intelligence. Terrorists are 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. That changes also the perspective on the desirable expertise. It seems that the expertise which is driven by policy is more respectful, because it is the expected policy produced by a groupthink. Hearing more alarming discourse is what listeners expect, hearing less alarming would lower the attractiveness and thus confidence of speaker's integrity as a respected expert, but also loyal to the epistemic community of experts in the policy of cyber security. The one who dares to raise important questions, such as Elon Musk who is constantly warning against artificial

209

210 Nicholson et al., "SCADA Security in the Light of Cyber-Warfare."

intelligence in the service of national security, are expelled from the democratic debate. The clear effect of the 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-ranking officials, authorities, usually these (very limited amounts of critical speeches) we used in the 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 the NSA, the CIA and the FBI in 2014.[211] 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 questions on Stuxnet were answered as an 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.[212] The influential 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 all at once. One may raise a legitimate question, whether thinking over terrorism in the White House just a 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 *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 the 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 raises enough doubts of a nation state's capabilities 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 learned, but we see international exercises in cyber defense on imaginative scenarios. These scenarios are drawing imaginative futures on the 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 the imaginative world. Organizing exercises based on a particular experience, on for example the Ukrainian blackout, would probably be too easy as the most problematic part in Ukraine despite its better defense that some critical infrastructures have in the United States[213] were absent 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 on how to develop policy of preparedness that would react to catastrophes in the normalized manner as Aradau and Munster recommend.[214]

The *church of knowledge* developed at policy conferences and practiced through exercises are qualifying supra-national authorities in asking a question of whether a particular policy has been

[211] International Conference on Cyber Security (ICCS) – http://www.iccs2016.iaasse.org/

[212] Pouillot, "'Sobjectivism': Toward a Constructivist Methodology."

[213] SANS ICS, *Analysis of the Cyber Attack on the Ukrainian Power Grid*.

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

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 understood as more *modern*. However, it is also a question aiming on a greater policy of internationally integrated networks of state authorities in 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 the 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 states can do little to such extremely quick developments of malicious technology. It is about secure technology that can be developed and finally security education, at least of operators, that tends to put a written password on sticky papers visible on their monitors. The Ukrainian attack was possible due only to a row of such human errors. National defense would do little to stop it. However, that fact does not fit to the discursively constructed perceptual field of policy experts in national cyber security drawing cyber doom in order to strengthen nation state authorities and who wish to govern technology developments related to cyberspace;[215] it is becoming a norm to have strong cyber defenses and a violation of global undisputable norms facilitates an exceptional response – a resistance.

## 8. Power, authority and governance

The final point we have been planning to elaborate on 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 on how to perceive a problem. Even its first protagonist talks 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."*[216] However, we follow several rules of ANT we 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[217] and that is the approach We are taking in the following text.

The concept of *assemblage* was introduced to the social theory by Deleuze and Guattari with a bit of a 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.[218] It can be understood as expansion by technology, because Deleuze and Guattari later contended that technology makes mistakes by being treated in isolation: *"The stirrup entails a new man-horse symbiosis that at the same time entails new weapons and new instruments."*[219]The relation plays a role in ANT as well as assemblage, the whole assemblage is a network of relations; no actor is influenced by others 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*.[220]

---

[215] Brito and Watkins, "Paper Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy."

[216] Latour, "On Recalling ANT," 15.

[217] Law, "Actor Network Theory and Material Semiotics."

[218] Deleuze and Guattari, *A Thousand Plateaus*, 52:90.

[219] Deleuze and Guattari, 52:90.

[220] Stevens, *Cyber Security and the Politics of Time*, 181.

However, our perspective is to approach assemblage as antagonistic networks that can exist thanks to that negative relation (state and crypto-anarchists). Hence, the assemblage applies to 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 constitutes the higher one: *"the properties of the component parts can never explain the relations which constitute a whole."*[221] Let's call these lower level assemblages *socio-technical dimensions* of the cyber security assemblage.

