SIMARGL

D3.1 Nexus of cyberspace actors

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: 30/08/2019
Document Submission Date: 29/08/2019

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:	**D3.1**
Deliverable title:	Nexus of cyberspace actors
Deliverable version:	V1.5
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:	31/08/2019
Actual date of delivery:	30/08/2019
Dissemination level:	P
Editor(s):	Nikola Schmidt (IIR), Martin Švec (IIR)
Contributor(s):	IIR, ITTI
Reviewer(s):	Michal Choras (FUH)
Ethical advisor(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	7/7/2019	IIR	First draft of the ToC
1.1	9/8/2019	IIR	Rewritten ToC, added some actors and cyberspace definition
1.2	22/8/2019	IIR	Almost all actors described
1.31	27/8/2019	IIR	Added international law perspective in a working version and some other actors
1.4	28/8/2019	IIR	Finalized actors, added introduction and conclusion
1.5	29/8/2019	IIR	Added finalized international law

Table of Contents

1. Executive summary

The document focuses mainly on various selected actors and discusses what scholars, businesses and government think about the actors' motivation. The provided nexus of actors in the attached table should serve as an orientation point for the reader how the actors relate to each other, what motivates them and what are their objectives in general. We took approach that should fulfil some requirements of the actors nexus completeness. However, at the same time we believe that a mere summarization of the actors and general introduction to the debate would be unsatisfactory as it would not bring anything new to a reader oriented in cyber security. Neither we wanted to cover everything, nor we decided to select the most important. We rather decided to take a novel approach and show how the link between culture, imagination, technological uncertainty and security practices merge into a perception of cyber space that can be both alarmist and critical. These two perceptions usually cannot be in the same document, however, we put them together to show the visible difference between them.

The former, alarmist, perception can be identified within a group of policy makers that tend to identify any opportunity to make progress in policy making with intention not to miss any single possibility of insecurities that should be covered by policy. However, such keen approach usually makes them blind from the consequences of exceptional politics they propose to implement. The latter, critical, approach do exactly the opposite, it deconstructs the discourse of the alarmists and provides an insight into the hidden intentions of these alarmists. One can argue that the absence of a single cyber terrorist attack does not satisfy the need for security from cyber terrorists, however, at the same time we should ask a question what the proportionate reaction on something is we do not have experience with. This dilemma is a very common one in cyber security as measurement of power in cyber space is almost impossible, which is understandably the reason why alarmist discourse is thriving.

Such dilemma also influences how cyber space is perceived from the international law perspective. Therefore, Chapter 5 seeks to explore the multifaced international law challenges faced by various actors in cyberspace.

2. Introduction

2.1 Motivation

The goal of this document is to provide a picture of the current debate over security in cyber space within the international relations and security studies disciplines. The objective was not to completely cover the debate from every corner but rather select opposing views on how technology influence security in cyber space.

2.2 Intended audience

We wrote this report for anybody willing to have a overall picture of the discussion in cyber security. However, our principal intention has been to somehow intervene into the alarmist discourse that can be perceived within the community of policy makers. We wanted to enlarge the picture of how the perception of insecurities form and how the discussion over actors can be tricky especially when some policies or international law interpretations are adopted.

2.3 Relation to other deliverables

The document, though quite long, provides the reader novel perceptions on actors and some dynamics but does not discuss power relations or origin of the discourse. This is planned for the following one, coded D3.2.

2.4 Structure of the deliverable

We begin with a cyber space conceptualization and follow with discussion on each selected actor. Then we summarize actor's assumed objectives. The final part discussed the current international law interpretation related to cyber security.

3. Cyberspace – definitions, perspective, fluidity and imaginations

"Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding..."

— William Gibson, Neuromancer (1984) —

Cyberspace – if you open a discussion with policy makers, usually each will be able to come with a different definition. Some will define cyberspace as a network of hardware utilities interconnected by cables, some will focus on the social platforms in which the social interaction take place, some will put emphasis on critical infrastructures linked through internet links, some will even include everything where data are transmitted both ways or broadcasted one way. There is no consensus what cyberspace is. There are consensuses between states on various platforms such as OSCE, in which states decided to define cyberspace before proceeding with creating confidence building measure. However, in order to properly understand what humanity has created here in last decades, one should take more unexpected way. The approach we are taking here is to study culture that surrounded the pioneering days of the digital communication and what that unimaginable space of future possibilities did to the imagination of possibilities between policy makers.

The first definitions from national security strategies tended to understand cyberspace merely in a technical way, as interconnected devices that communicate. The cyberspace as socially constructed environment was almost or completely omitted. It took decades before national strategist included the component of social interaction and still the definitions seem to avoid addressing the hard-to-grasp social environment. However, we might witness a change in the forthcoming years due to the propaganda activity by Russia, which is using social networks and other services where the interaction of people take place to put through its foreign policy interests by weaponization of information, [1] its cognition while avoiding any attacks on physical devices (in this particular strategy).

We would like to firstly deconstruct the above shown quotation, in which the first ever use of the term cyberspace appeared.[2] *Neuromancer* as has been perceived as a masterpiece in cyberpunk literature that created the first pictures of digital future. Many other thinkers referred to Gibson because that time, and for years later, nobody else dared to change the vision Gibson sketched. The newness in the term in relation to ongoing cyberpunk subculture expressions was the addition of its interconnectedness. The emergence of the Internet in the 60s evolved as a national defense project,[3] but its real social consequences became very quickly self-evident; especially in the 80s when the internet was already very actively used in academia. The possibility that everybody and everything

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

[2] Neuromancer is usually mentioned as the first literature piece showing a word cyberspace. In fact, Gibson coined the term earlier in his very short science fiction Burning Chrome published in the July issue of magazine Omni, which he read for an audience of four people including Bruce Sperling in 1981. Later it was nominated for a Nebula Award in 1983. Gibson, "Burning Chrome."

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

can be connected in one interconnected world was certainly utopian, but now an achievable vision; however, with a different consequences that we expected.

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

Gibson created a new battlefield on an information basis. He shows how we can attack back using counter-information, and he showed us a new man who can stand up having the faculty to distinguish between information and noise; to be oriented in a black market of cyberspace (observe the link with a current term *the Darknet*). On the other hand, the protagonist in the story is artificial intelligence that shows the hard-to-distinct reality and humanity from unreal and artificial life form. All of these infinities are covered by multinational corporations that hangs as an umbrella over totalized uncontrollable infinite oceans of information. This infinite complexity also contains a vast amount of enemies that seek for Deleuzen and Guatarris *reterritorialization*[4] of the real within the vast labyrinth of *virtuality, hyperreality* or *integral reality*.

In contrast, national security strategies or more precisely national cyber security strategies tend to provide us only with simple definitions that have been developed by analysts who wanted to point out a growing security problem in cyberspace – those who created the alarmist discourse in national security agenda in cyberspace. First of all, they tend to omit the distinction between technical infrastructure and the abstract social construct above it. They usually vary around different physical/technical perspectives or we can say they tend to compete who chooses the better and more important devices connected to an ultimate global network to show the policymakers that even they depend on things related to the Internet.

Let us show some of these oversimplifying definitions: "The interdependent network of information technology infrastructures, and includes the Internet, telecommunication networks, computer systems, and embedded processors and controllers in critical industries."[5] Another one starts with the term nervous system that has links to the above drawn dystopian world, but the whole document does not work with that perspective very brightly: "Nervous system – the control system of the country (…) composed of hundreds of thousands of interconnected computers, servers, routers, switches and fiber optic cables that allow our critical infrastructure to work."[6] Using the term nervous does not have any other reason in the mentioned strategy other than to depict how complex it is. However, one may argue that here we come with the first seed of imagination as using the term nervous might have other reasons, maybe a system, on which we all depend and cannot live without? It increases seriousness of the network security by choosing this particular term, while the term itself says nothing to its functioning. Definition that constitute emotions rather than being providing some

[4] Deleuze and Guattari, *Anti-Edipus. Capitalism and Schizophrenia*.

[5] White House, "National Presidential Directive 54."

[6] TheWhiteHouse, "The National Strategy to Secure Cyberspace."

explanatory outcome. Other definitions add a layer of information: "Digital environment enabling the origin, processing and exchange of information, made up of information systems and the services and networks of electronic communication."[7]

However, it took some time since these definitions have included its change *by the use of it*. The following is, thanks to the research of the author that lies behind it, probably the best available definition for policymakers:

"A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."[8]

Right now, we have three layers, the technical infrastructure that is interconnected through networks, the information stored somewhere within and the *fluid character* caused *by the use of it*, but we still do not have the abstract layer. The Encyclopædia Britannica defines the term *cyberspace* thoroughly, but in the second sentence it mentions the distinction between internet and cyberspace; respectively the distinction between the infrastructure and the generation of the *place* produced by the interconnected network that is consisting of information[9] can be understood as our active creation and reflection of that place, an abstract place as it does not have physical proportions. The distinction between outer-space and cyber-space can be made on distinction between exploration and construction,[10] respectively *exploration of the real* and *construction of the virtual*. Cyberspace in cyberpunk subculture, but also later during the dawn of computer games and chatrooms was understood as a *virtual place* where interactions between people occurred. Without these interactions no cyberspace would exist.

Today, we can add also machines as the internet is full of information collected by automated systems (systems that do not merely distribute, but generate information), e.g. publicly available satellite imagery; maybe traffic information would be a better example as we make immediate decisions based on such information distributed using automated systems. Google traffic collects anonymous data from cell phones, excluding anomalies such as frequent stops of postal or any other delivery vans and produces colors on a map.[11] These colors representing levels of traffic jams are used to calculate the shorter path. The driver then follows the car GPS navigation system. This is just a small example in which our pragmatic reflection of data automatically generated through cyberspace directly influences our decisions. However, artificial intelligence marches into our lives as Google introduces its ChatBot. It will soon help us solve technical problems with our computers by answering, even clarifying, questions in language quality and insight that people might not even register they are talking to a bot.[12]

Martin Libicki in his book from 2007[13] divided cyberspace into four layers, and he added the pragmatic one:

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

---

[7] Jirásek, Novák, and Požár, *Cyber Security Glossary*.

[8] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem."

[9] Bussel, "Cyberspace."

[10] Choucri, *Cyberpolitics in International Relations*, 51.

[11] NCTA, "How Google Tracks Traffic."

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

[13] Libicki, *Conquest in Cyberspace: National Security and Info*, 236–37.

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

Right now, we can add the postmodern perspective to the whole conceptualization. Postmodernism as a theoretical approach and as a culture emanates also from the *uncertainty of technology innovation* and its societal implications. The technology on the one hand tries to not only help us to understand the dynamics, but to answer the uncertainty during a constitutive process. I mean a process in which the technology plays both roles, of the agent and of the structure. Giddens, as a postmodern sociologist, introduced this idea in which the agent and the structure are mutually constitutive,[14] where practices translate into habits during a performative dance between the both.

Schmidt used this idea to explain the sociological constitutive notion in cyberspace conceptualization,[15] in which he tried to put the principal theoretical basis of cyberspace existence back to the postmodern perspective; to the age in which the logic of internal cyberspace dynamics emerged as Gibson's hallucination of millions of operators connected to the network. Without the connection and consequent shaping by ideas, cyberspace would not be possible. The nature of its security is not limited to working routers and servers. It is mainly dependent on how we reflect its implications to our lives. The principal argument Schmidt wanted to point out was a power switch we can witness in cyberspace. Every single national defense strategy in cyberspace tends to translate conventional power to cyber power pointing on accessibility of every system in critical infrastructure[16] while omitting the very fact of its postmodern inaccessibility as cyberspace changes fluidly. Services, software settings, hardware configurations, all them evolve on a daily basis, but also as the technology evolve, people's habits change in space and time. What we are witnessing today is a real performation of a cyberpunk imagination, in which the high-tech environment and cyberpunk culture are both mapping and illuminating the imagined reality.[17]

Gibson's *hallucinations*, Britannica's cyberspace *production* on the links of internet generating abstract virtual world, Kuehl's perspective of its shaping *by its use of it* and Schmidt's *sociological approach* to cyberspace conceptualization using Giddens theory are all constitutive stepping stones to cyberspace conceptualization; to better understand the space we all have been creating and will constantly change in near or far future. Cyberspace helps to produce new realities and these realities certainly empower new people who like to exploit their opportunity based on their knowledge; and these motives are not taken seriously.

However, if we have to take into consideration all the characteristics of cyberspace for purposes of national security strategies, almost all the definitions I cited above seriously lack a lot of later discussed specifics which are critical for any meaningful approaches by policymakers. One has to admit that even without doing the etymological research of the term *cyberspace*, we read news about threats that include the cognitive layer every single day. The Russian propaganda for example, which is currently a very tangible topic and might have serious consequences in the long term[18] despite some allegations that the bigger problems are produced by "useful idiots" rather than by the direct propaganda itself.[19] However, the sociological approach is valuable even in hard security policy as it shows that attacks on hard targets such as power plants are not currently part of the adversaries.

---

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

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

[16] Kramer, "Cyberpower Natl. Secur."

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

[18] Samadashvili, "Muzzling the Bear Muzzling the Bear. Strategic Defence for Russia's Undeclared Information War on Europe."

[19] Snegovaya, "Putin's Information Warfare in Ukraine."

When it comes to state hostilities, the influence of Russia in European politics and even to the presidential campaign in the USA has become a norm. When it comes to the resistance, the ability of states to govern technology development the way they want to see their desirable politics is far from possible. In the end, we have strong political players on the global scale in the USA and Russia who try to destabilize their political systems and then decentralized communities that tend to isolate themselves from political turmoil in geeks, crypto-anarchists or libertarians taking their opportunity and at the same time rising unnumbered amount of artificial intelligence self-learning system. The reality looks like a dystopian post-modern chaos where nobody knows who is on what side or whether there are sides to take.