First, we were drawing on motivations of hackers and their ideology. We did so as we 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 one has the will to adopt it. Intentions matter, intentions cause *effects.* If there are uniform effects caused by the heterogeneous actors, it can be studied as a network of actors.[222] Actors that are both human and non-human and interlinked in a global networked assemblage,[223] but distinct from the other *socio-technical dimension* by having a 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 a dystopian future. The comparable tensions in inner consciousness that are well related to Kafka's writing of *The Castle*[224] or *The Trial*[225] on which Deleuze and Guattari build their perspective.[226] Kafka's writings, despite their lack of being pure cyber-punk or science fiction, are 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 a blind following of rules in the administration could be 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 a central authority, but within a *network assemblage* with unexpected contingent effects practicing *actualized power*[227] that certainly fuels the *technical radical uncertainty,* of those who are dependent and materialize the *immanent power*. [228]

Second, some hackers are celebrated as heroes (Snowden, Assange) who produce the *fantasy of masterful.*[229] That inspiration, as the Pasteur in the *pasteurization of France,*[230] 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

[221] DeLanda, *A New Philosophy of Society: Assemblage Theory and Social Complexity*, 40:10.

[222] Mol, "Actor-Network Theory: Sensitive Terms and Enduring Tensions."

[223] Abrahamsen and Williams, "Security Beyond the State: Global Security Assemblages in International Politics."

[224] Kafka, *The Castle*.

[225] Kafka, *The Trial*.

[226] Deleuze and Guattari, *A Thousand Plateaus*.

[227] Deleuze and Guattari.

[228] Deleuze and Guattari.

[229] Mol, "Actor-Network Theory: Sensitive Terms and Enduring Tensions."

[230] Latour, *Pasteurization of France*.

altering each other with critical implications to social dynamics of global society. The speed of social change that has 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 like a 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 the 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's credibility and ability to govern[231] 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 as 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 a 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, language plays a crucial role in the cooperation as the adoption of a 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. The crypto-anarchist movement provides enough content for that imagination. The result is clearly *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 option,[232] because they live in a shared inter-institutional and international consciousness sharing knowledge, opinion and beliefs.[233] They might easily become the scientific advisers to policymakers[234] as they are exactly the experts, whose expertise is accepted without a 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 of how the discourse within a particular assemblage produces 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 to be expected when one calls for ultimate security from any possible cyber terrorist attempt. However, that development, in addition understood as legitimate, is what Baudrillard calls 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 called a policy against doom scenarios.

The same as seen above can thus be applied to 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 produces a material existence and a *sense*. A sense that *cyber terrorism* is a plausible future and thus we have to strengthen ties of nation state power to secure national security. In this permanent state of

---

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

[232] 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.

[233] Barnard-Wills and Ashenden, "Securing Virtual Space: Cyber War, Cyber Terror, and Risk."

[234] Jasanoff, *The Fifth Branch: Science Advisers as Policymakers*.

exception of terrorist threats discursively constructed,[235] we are drawing only the most improbable events with heavy impacts.[236] Two totally distinct worlds can exist because they are in this *tension,*[237] tension that creates a relationship between two; tension producing *agencies* on both sides.[238] The relational tension and the fact of synchronized productivity of new behaviors, expressions, realities as well as territorial organizations is what produces 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 as a space that is not merely a 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[239] 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[240] 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 businesses have been capable of doing using NASA money in the last decade is a very common argument of the liberals proposing lower power for states in technology development. However, it was a state that decided and funded the Apollo program that produced so many spin offs to 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.[241] Business has proved an ability to invent technologies that states were not, but that usually do not need to cover security issues in a national security perspective despite the fact it might have covered their business interests and related security. The governance indeterminacy might be a problem in a centralist government, but might not in a decentralized government, which supports participation if one has the will to participate. The distinction between the development of open-source Linux and the proprietary development of Microsoft Windows has shown that the decentralized governance of software development can meet even higher security measures than centralized. 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 a decentralized open-source community.

Before the government can pursue its objectives, it needs 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 a 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 in anti-centralist presumptions, which are written in their constitutive writings.[242] On the other hand, states are living in their permanent state of exception, in which security is not given and the 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

---

[235] Ditrych, "A Genealogy of Terrorism in States' Discourse."

[236] Cavelty, "Cyber-Terror--Looming Threat or Phantom Menace? Th."

[237] Mol, "Actor-Network Theory: Sensitive Terms and Enduring Tensions."

[238] Müller, "Assemblages and Actor-Networks: Rethinking Socio-Material Power, Politics and Space."

[239] Bush, *Science - The Endless Frontier*.

[240] Wynne, "Risk and Environment as Legitimatory Discourses of Technology: Reflexivity inside-Out."

[241] Barry, *Political Machines: Governing a Technological Society*, 201.

[242] Barlow, "A Declaration of the Independence of Cyberspace."

by social contract. If nation states are working on cyber defenses due to the well of successful materializations 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*.[243] If we follow the experience with open-source and proprietary software, we might devise that it would be a 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,[244] 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 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,[245] 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 the application of the same norms on all communication networks in order to secure *cyberspace*, an undisputable norm. As we pointed out already in the chapter about *Construction of security crises under technological radical uncertainty* the co-production process introduced by Sheila Jasanoff[246] 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 developments of the 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 the 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 the 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 drives 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. We would understand it as a suicide of the nation state governance model.

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 responsibilities,[247] 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. However, there are only two options of further development, a super-authority that was already proposed at the ITU Dubai Conference in 2012[248] 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 tends to extremely securitize cyberspace to strengthen its power – to use

[243] Mitchell, "Society, Economy, and the State Effect."

[244] Deleuze and Guattari, *A Thousand Plateaus*.

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

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

[247] Lessig, *Code and Other Laws of Cyberspace*.

[248] ITU, "Forging the Future."

cyberspace to its advantage,[249] but which resonates within citizens as an authoritarian rule.[250] 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 with the difference between *politics* and *the political*.[251] 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 a particular political agenda is established through artifacts, activities or practices that become objects of contestation[252] - 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."*[253] Foucault revealed the fundamental fluidity of power that *"passes through individuals. It is not applied to them."*[254] It is an individual who practices power based on beliefs within the social structure s/he well knows 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 World War Two. Power is not about what it is, but about what it does[255] that implies a creation of *regime of practice*,[256] which we observe in the building of international projects 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 fulfill an absurd utopia of global surveillance megastructures not far from Foucault's *panopticon* to preserve ultimate security from terrorists, 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[257] 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."*[258] Both developments are strictly antagonistic, but fulfilling itself at the same time. No *oligopticon* would be possible in people's minds, it would never materialize into usable technology that is changing the world so quickly, if we did not observe the construction of *panopticon* in the massive global surveillance hydra. It would not be present in their intentions, in the *causes and effects of* the network assemblage of crypto-anarchists producing the liberating technology out of and against the will of centralized power in sovereign states. Nevertheless, they will continue this practice, if the tendency to create more powerful states beating imaginative cyber terrorists, preparing for imaginative cyber war, but burning its credibility by stealing the privacy of citizens to secure global cyberspace persists. In the light of the Snowden revelations, it seems like an exercise of authoritarian

[249] US-DoD, "Department Of Defense Strategy For Operating In Cyberspace."

[250] Barlow, "A Declaration of the Independence of Cyberspace."

[251] Barry, *Political Machines: Governing a Technological Society*, 201.

[252] Barry, 6.

[253] Deleuze, *Foucault*.

[254] Foucault, *Society Must Be Defended: Lectures at the Colle`ge de France 1975–1976*, 29.