Talking about security in the sense of connectivity between devices would be really shortsighted. The following list introduces some of the most important characteristics related to the current shaping of cyberspace and how each characteristic contributes to the post-modern chaos:[20]

- *Temporality* – if one is interested in an attack of an enemy, there is no traditional discussion on how much it will take since the launch of the operation. Everything is going on in real time. The preparation phase is critically important, while the operation itself might be extremely short. Even just a moment. Time disappeared.
- *Physicality* – physical accessibility loses its sense when it comes to politics of cyberspace. The constraints of physical distance, the geography itself and the situation of the infrastructure changes significantly. The ability to influence political processes in other countries directly, changes the strategy every day from far distances, use a cyber-attack against power grid, all of this is completely different since the cyberspace have been developed. When the first air forces were deployed, the strategy significantly changed, because air could go over the front lines, attack supplies and return safely back. Cyberspace changed this completely, we do not need to be physically present to cause serious harm and even completely destabilize other countries.
- *Permeation* – the fact that people do not behave according to habits in their "real" social life, that actors, including states, do not obey rules and laws. This characteristic is important in understanding how any kind of regime cannot be applied to people in their operation of technologies connected to the Internet.[21] As it is completely (almost) unable to enforce a regime in cyberspace, it is also completely unable to govern the technology that deepens the complexity of the technologies. Developing norms of behavior, rules of the road for new actors in space that change so quickly becomes an unachievable objective. That of course seriously harm even the notion of moral behavior and the polarity between good and evil implications caused by the technology usage, development and exploitation.
- *Fluidity* – the very post-modern characteristic. The one that depicts the constant change of the environment, services, habits and routines.[22] Not only the technical infrastructure, but also available services and the long chain of consequences are directly or indirectly connected to the real physical domain of our lives. There are real businesses that experienced their failure due to emergence of even illegal services online. The debate over intellectual property would be a clear example. [23]
- *Participation* – as will be discussed in the rest of this chapter, cyberspace seriously changed the way in how people can participate in public life. Activism, with – of course – its supposedly negative connotation as a *hacktivism*, fuels power of non-

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

[21] Hughes, "A Treaty for Cyberspace."

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

[23] Koepsell, *The Ontology of Cyberspace: Philosophy, Law, and the Future of Intellectual Property*.

governmental institutions and any other non-state actors and gives an unprecedented possibility to people to show united opinion quickly and also massively. This characteristic seriously shook with whole states during the Arab Spring.[24] However, participation characteristics are important in any kind of non-physical organization. People are not only able to topple down regimes, they are also easily achievable by those who might have interest in toppling down the regime as we can see in current Russian behavior in socially constructing unreal *signs* in the audience in Europe and elsewhere.[25]

- *Attribution* – one of the most important characteristics in interstate relations. The fact that the origin of an attack is hard to attribute to a particular actor, and the fact that the actor is not willing to change it as the state can easily exploit it to its advantage, creates antagonistic moment Schmidt called *dual-interest of states*.[26] On the one hand, they tend to discuss how to divide privacy and anonymity to beat current ultimate anonymity and keep people private online. On the other hand, it is in their very interest to be hidden behind the attribution problem to conduct operations in cyberspace and circumvent international law; especially in operations that by the definition do not violate international law, but seriously undermine national security.[27]
- *Accountability* – the characteristic related to the attribution problem. When the attribution is problematic, the accountability is impossible. Some scholars propose more structured responsibility to states if they fail to avoid cyber-attacks emanating from their territory,[28] but the dual-interest keep these ideas grounded.

The debate could go deeper but let us start developing the point of this section here. The definitions we saw above, which were related to the national administration of the USA, must have had influence on policy making. Researchers in critical studies already pointed out the enormous effect of security framing of the so-called critical infrastructure threats were based on pure imagination.[29] Some of the texts we are providing later reflect this securitized alarmist discourse to provide the perspective how such discourse looks like. These definitions share the uncertainty of the communication technology and as such tend to create future possibilities based on apocalyptic visions. The fact that military has to defend their networks to be operable, the fact that one must be able to make a call over laid wires, the fact that physical network architecture matters in cyber security raises attention to the physical layer. All the definitions and perceptions visible in first national cyber security strategies share this simplification. For example, the Dutch national cyber security strategy does not talk about cyberspace, but about *digital domain* to make it more chaotic, however, the definition still contains that simplification approach: "*The digital domain is the conglomerate of ICT tools and services and comprises all entities that can be or are digitally linked. The domain comprises both permanent, temporary or local connections, as well as information, such as data and programme codes, located in this domain where geographical limitations do not apply.*"[30]

The nervous network, the digital domain, the global and dynamic domain, the warring domain, the electromagnetic spectrum, the realm of electronic communication, the notional environment and so

[24] Perthes, "Europe and the Arab Spring."

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

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

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

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

[29] Cavelty, *Cyber-Security and Threat Politics: US Efforts To*; Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse."

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

on. One may ask why the need of cyberpunk debate when all of this is about cyber security as a national security agenda. The answer is clear:

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

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

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

Fourth, hackers depicted as *"password pirates and electronic burglars"* who possess *"a certain techno-scientific power"*[31] are a nightmare for policymakers, because in fact they possess power nobody understand. On one hand, their adversaries (so be it anybody) adore their capabilities and use them as a powerful tool when enabling cyberspace for national security interests during some special operations such as Stuxnet.[32] On the other hand, they simply cannot withstand the fact of their incapability to face them despite the fact that the incapability emanates from the complexity rather than from lack of knowledge as the complete understanding is unachievable. Hence the defensive countermeasure is the drawing of dystopian doom scenarios[33] in the real world producing securitization terms such as critical infrastructure. A different approach would be to propose techno-geeks a job in state administration.[34] However, that move – in the contrary to their will – confute them of that incapability to understand the cyberspace possibilities. That in circle again empowers the techno-geek community. An interesting example would be the discourse behind the rise of bitcoin. The crypto currency, or digital currency, has its own important general advantages especially in the technology of block chain on which it builds, but also underline the achievability of the crypto-anarchist objectives as will be discussed later. The discourse of people supporting and promoting usage of block chain technology is usually oriented to mock politicians even in situations, when they are willing to recognize it as a genius invention.[35] The resistance understands the will to support it as false and as another cheating of governments on the rising liberty of people enabled by bitcoin.

Fifth, we should understand this moment in motion rather than as a solid moment in space time. Cyberpunk is not a future prediction for policymakers, it is an inspiration for techno-geeks. It empowers their motivations and action. In *Neuromancer*, operators are making money by selling information, which is the currency in that world. Those who steal from banks nowadays, have a computer, capability and information, and nothing else. This power gives them a radical vision of an ultimate liberal world without nation states and for nation states the future is so unpredictable that drawing doom scenarios seem to be the rational way.

The proper way forward to understand where we stand would be somewhere between the imaginations in cyberpunk subculture and a sober perspective that nothing serious has happened yet, thus no doom scenarios will ever fulfil. This technological uncertainty as a dynamic that is so specific to cyberspace given the extreme pace of technology evolution, that alarmist discourse might be necessary in order to keep all possibilities on the table, however, without critical assessment of the

---

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

[32] Nicolas Falliere and Chien, "W32.Stuxnet Dossier."

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

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

[35] Castillo, "European Parliament Member: Everyone Should 'Get Some Bitcoins.'"

alarmist approach we might reach a dystopian political future because every uncertainty tend to socially construct possible futures that will later enable exceptional politics that has nothing to do with liberal democracy.