[255] Foucault, *Society Must Be Defended: Lectures at the Colle`ge de France 1975–1976*.

[256] Foucault, "Questions of Method," 75.

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

[258] Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory*, 181.

rule despite its liberal democratic foundations[259] and 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 a 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 we perceive as very dangerous to open minded liberal global democratic societies, but at the same time the will along with the inability to reach the utopia of panopticon by a nation state may lead to 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.[260]

# 9. References

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. https://doi.org/10.1111/j.1749-5687.2008.00060.x.

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

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, 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.

"BAE Homepage," 2016. http://www.baesystems.com/en/cybersecurity/feature/it-s-not-just-security---it-s-defence-.

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. https://doi.org/10.1177/1206331211430016.

Barry, Andrew. *Political Machines: Governing a Technological Society*. London: Athlone Press, 2001.

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. https://doi.org/10.2307/3089803.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B J

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

[260] Wendt, "Why a World State Is Inevitable."

Walker. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8, no. 2 (2014): 121–44. https://doi.org/10.1111/ips.12048.

Bauman, Zygmunt, and T May. *Thinking Sociologically*. Blackwell Publishers, 2001.

Beck, Ulrich. "Risk Society: Towards a New Modernity." London: SAGE, 1992.

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

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. https://doi.org/10.1080/09557571.2011.558054.

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.

Bush, Vannevar. *Science - The Endless Frontier*. Washington D.C.: National Science Foundation, 1945.

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.

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. https://doi.org/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.

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.

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. https://doi.org/10.1177/0306312702032002003.

Collins, Harry, and Trevor Pinch. *The Golem at Large: What You Should Know About Technology*. Cambridge University Press, 2002.

Cox, Robert W. "Social Forces, States and World Orders: Beyond International Relations Theory." *Millennium: Journal of International Studies* 10, no. 2 (June 23, 1981): 126–55. https://doi.org/10.1177/03058298810100020501.

Culler, Johnathan D. *Ferdinand de Saussure*. Cornell Paperbacks : Linguistics, Literary Criticism. Cornell University Press, 1986.

Deibert, R. J. "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace." *Millennium - Journal of International Studies* 32, no. 3 (2003): 501–30. https://doi.org/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. https://doi.org/10.1353/jod.2010.0010.

DeLanda, Manuel. *A New Philosophy of Society: Assemblage Theory and Social Complexity*. *Continuum*. Vol. 40, 2006. https://doi.org/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.

Ditrych, Ondřej. "A Genealogy of Terrorism in States' Discourse." Charles University, 2011.

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. https://doi.org/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. https://doi.org/10.1504/IJCIS.2005.006122.

Durkheim, Emile. *The Rules of Sociological Method*. New York: Free Press, 1950.

Endeshaw, Assafa. "Internet Regulation in China: The Never-ending Cat and Mouse Game1." *Information & Communications Technology Law* 13, no. 1 (2004): 41–57. https://doi.org/10.1080/1360083042000190634.

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.

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.

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

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, Michel. "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. https://doi.org/10.1177/053901847000900108.

Fukuyama, Francis. *Our Post Human Future: Consequences of Biotechnology Revolution*. New York: Farrar, Straus and Giroux, 2002.

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.

Giddens, Anthony. *The Constitution of Society*. Polity Press, 1984.

Gieryn, Thomas F. *Cultural Boundaries of Science: Credibility on the Line*. Chicago: University of Chicago

Press, 1999.

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

Hacking, Ian. *THE SOCIAL CONSTRUCTION OF WHAT ?* Cambridge, Massachusetts and London, England: Harvard University Press, 1999.

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. https://doi.org/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.

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.

Irwin, Alan. "Constructing the Scientific Citizen: Science and Democracy in the Biosciences." *Public Understanding of Science* 10, no. 1 (2001): 1–18. https://doi.org/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. https://doi.org/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.