4. The nexus of actors

Actors	Principal adversary	Objectives		Methods		Implications to international security
		Primary	Secondary	Primary	Secondary	
Geeks	no-one, alters the system	empowerment through cyberspace	deepen the technological complexity	specific knowledge	specific technologies	development of specific technologies
Activists	state system		ultimate liberation of the society		social structures	massive use of certain technologies
Criminals	law enforcement agencies		revenue		transnational criminal networks	abuse of the technologies
States (international perspective)	national counter intelligence	national security	industrial and state espionage	hidden behind attribution problem	massive penetration of networks & buying information on a black market	escalation of activities
Intelligence	foreign countries		proactive prevention	gathering intelligence	active probe of information flow	lowering confidence in liberal state
Law Enforcement	cyber criminals		proactive punishment	prosecute criminals	forensic analysis of past	lowering obsolete crime & deepening complexity of future crime
States (national perspective)	terrorists/geeks, crypto-anarchists, foreign countries, intelligence		national defense	securitization of international terrorism	construction of institutions, empowerment	more powerful state, less confident citizens
Corporations	ALL	revenue	good relations with states, for now	securitization of critical infrastructure	technology standardization	decay of democratic systems
Citizens	ALL oppressing and disturbing	democracy	independence on state control	using tools making life better	adopting crypto-anarchist tools	lower confidence in liberal democracy
Cyber terrorist	ALL	Chaos	Disbelief in liberal regimes	Unknown, no cyber terrorist act has happened yet	Actor as a tool for securitization of cyberspace by states	Empowering states and lowering privacy

Artificial Intelligence	- ? -	achieving goals	semi-autonomous self-alteration	environment alteration	technology self-evolution	uncontrollable AI "crime" and "espionage"

Table 1 - The nexus of cyber space actors

Empowerment through cyberspace	Powerless people in their common lives may tend to use technology to gain power. Geeks, cyber activists, all who use technology in order to gain more power, to leverage power of those who in their perspective are oppressing them, to give power to the oppressed.
National security	States are those who are responsible for national security. However, the question is what is the ideal state of national security? Is it a security from other states intrusion, is it a conform society willing to subordinate themselves to the state, is it a state where no criminals are exploiting cyber space to gain revenue? We work with national security mainly as a state, in which the state as an actor tend to fulfil its role in social contract with citizens. However, is national security more than a global security providing global citizens an environment to flourish? These are conflicting views that different states may adopt. Even democratic states may tend to be more protectionist, authoritative and focus on hard security from the soft security. Such a difference is used as a principal differing element in general academic analysis of what is considered to be security.
Revenue	Profit. This objective is nothing more than a mere capitalist objective to make a profit.
Democracy	As Robert Dahl puts it, democracy is not an ideal state, it is unachievable ideal we should pursue all the time in order to live in a free society. Democracy is the principal source of legitimacy for the actor possessing power. We use democracy here as an argument against activities that lower privacy and freedom of citizens in the name of national security (nobody understands). The political ideal, which is the key for those who want to live and flourish.
Achieving goals	Mechanical principles of an artificial intelligence looking for fulfilling humans' will. However, AI is not about solving problems only but about deep learning providing a completely different picture. The goal can be

	so complex that human mind might not be able to even recognize it. Achieving goal can be an ideal state of its operation, while the important part can remain hidden.

Table 2 - Actors' primary objectives

4.1 Geeks or techno-geeks

Baudrillard's simulation represents the uncertainty in technology development; the uncertainty producing realities out of the *presumable real*, in which those who provides knowledge suggest to oscillate between promoting study of changes and providing stability;[36] in the quagmire of post-modern instability, contingency and fluidity. We can observe the distinction between that *presumable real* and the *individual real*, the construction of the subcultural world, which is detached from the outside world and untouchable by people untouched by technology or without a clue as to how the newly generating techno-social environment works. These "outside" people that care about the *presumable real* are making decisions over a social environment they can barely control. It is a courageous claim; however, never ending argument, simplified into an expression that all the *"threats emanating from cyberspace"*[37] are a problem, proves the inability to distinguish appropriately where the power comes from and how these threats significantly vary in their internal potential to disrupt societies or destroy critical infrastructure. Cyberspace is a social construction and the plethora of threats it can bring up is as wide as all the threats we can even imagine in a physical space.

How people who see only the physical cable from power plants can secure the cyberspace from geeks as non-state actors or geeks employed by other states remain clearly questionable. The problem of socially constructed cyberspace is not a geeky construct. Evidence finds a nice example of the relation to a serious national security agenda; such as Operation Orchard which was conducted by Israel by flying into Syrian airspace with the result being a bombing of a purported nuclear reactor.[38] This is just one example of so-called cyber war; however, the point is that Israel altered data on the way to monitors in order to change the visual representation of reality. The operators in Syria then could not make a decision as they did not see anything suspicious. The one who has this ability possesses an enormous power as the alteration is hardly recognizable, at least not by the operator who is responsible for the right and prompt decision.

The ability changes as the environment changes, who controls the environment, obtains specific ability related to that respective environment and as there is no single biggest authority or ultimate actor in cyberspace, because each single operator socially constructs it, these operators will have power only over those parts over which construction they are part of. When we were talking about "a target in a constant motion" causing ontological insecurity without an ability to create a sociological frame of current fluid society,[39] this clearly applies to cyberspace as a socially constructed environment that changes in the same unpredictable way as the wind. Additionally, there is no more or no less power, there is only a critical knowledge related to particular implications that materialize in momentous power. One may possess more detailed knowledge implying more power, but this power will still be a very specific one.

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

[37] Inkster, "China in Cyberspace"; Melzer, "Cyberwarfare and International Law"; Czosseck and Geers, *The Virtual Battlefield: Perspectives on Cyber War*; Cavelty, Mauer, and Krishna-Hensel, *Power and Security in the Information Age: Investi*; Schmidt, "Critical Comments on Current Research Agenda in Cyber Security"; TheWhiteHouse, "International Strategy for Cyberspace"; Geers, *Strategic Cyber Security*; Melnitzky, "DEFENDING AMERICA AGAINST CHINESE CYBER ESPIONAGE."

[38] Tabansky and Ben Israel, "Striking with Bits? The IDF and Cyber-Warfare."

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

Geek, the one who possesses power that the others cannot even imagine, not necessarily in its scale, but in its technological specificity. That immeasurability of skills is what constitutes the technological radical uncertainty, where plausible knowns and normalized reactions are unreachable as skills of geeks are immeasurable. The definition from an urban dictionary perfectly catches the meaning of a geek: *'someone with ridiculous skills on a computer or other electronical device and scares us mere earthlings. They have a habit of breaking these after stretching them beyond their ability for normal usage. They also sometimes know more about a product than the producer.'*[40] The actual application of the definition into a contextual meaning is described in the cited dictionary as follows: '*so I just took out the hard drive, cleaned the terminals and de-floobied the remainder of the computer so I could download this software which enabled me to detonate a bomb on the other side of the world which is specifically programmed to kill everyone except me.'* One may argue that the meaning is overemphasized, it is of course, but the core meaning of ungraspable or unimaginable knowledge to do such things is what drives national security imaginations to a point, in which they talk about an infinite fog of threats emanating from cyberspace. The clash between a geek having specific knowledge and a five-star general having a nuclear button, but no power to stop a geek, is the core of the fear that drives national cyber security imaginations into the doom scenarios.

Geeks have no advarsaries. The enabling capability of technology, in geeks motivations, is clearly to enable the human capacity and make them less dependent on political system.

4.2 Cyber activists

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather . . . "

John P. Barlow, "A Declaration of the Independence of Cyberspace" [41]

The Declaration by Barlow clearly shows what imaginations of possible people's liberation cyberspace – as a new space for social interactions – enabled through the novel technology. However, this is even a clear depiction of will by various activist groups that cannot remain without reaction of nation states. Cyber activists, online activists or activists simply using technology to reach their objectives are different from geeks because they use the technology to enable their ideology. This category thus describes more or less overlapping actors that have one denominator – the ideology that technology can enable.

Cyber activists are more or less *positive technology determinists* – they are convinced that technology can bring them good. However, while geeks think in general that the decentralization of technology development will make people less dependent on higher authorities namely nation states, crypto anarchists have their ideological ends and focus on particular technologies such as Bitcoin that can enable them to make the societal change.

Cyber activism can be divided into various subgroups according to the ideology they pursue. The most notable are hacktivists, crypto anarchists, (crypto) anarcho capitalists and cyber terrorists. We can definitely discuss other possible groups as the distinctions between them are fluid as the cyberspace itself. These groups can easily overlap as cyberterrorist can be easily perceived as hacktivists because more authoritative regime will call benign hacktivists with only protest aim cyberterrorist if they jeopardize political objectives of the authoritative regime. Moreover, some actors may have their ideology less important in their motivations, the others more important. However, the

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

[41] Ludlow, *Crypto Anarch. Cyberstates, Pirat. Utop.*

point is that all of these actors, whether organized in groups or single faint dark night wolfs, are using technology to enable their ideological ends.

It should be emphasized that the transfer of activism to the cyber space has transformed it. We argued in the section about cyber space that it changes its shape as our habits how to use it change. As protesters became anonymous and their causes borderless, civil disobedience can turn into political disruption. The difference is – now just a few skilled individuals are enough (or even enjoy more significant power) to cause disruption with a click than masses of people occupying streets [42]. Such super-empowerment of individuals is understandable perspective as some of their capabilities can be equal to what nation states can do [43], however, at the same time this perspective and the inability to measure the power nurture the idea that hackers can do whatever they want including triggering international warfare [44].

4.2.1 Hacktivists

'Hacktivism' is a portmanteau of 'hacking' and 'activism'. The term was coined by Omega, the member of the US retro hacker group Cult of the Dead Cow in the 1990s [45] in the early days of the World Wide Web. They are all used to describe a form of political activism in which computer hacking skills are actively engaged against government entities, commercial institutions, corporations or individuals [46].

Hacktivism has its roots in the early days of the Internet. Those days, hackers primarily congregated on Usenet and message boards. The fact that many "of those early hackers were motivated by idealism, with a general tendency towards left-wing, anti-capitalist, anti-corporate viewpoints (…) combined with a sense of anarchic mischief and a love of messing with people and systems, spurred numerous hacks protesting various social and political issues" [47]. With the rise to stardom of activists Anonymous and hacking group LulzSec, cyber-attacks are said to have entered a new phase. (Mansfield-Devine, 2011)

Nowadays, hacktivism applies to both individuals and groups that use hacking to bring about political or change, thus merging traditional political activism with the Internet. Hence, cyberspace becomes the medium that allows them to express their political and social discontent [48]. More specifically, cyberspace resources become a means of general protest, promoting an expressed ideology or a political agenda, in legal or (more commonly) illegal ways. In addition to this, hacktivism can indirectly be utilised to reach hidden, underlying goals of political, military or commercial character. In some sense, hacktivists may be perceived as a cyberspace equivalent to the groups carrying out acts of civil disobedience, such as Greenpeace. [49] Their actions, more often than not, have no lasting effect on their targets beyond reputation. [50] Unlike cybercriminals, hacktivists are usually not motivated with financial profit. Rather, it is some kind of burning rage inside them that becomes targeted at their victims for whatever reasons. [51] In other words, they are motivated by a cause, no matter if they wish to embarrass celebrities, highlight human rights, wake up a corporation to its vulnerabilities or go after entities whose ideologies they do not find agreeable, who they feel do not

[42] Magal, "WHO ARE THE HACKTIVISTS?"

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

[44] Schmidt, "The Birth of Cyber as a National Security Agenda (PhD Thesis)."

[45] Jeff Shantz, *Cyber Disobedience: Re-Presenting Online Anarchy*.

[46] Sorell, "Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous."

[47] Afifi-Sabet, "What Is Hacktivism?"

[48] Gargano, "Three Common Threat Actors and the One You Might Not Know About."

[49] Ohlin, Govern, and Oxford, "Nicolò Bussolati ' The Rise of Non-State Actors in Cyberwarfare ."

[50] Security, "Cyber Threat and Cyber Threat Actors," 2018.

[51] "Proactive Defense: Understanding the 4 Main Threat Actor Types."

align with their political views or practices [52] [53]. Hacktivists may also steal and disseminate sensitive, proprietary, or, sometimes, classified data in the name of free speech. [54] Unlike the majority of attackers, hacktivists do crave publicity; this is why they often enter public, popular social media platforms, like Facebook, Twitter, or YouTube. Hence they are eager to e.g. share the data they have stolen. [55]

It is difficult to construct a profile of a typical hacktivist, since this mixed group of people may consist of individuals ranging from script kiddies to professional black hats, from bored teens to rogue non-state actors and from lone cyber-vigilantes to cyber-groups. [56] "They may range from local units composed of no more than a dozen persons to large transnational organisms with several satellite sub-groups."[57] What they do have in common is that they are almost always personally anonymous, yet they seek a collectively distinguishable recognition [58]. Also, most of them connect through a variety of non-mainstream social networking services, such as forums and message boards like „4chan", wikis like „Encyclopaedia Dramatica or specific IRC channels. [59]

As hacktivists often work alone, their attacks are extremely difficult to predict, or even respond to quickly and whether they are a network administrator, a mid-level IT person or even a college student, there is no way of knowing in advance who they are or when they will strike. [60]

Hacktivism causes controversies. No matter how noble the cause, the cyber attacks hacktivists carry out are objectively illegal. On the other hand, some people actually applaud vigilante hackers who take the law into their own hands. [61] Although the today's mainstream usage of the world 'hacker' mainly refers to online criminals, understood as highly skilled individuals who are capable of subverting computer security to "crack in", hacktivist are challenging this view as they cause the social imaginary to stretch, usually between harsh criticism and exaltation. Their activities are generally of lawless nature. Thus, hacktivists divide the public opinion. Does the fact that they wish to raise awareness about a particular matter and bring about some kind of social or political change make them 'good'? Hacktivists themselves often claim their actions are for the greater good, e.g. in order to encourage better security or a more responsible custodianship of personal data. [62] However, their weapon of choice is information – unfortunately, mostly stolen. Therefore, are they in fact criminals? Actually, how people categorise hacktivists depends mostly on whether they sympathise with the same causes they do. [63] As Dan Lohrman describes this moral and ethical dilemma: *"There is an evolving definition of right and wrong regarding hacking. For example, I may think that Edward Snowden stealing NSA records was wrong. However, I may also agree that the information he disclosed was valuable to society to help protect online privacy. Although I do not believe that the ends justify the means, millions of Americans now believe that Snowden was a hero. Bottom line, they think his illegal actions were justified."* [64] However, there are often situations in which popular discourse does not back up hacktivists – especially if their targets are not only faceless institutions, businesses and

[52] Fowler, *Data Breach Preparation and Response*.

[53] Sigholm, "Non-State Actors in Cyberspace Operations."

[54] Sigholm.

[55] Mansfield-Devine, "Hacktivism: Assessing the Damage."

[56] Sigholm, "Non-State Actors in Cyberspace Operations."

[57] Ohlin, Govern, and Oxford, "Nicolò Bussolati ' The Rise of Non-State Actors in Cyberwarfare ."

[58] Dogan, "Contextualizing Hacktivism: The Criminalization of Redhack."

[59] Sigholm, "Non-State Actors in Cyberspace Operations."

[60] "Proactive Defense: Understanding the 4 Main Threat Actor Types."

[61] Afifi-Sabet, "What Is Hacktivism?"

[62] Mansfield-Devine, "Hacktivism: Assessing the Damage."

[63] Magal, "WHO ARE THE HACKTIVISTS?"