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. https://doi.org/10.1177/03063127030333004.

———. *Designs on Nature: Science and Democracy in Europe and the United States*. New Jersey: Princeton University Press, 2005. https://doi.org/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. https://doi.org/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.

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.

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

https://doi.org/10.1177/0162243910385787.

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.

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.

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. https://doi.org/10.1177/0967010610393775.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

Lewis, Aidan. "Jaywalking: How the Car Industry Outlawed Crossing the Road." *BBC*, February 12, 2014. http://www.bbc.com/news/magazine-26073797.

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/.

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.

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.

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.

McDonald, Matt. "Securitization and the Construction of Security." *European Journal of International Relations* 14, no. 4 (2008): 563–87. https://doi.org/10.1177/1354066108097553.

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

https://doi.org/10.1177/016224390002500202.

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. https://doi.org/10.1177/1745691612459060.

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. https://doi.org/10.1177/1461444808100161.

Müller, Martin. "Assemblages and Actor-Networks: Rethinking Socio-Material Power, Politics and Space." *Geography Compass* 1, no. September (January 2014): 1–20. https://doi.org/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.

Netanel, Neil Weinstock. "Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory." *California Law Review* 88, no. 2 (2000): 397. https://doi.org/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. https://doi.org/10.1016/j.cose.2012.02.009.

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

———. "Where Computer Security Meets National Security." *Ethics and Information Technology* 7, no. 2 (2005): 61–73. https://doi.org/10.1007/s10676-005-4582-3.

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

Pouillot, Vincent. "'Sobjectivism': Toward a Constructivist Methodology." *International Studies Quarterly* 51, no. 2 (2007): 359–84.

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.

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.

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.

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. https://doi.org/10.1177/0306312703033001038.

Russell, Bertrand. *Mysticism and Logic: And Other Essays*. Longmans, Green and Company, 1919.

Ryan, J. *A History of the Internet and the Digital Future*. London: Reaktion Books, 2010.

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.

———. "Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War." *Defense and Strategy* 14, no. 2 (2014): 73–86. https://doi.org/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.

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. https://doi.org/10.1126/science.6986654.

Sismondo, Serge. *An Introduction to Science and Technology Studies*. Wiley-Blackwell, 2010.

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

Stevens, Tim. "Apocalyptic Visions : Cyber War and the Politics of Time." *Available at SSRN*, 2013, 1–28. https://doi.org/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. https://doi.org/10.1007/s10611-007-9061-9.

Stone, John. "Cyber War Will Take Place!" *Journal of Strategic Studies* 36, no. 1 (November 10, 2013): 101–8. https://doi.org/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.

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.

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

US-DoD. "Department Of Defense Strategy For Operating In Cyberspace," 2011. http://www.defense.gov/news/d20110714cyber.pdf.

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

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.

Wendt, Alexander. "Anarchy Is What States Make of It: The Social Construction of Power Politics." *International Organization* 46, no. 02 (March 1992): 391. https://doi.org/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 (December 21, 2003): 491–542. https://doi.org/10.1177/135406610394001.

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

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

Wynne, B. "Risk and Environment as Legitimatory Discourses of Technology: Reflexivity inside-Out." *Current Sociology* 50, no. 3 (2002): 459–77. https://doi.org/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. https://doi.org/10.1177/03063127030333005.

Zubrin, Robert. "The Case For Mars," 2012. https://doi.org/10.1016/0019-1035(85)90164-2.