[64] Lohrman, "Hacking For Cause: Today's Growing Cyber Security Trend."

governments, but also 'regular' individuals. Then, what was meant to be transparency turns into harassment. [65] In addition, hacktivism is no longer driven by well-meaning amateurs or bored teenagers. Its nature is changing; the cause-based hacktivism is being replaced by heavy-duty, politicised attacks – even attacks carried out by nation states. [66] Finally, retribution, containment and negotiation can be very difficult, as it is not possible to point to a specific leadership in an offending organization. Even when a large crackdown against hacktivists occurs, it still equals a small fraction of the actual number of individuals involved. After 14 members of Anonymous were arrested by the FBI, the movement swiftly regrouped and began taunting law enforcement anew. [67]

Hacktivists as for any other activists have as adversary nation states. They apparently want the liberation of the society through the technology but let's say clearly that hacktivists' motivation is to make people more decision-capable by using more complex tools in their life that will make them more free as they will have more space to make the free decision influencing their life. That make hacktivists close to geeks that do not have any ideological motivations. While geeks do not have any ideology motivations, hacktivist ideology can be thus called *weak anarchy*.

4.2.2 Crypto anarchists

The crypto-anarchy movement has emerged from the capability based on opportunities of a globalized cyberspace. We can date the origins of the movement to the year 1988 in which *The Crypto Anarchist Manifesto* was written by Timothy C. May and publicly read at the Crypto '88 conference; later it was used as a founding paper for a crypto anarchist movement in 1992.[68] Consider the dates, the World Wide Web emerged in 1989 in its prenatal shape; the first web browser was written by the author of HTML language Tim Berners-Lee, an employee of CERN in Switzerland, in 1990. The manifesto looks forward to the future and declares how the future of cyberspace should look like. Let me cite the manifesto completely (emphasis is made by me for further argumentation):

> "A specter is haunting the modern world, the specter of crypto anarchy. Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a *totally anonymous manner*. Two persons may exchange messages, conduct business, and negotiate electronic contracts *without ever knowing the True Name, or legal identity*, of the other. Interactions over networks will be *untraceable*, via extensive rerouting of *encrypted packets* and tamper-proof boxes which implement cryptographic protocols with *nearly perfect assurance against any tampering*. *Reputations will be of central importance*, far more important in dealings than even the credit ratings of today. These developments will alter completely the *nature of government regulation*, *the ability to tax* and *control economic interactions*, the ability to *keep information secret*, and will even *alter the nature of trust and reputation*. The technology for this *revolution*—and it surely will be both a social and economic revolution—has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences *monitored closely by the National Security Agency*. But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable. And the next ten years will bring enough additional speed to make the ideas *economically feasible* and *essentially unstoppable*. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers, and encryption chips now under development will be some of the enabling technologies. *The State* will of course *try to slow or halt* the spread of

[65] Magal, "WHO ARE THE HACKTIVISTS?"

[66] Caldwell, "Hacktivism Goes Hardcore."

[67] Pompon, "Doxing, DoS, and Defacement: Today's Mainstream Hacktivism Tools."

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

> this technology, *citing national security concerns*, use of the technology by drug dealers and tax evaders, and *fears of societal disintegration*. Any of these concerns will be valid; *crypto anarchy will allow national secrets to be trade freely* and *will allow illicit and stolen materials to be traded*. An *anonymous computerized market* will even make possible abhorrent markets for *assassinations and extortion*. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy. Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will *cryptologic methods fundamentally alter the nature of corporations* and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus *altering forever the concepts of land and property rights* in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which *dismantle the barbed wire around intellectual property*. Arise, you have nothing to lose but your barbed wire fences!"

The depicted future in 1988 has materialized in today reality in a very similar shape as predicted. The *true name* or *legal identity* today is a luxury in any social network other than Facebook and Facebook does not provide us with certainty about the names of people around. Russian trolls would serve as an example to that no-rule. The *non-traceability* is in national security discourse described as the *attribution problem*. The fact that people wanted to be untraceable made untraceable states as well and finally founded one of the biggest problems in cyber security. The attribution problem produces dilemmas in all meaningful policy related debates. No attack can be fully attributed to a particular state even when some "proof" based on "sophistication as a criterion"[69] is available; the complexity of forensics makes it a near impossibility. This fact causes serious troubles to the international law application, which has been thoroughly studied,[70] but is shortsighted against threats of slow *societal disintegration* that states finally have to face.[71]

Traceability is directly related to currently used communication technologies such as the IPv4 protocol that has been used since 1972, but also to *encryption*, which is a very heated debate today as it has been the last decades. The most recent moment, in which the corporation Apple denied the request of FBI in the United States to unlock a mobile phone of a killed terrorist in California, might serve as a clear example.[72] Apple argued that they simply could not assist the FBI in this possible leading case as they do not have only American clients and that cracking the phone would show that the security of Apple products is only a marketing whiff. Additionally, decrypting phones does not mean decrypting all the possible encrypted instant messaging that might still be inside the phone, so the FBI's request does not follow their needs. Another argument is that assisting the FBI could mean a need to assist any other governments in the future, including authoritarian governments. Finally, the FBI made its own way into the phone and the possibility of a third party involvement was not denied.[73] The latest news shows that the FBI was probably not able to break it without an intervention of a third party.

The debate is not limited to one case with Apple. The threat of global terrorism usually raises a question of whether anonymity should equal privacy and whether ultimate anonymity is defensible in

---

[69] Guitton and Korzak, "The Sophistication Criterion for Attribution."

[70] CCDCOE, *Tallinn Manual on the International Law Applicable*; Schmitt, "International Law in Cyberspace: The Koh Speech An."

[71] Schmidt, "Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War"; Ranger, "The New Art of War: How Trolls, Hackers and Spies Are Rewriting the Rules of Conflict."

[72] The~Economist, "Taking a Bite at the Apple."

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

the long run.[74] The current situation in instant messaging for mobile phones already gives *nearly perfect assurance against tampering*. The terrorists of the late 2015 Paris attacks used the nearly perfectly secure instant messenger Telegram,[75] which is understood as a nearly unbreakable system.[76] Breaking the iPhone would certainly not solve all the obstacles of encryption in catching terrorists.

All of these services have become *economically feasible*, Telegram is for free and such services are literally *essentially unstoppable.* No authority has power to enforce the drop of the encryption technologies and when the technologies are cleverly developed there is no chance to break them. The accessibility to such technology today is not limited and there are no prospects it might be in the near or far future. We have to take into consideration that fighting liberating technologies in cyberspace, especially these, which play a role in intellectual property laws violations, has only produced more durable technologies for the same purpose. In that perspective, its *illicit usage, tax evading* or *societal disintegration* has become everyday reality. Governments are losing control over a vast amount of human activity as Sheila Jasanoff argues [77] and they were not in this situation.

Another example of the trend how states are losing control over technology and its influence on society would be the case with global taxation. It has become a problem with services such as the global accommodation portal AirBNB or global taxi service UBER.[78] All of these services have become true thanks to a rising trust in *online reputation.* Systems of reviews and feedbacks are becoming important for our digital identities; the possibility to buy or sell products on portals such as eBay has become real only thanks to the system of *online reputation of our digital identity.* The self-control reputation systems provide better security to users than states through their regulation and law enforcement. Understandably, when it comes to these services, states do their best to put them under control. However, as the tax collection of global players is not an easy task, they also tend to prohibit them at all within their territories, but they barely can. Uber is a peer-to-peer service between users' mobile phones only and its success is visible all around the world.[79] Governments of course try to deal with this reality of their erosion in tax collection and regulation ability and as I argue later they have two options. Either to free ride as some countries do when they provide tax havens or unite in order to regain power in global business taxation, regulation and governance.