# 10. Annex

## 10.1 Implications to national security, a technical perspective

### 10.1.1 Development of specific technologies

The 'Digital Revolution' continues to transform global communication through technological advances in computing, microprocessors, digital phone and the Internet. It is compared to the agricultural and industrial revolutions in terms of impact, and as the origin of a new Information Age. Claude Shannon's acclaimed article '*A Mathematical Theory of Communication'* in 1948 is credited as the influencer for the transformation from analogue to digital formats that followed in the next decades[261]. The ensuing rapid development of digitalised technologies, and incremental growth in the use of computers since the invention of the World Wide Web by Tim Berners-Lee in 1989, has led to an Internet penetration rate of 58.8% of the world's population[262] [263]. The latest statistics on mobile phone usage shows around 4 billion unique users and digital population continues to increase year-on-year [264]. There are few signs that an appetite for the latest digital gadget has diminished with forecasts predicting that these trends will continue for the foreseeable future. In just a few decades, a connected world has empowered citizens and transformed capabilities across multiple sectors by turning data into knowledge, saving lives, improving economic growth and education, and stimulating social change.

At the same time, however, the rapid infiltration of technological advances deep into the fabric of society has brought many challenges. Along with digital development has been the ingress of digital crime. In some cases, traditional crimes simply transverse to the digital world but, simultaneously, the development of new technologies provide new exploitable opportunities, as evidenced in the evolution of cybercrime. Inherent system vulnerabilities, and an economic environment where demand for the latest gadget is prioritised over security issues, have facilitated a new ecosystem of criminal activity. Tech savvie criminals exploit, to their own advantage, the slow progress of security improvements and the shortcomings in cyber resilience training and education which leaves much of the populace exposed to the latest threats.

Whilst the depth and intensity of the benefits deriving from this revolution are widely acknowledged, it is correspondingly understood that the pace of technical innovation has left many unprepared and ill-informed on its potential effects and possible implications. Currently, this is reflected in concerns about the means to constrain AI technology if its capabilities outpace those of humans[265].

A disparity between societal shifts and understanding often exists, leading to distorted perceptions, an increase in fear and worries, and opportunities for the nefarious to take advantage of

---

[261] A Mathematical Theory of Communication, Shannon, Claude E.; Weaver, Warren (1963). The mathematical theory of communication (4. print. ed.). Urbana: University of Illinois Press. p. 144. ISBN 0252725484.

[262] https://en.wikipedia.org/wiki/Digital_Revolution,

[263] https://www.internetworldstats.com/stats.htm

[264] https://www.statista.com/statistics/617136/digital-population-worldwide/

[265] https://www.pewinternet.org/2018/12/10/artificial-intelligence-and-the-future-of-humans/

the situation. Empirical research has a part to play in bridging these gaps through presentation of the facts, in order to dispel misconceptions, to further education in essential topics and to empower users with the confidence to be pro-active about security.

### 10.1.2 Massive use of certain technologies

The fundamental technological component behind the rapid accent of the Digital Revolution is the development of the metal-oxide- semiconductor field-effect transistor (MOSFET, or MOS transistor)[266] MOS microprocessors and memory chips have facilitated the transition of computing into mobile devices through the simultaneously development of computer networking, the Internet, digital broadcasting and online services. However, the Internet is the predominant vector in the transformation of global communications[267]. According to Internet World Stats as at 30 June 2019 there are 4.5bn (58.8% of total population) users of the Internet[268].

Integral to the rapid progress of the Internet is the development of robotic software applications, so-called "bots". The running of tasks or scripts is performed automatically and more quickly than by humans. Bots have transformed network computing processes by facilitating the growth from the performance of simple, basic tasks into powerful search engines that crawl the Internet and direct traffic to requested information. Bots are ubiquitous to the Internet as we know it today and enable many of its primary and beneficial functions including speed of website access. Although estimates vary year-on year, approximately half of all Internet traffic is considered to be from bots[269]. Table ?? illustrates some common types of bots and their uses.

Table 1 Examples of Bot Uses

| Bot | Type | Function | Examples |
|---|---|---|---|
| Search engine | Web crawlers or spiders | Browse web pages and index content, generate feedback for informed ranking of websites based on placement of significant words | Googlebot, Bingbot, Yandex bot, etc |
| Copyright | Web crawlers | Searches for duplicated text, music, images, videos that may violate copyright laws | YouTube, Sony, etc. |
| Site monitoring | Web scraping crawlers | Collects content, adding to a database, extracting relevant bits of information for analysis e.g., price and product comparison, weather monitoring, vulnerability monitoring | 200Please Bot, Artmixx, CMS Crawler, etc |
| Text-reading | Text-reading algorithm | Elaborate algorithms browse text and analyse according to specific keywords and frequency, filter comments in social media or online news outlets, flag and exclude specific types of comments (e.g. offensive or spam). | Google Translate, trading bots |

[266] https://en.wikipedia.org/wiki/Digital_Revolution#cite_note-auto-34.

[267] http://aasa.ut.ee/augsburg/literature/CASTELLS_BBVA-OpenMind-book-Change-19-key-essays-on-how-internet-is-changing-our-lives-Technology-Internet-Innovation.pdf

[268] https://internetworldstats.com/stats.htm

[269] https://www.techsparq.com/blog/2018/10/29/the-evolution-of-bots

| | | | |
|---|---|---|---|
| Feed | Web crawlers | Search for newsworthy content to add to another website | Aggregator sites, social media networks, googlefeedfetcher, Yahoo Pipes |
| i) Chatbots (simple) (ii)Conversational AI (Advanced) | Text or auditory algorithm | i) Simulates a human to conduct a conversation such as virtual assistant software. ii) Interaction that passes the Turing assessment test of AI capabilities. | Apple Siri, Google Alexa, DoNotPay |
| Video game | AI algorithm | Takes the place of a human player | State Machine algorithm, Monte Carlo Search Tree (MCTS) (online chess, Go), Massively multiplayer online role-playing games (MMORPGs) |

Bots, and especially botnets, a network of connected computers, have acquired a negative connotation. Having gained such a reputation is disappointing as bots, and botnets, are the backbone of Internet functionality. Undeniably, however, the metrics on bot traffic show that this impression is difficult to contradict. Year-on-year reports vary but it is clear that 'bad' bots constitute around a quarter of all Internet traffic, which is about one half of all bot traffic[270]. Bots, legitimate or otherwise, provide access to a revenue model and the means with which to earn good financial returns.

Botnets, when used as collaborative tools, provide partners with combined resources to carry out research on large scale. This type of collaboration is popular among volunteer computing projects. An example is the Berkeley Open Infrastructure for Network Computing (BOINC) which operates as a platform for "*...high-throughput computing on a large scale (thousands or millions of computers*)"[271]. Some of the well-known users of BOINC include; climateprediction.net (Oxford University)[272]; LHC@Home (Large Hadron Collider - CERN (European Organization for Nuclear Research); and the World Community Grid, to further non-profit research on some of the world's most pressing problems – (IBM Corporate Citizenship) [273]. The BOINC platform is the model of a use case that the early computing pioneers would have envisaged for their innovation in networked computers – a connected world used for the good of world problems.

Good botnet ventures such as BOINC are, sadly, not the ones that make for eye-catching headline stories. It is an unfortunate reality that 'bad' botnets have added to the list of world problems through the havoc caused by the nefarious intent of their operators. Additionally, an aura of anxiety and fear has been spawned around the terminology. Although 'bad' bots and botnets do not outstrip their good counterparts in terms of traffic, they appear to eclipse them in terms of notoriety, leading to a generalised misconception that all bots are malicious. This trend, and its associated fear, continues into future innovations, notably AI technology, as highlighted in 10.1.1 Development of specific technologies above. The assumption appears to be that the extensive use of new AI technology is risky due to the potential unpredictability of its capabilities. However, AI technology is a growth sector and it is unlikely that anxieties over its use will curtail further research or its integration into the most fundamental of everyday activities.