Another topic mentioned in the manifesto and clearly visible today is the inability of states to keep national security secrets. Cases such as those leaked by Edward Snowden show how one dedicated man can significantly damage national security structure and how security policy is regarded by the public. Snowden is a clear representative of these fundamental fears. It shows fears about implications coming from a huge amount of data about hundreds of millions of people in the hands of few.[80] It shows what implications the application of crypto-anarchist ideology in practice can have to national security – a destruction of confidence into a concept of a nation state, in case of democratic states, in a democratic nation state which is quite more important as it does decreases confidence in the liberal democratic regime. Here, it is important to mention that illiberal behavior of once considered liberal democratic state necessarily deconstruct citizens' perception of its legitimacy.[81]

The whole situation with intellectual property that has changed the world from distribution of recordings on plates to data streaming all around the world was predicted as well. The idea of information smuggling is visible in private intelligence driven operations such as Red October[82] and

---

[74] The~Economist, "The Terrorist in the Data."

[75] The~Economist, "Unfriended."

[76] Telegram.org, "FAQ Telegram Security."

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

[78] The~Economist, "All Eyes on the Sharing Economy."

[79] The~Economist, "Uber Is Now More Popular than Taxis or Car Rental with Business People."

[80] The~Economist, "Over to the Dark Side."

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

[82] Gomez, "Operation Red October Fuels Debate over Cyber Espionage."

the remark on *CryptoNet* is certainly the *Darknet* today in reality. The former predicted, the latter depicted by authorities that needed to add the dark connotation in their defense to make clear who possesses legitimacy. The clear emergence of two fighting discourses based on one emerging reality. However, all of the above-mentioned examples show one single phenomenon and that is the decay of power of nation state. In case of data streaming, millions people pay to Spotify, while the nation states have nothing to say to the service and how it does treat authors of music, the market does. In case of Red October shows that nation states will not need to be part of international espionage nexus because they can simply buy information from the decentralized networks. Darknet is a good environment for intelligence agencies to keep cover and so on. The situation at the same time causing decay of nation state power, while it does creates a new power environment where decentralized networks exist alongside with nation states. The world is changing and a lot as predicted in the manifesto.

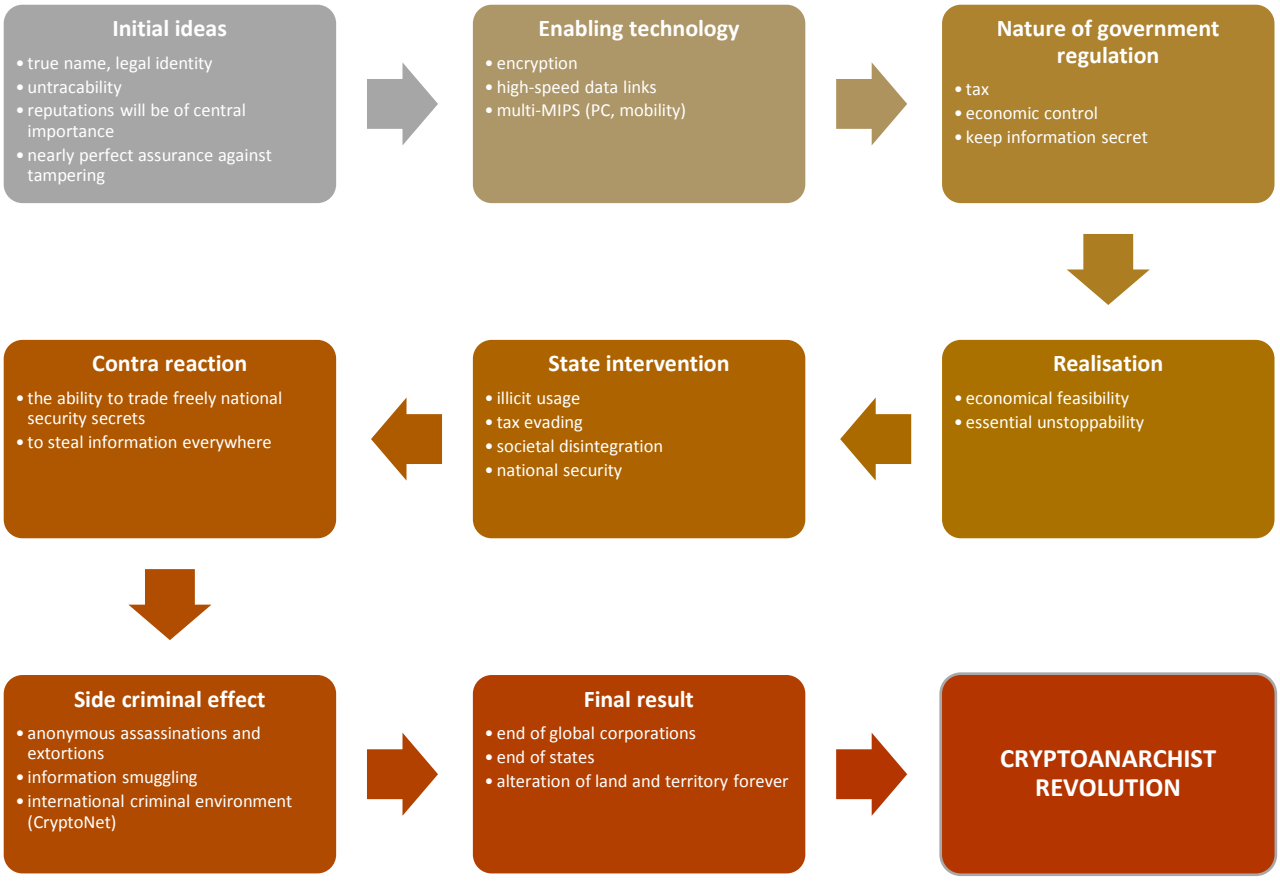

Figure 1 - The Crypto Anarchist Manifesto logical structure

Additionally, thirteen years later the reality was on the way. In an edited book from 2001 named *Crypto Anarchy, Cyberstates and Pirate Utopias*, the editor Peter Ludlow in the introduction argues that these utopic *cypherpunks* might be soon or later able to escape detection by states using advanced cryptography.[83] Seven years later Satoshi Nakamoto, still probably a genius ghost[84] who has never been met by anybody, published an article explaining the mathematical model of Bitcoin, which has

[83] Ludlow, *Crypto Anarch. Cyberstates, Pirat. Utop.*

[84] Greenberg and Branwen, "Bitcoin's Creator Satoshi Nakamoto Is Probably This Unknown Australian Genius."

since been the first widely used digital currency, which is also called a crypto currency.[85] The system is designed so that all transactions between wallets are open and visible to everybody. The system is used as a perfectly reliable clearing service for transactions as the clearing is provided by the community, which *mines* bitcoins by providing computing power for the clearing process. However, it is still bulletproof for hijackers on the way. Moreover, if an owner of a wallet is not making mistakes, the real identity is not discoverable. That includes exchanges with real money as the owner of an encrypted wallet is not known; yes, there are methods on how to unveil the identity by combining more data flows from one or other sources[86] or simply by buying a product delivered to a particular address, but supporting an assassination of a hated politician with anonymous bitcoins is reality as well[87] and it was mentioned as a possible future in the Crypto Anarchist Manifesto. Germany, for example, recognized bitcoin as a "private money" in 2013 and made it a totally legal currency; however, it is not recognized as a foreign currency, nor as a product, but as a "unit of account".[88] Other countries, in the contrary, have made it illegal; including Russia, China, Laos, Iceland or Bolivia.[89] The question whether these countries can effectively regulate the exchange in cyberspace remains clear; they cannot. Fifteen years earlier, the question of a completely detached cyber-crime environment was a discussion within utopias, right now it is a reality.