[270] https://resources.distilnetworks.com/white-paper-reports/bad-bot-report-2019

[271] https://boinc.berkeley.edu/index.php

[272] https://www.cpdn.org/

[273] https://www.worldcommunitygrid.org/discover.action

### 10.1.3 Abuse of the technologies

Bad bots are designed to automatically perform malicious tasks and to remotely take control of other computers as a botnet, known as zombies, to execute malicious acts on a large-scale. Millions of bots sent from single, or multiple IPs, can strangle bandwidth for negative impact, such as Denial of Service (DoS) attacks. Abuses of this type are now commonplace as evidenced in reports that show the number of bad bots incidents year-on-year. For example, in 2014 Bad bots were measured as 22.8% of all traffic, good bots as 36.^% and human traffic as 40.9%[274]. In 2018 these were measured as 20.4%, 17.5% and 62.1% , respectively. As the authors state, there was a slight decrease in bad bot traffic in 2018 compared to 2018 but bad bots still represent one fifth of all internet traffic. The bots were measured according to the following level of sophistication:

- Level 1 (Simple) - Connects from a single, ISP-assigned IP address, not browser-based,
- Level 2 (Moderate) – Simulates browsers, can execute Javascript,
- Level 3 (sophisticated) – Simulate human behavior, evade detection, connects to sites using malware installed in browsers,
- Advanced Persistent Bots (APBs) - Combine moderate and sophisticated techniques to evade detection and reduce traffic noise, enter through anonymous proxies and peer-to-peer networks, can change user agents, persistent (low and slow).

APBs are stealthy and may remain undetected for long periods of time. In 2018 they were attributed to being 73.6% of all 2018 bad bot traffic according to Distil Networks '*Bad Bot Report 2019: The Bot Arms Race Continues'.*

As automated technology advances, criminal bot creators utilise state-of-the-art methods to thwart the latest security mechanisms. Such sophisticated developments significantly raise the bar against successful mitigation of automated threats. In a defensive response, The Open Web Application Security Project (OWASP) lists the different bad bot types in its Automated Threat Handbook[275]. The list provides an ontology that describes real-world automated threats to web applications in a common language for developers, architects, operators, business owners, security engineers, purchasers and suppliers/ vendors. The aim is to facilitate clear communication and help tackle the issues around the abuse of automated functionalities.

### 10.1.4 Escalation of activities

As technology advances, malicious actors adopt new sophisticated techniques. For example, IoT Botnets are now behind the latest, and most powerful of DDoS attacks. An IoT botnet is able to control IoT devices, such as cameras, routers, DVRs, wearables and other embedded technologies. An IoT botnet is capable of persistently targeting more and more devices, making it more powerful than earlier botnets. They may comprise of hundreds of thousands of compromised devices, for very little cost to the attacker compared to gaining access to, and control of, servers.

The first major report of the destructive power of an IoT botnet came in October 2016 with the launch of the Mirai Botnet. Mirai was first launched in 2016, hitting a well-known security journalist's blog site followed by an attack against Dyn, a major DNS provider. This attack generated 1.2 terabits of malicious traffic which forced Dyn off the Internet for hours. Since then, there have been numerous other attacks from Mirai but new variants are continuously being developed as it is evolved to take advantage of new market trends[276]. Mirai variants have been found with zero-day exploits to attack consumer-level devices and malware payloads to attack cryptocurrency miners. According to IBM X-Force, Mirai and its variants was the most popular malware in the first few months of 2019[277]. It was

[274] https://resources.distilnetworks.com/white-paper-reports/bad-bot-report-2019

[275] https://www.owasp.org/images/3/33/Automated-threat-handbook.pdf

[276] https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/

[277] https://exchange.xforce.ibmcloud.com/collection/Mirai-and-Mirai-Like-Botnet-Activity-e144024b6b831d5481f2657bc9978f86

seen twice as many times as its nearest rival, Gafgyt. IBM X-Force researchers predict that IoT bonnets will be increasingly pervasive as the popularity of IoT devices continues.