Dorothy Denning argued in 2001 that a new technology called *key escrow* will exchange the liberal cryptologic methods with new one into which the authorities will keep access,[90] while she argued against the feasibility of crypto anarchy ideas. Dorothy Denning finally admitted the low probability of spread of this technology and usage just in the next chapter.[91] However, the reality today is more complicated. Corporations use that technology to watch communication of their employees in general, while authoritarian states do the same, e.g. Russia, which is a bit special as each developer of any cryptographic technology needs a license according to the Russia Federal Law N 128-FZ *On Licensing Certain Types of Activity*. This is for sure not a solution as software can be acquired globally with no real restriction and if states restrict access to particular webpages, one can use The Onion Network to access everything and remain anonymous.

An example about this losing battle between governments and geeks comes from Russia. In the case with VKontakte and Telegram messenger. They were both developed by Nikolai and Pavel Durov, Russian citizens who had to leave VKontakte when the government took over this most popular social network in Russia. The specific advantage of Telegram in comparison to all other messengers around is that encryption keys are generated, stored and deleted in each device. There is no way to break the system from a central point; authors do not save these keys on servers. This characteristic can be easily confirmed as the software is open source; thus community driven (the open source code is available to everybody). An example of community driven power over state institutions hardcoded into the software, which in addition has its own API, hence the logic can be used in infinite instant messengers others will develop later.[92] There is no way for anyone to break it. The spread of such technology would make the *key escrow* technology a nonsense.

---

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

[86] A list of proven methods are available in Reid and Harrigan, "An Analysis of Anonymity in the Bitcoin System," 5–6.

[87] Boas, "Sinister New Site 'Assassination Market' Enables Users to Contribute Bitcoins for Murder of US Officials."

[88] Clinch, "Bitcoin Recognized by Germany as 'Private Money.'"

[89] "Bitlegal Tracks the Evolving Regulatory Landscape of Cryptocurrency, Digital Assets and Distributed Ledger Technology around the World."

[90] Denning, "The Future of Cryptography."

[91] Denning, "Afterword to 'The Future of Cryptography.'"

[92] Shu, "Meet Telegram, A Secure Messaging App From The Founders Of VK, Russia's Largest Social Network."

One of the most profound examples where states cannot match geeks in their technological advancement is the Pirate Bay from Sweden; a torrent indexer. A web portal that provides just a list of torrents concerning movies, series, TV shows, porn, computer games, software and whatever else one can imagine. The torrent is a genius technology that is precisely designed to be unbeatable by authorities. How it works is that one user has a movie that others can download but not exactly directly from the user. That is where the torrent comes in. The point is that the availability of the movie is within the community of people who seek the movie; yet they do not know each other. Torrent clients maintain balance between each other so that new incoming users can download pieces from these who came before them and so on. The movie is not stored on a server, but pieces of this movie is stored on users' computers that have been connected for some time and already downloaded portions from those who already watch the movie in that time. The web portal Pirate Bay maintains a library of these torrent files and has been a target of authorities several times. The developers were sentenced to imprisonment for up to almost one year, but the community around has kept the system on.[93] The last attempt by authorities, the so called 2014 December raid, to topple down the Pirate Bay caused a switch of the used technology to a completely decentralized system CloudFlare, a company which offers reverse proxy services that helps sites to withstand DDoS attacks or other attempts of enforced shut down.[94] Right now, Pirate Bay does not provide even the torrent files, but only magnet links. Hence, the web portal is probably unbeatable by the law enforcement agencies, but also can withstand direct DDoS attacks. Hydra from ancient Greek legends would serve as a near perfect depiction where this battle leads.

A good example how technology can cause *societal disintegration* would be the development during the Arab Spring. Technology once reflected as a possible democracy enabler as put by Laura C. Morris: "in reality the Libya case demonstrates that Internet conviviality creates unity and has a democratising power that can be shared beyond what in the real world would be the traditional barriers of social and economic standing"[95] transformed into democracy disintegration tool. The phenomenon we have been experiencing especially since the annexation of Crimea is more a threat to democracy than its enabler and shows how social networks can be terribly misused.[96]

Crypto anarchists have a clear adversary in nation states. However, in contrast to hacktivists, crypto anarchists have a strong ideological objective. The enabling capability of technology, in crypto anarchists, is motivated by their belief that technology can enable completely new political system. Here anarchists may tend to overlap with the anarcho capitalists because the same community tend decentralize technology (anarchists) or to use it as an opportunity for global business (capitalists). Crypto anarchists are not geeks fascinated by technology, they use the technology to deliver anarchic ideology, better expressed utopian ideology of full independence on nation states. It is probably impossible that the technology they develop will one day dismantle nation states, however, what the technology is capable of is definitely a slow decay of power of nation states and decrease of our confidence in liberal democracy when some illiberal behavior is unveiled by the crypto-anarchic community. They are also capable to deliver tools that can be used by terrorists or services that will change a whole commercial sector as with music distribution.

While geeks do not have any ideology motivations, hacktivist ideology can be called *weak anarchy*, the crypto anarchists' ideology should be called *strong anarchy* as their objectives are strongly influenced by their willingness to reach the ideological shift in the society.

[93] Larsson, "Charges Filed against the Pirate Bay Four."

[94] "CloudFlare."

[95] Morris, "Contextualizing the Power of Social Media: Technology, Communication and the Libya Crisis."

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

4.2.3 Anarcho-capitalists

Actors including geeks, crypto-anarchists, cyber criminals but also nation states hidden behind the attribution problem are empowering themselves through cyberspace, they support development of particular technologies enabling them towards their objectives. Geeks deepen them through open-source concepts of open development groups of hundred thousand people; crypto-anarchists use them to enable their ultra-liberal ideology as they slowly move from idealistic anarchism to anarcho-capitalism, cyber-criminals to support their international criminal networks in reaching an objective of gaining profit and foreign countries in collecting industrial espionage.

A subgroup along with crypto anarchists would be crypto (anarcho) capitalists, known as anarcho-capitalists. The difference from crypto anarchists is that they do not act to reach the ideological ends in privacy and independence on state but believe into capitalist market principles as the best tool to liberate people in order to establish new society based on principles of free markets and private property using modern communication technologies. Anarcho-capitalists think that market can solve every single problem for good through Smith's invisible hand. They believe into self-regulation of every aspect of our lives and that such self-regulation can only leads to good ends. Trust is a commodity that can be exchanged, thus even courts would be making decisions in market competition. Laws are reflected as violent coercion because of the threat of imprisonment.

Anarcho-capitalists is a group of radical anarchists that have grown on the shoulders of traditional anarchism, used technologies developed by geeks or crypto anarchists who wanted to liberate people from authority oppression, however, anarcho-capitalists went further and want to use these technologies for a radical societal change. The anarcho-capitalist political philosophy is mainly enabled by the success (and fall) of bitcoin[97] that proved enormous durability, concentrated massive capital but mainly was developed on the blockchain principle that is truly revolutionary technology. Blockhain has the capability to deliver undisputable trust by saving any transaction into a chain/ledger that is publicly available and non-editable as any following edit adds a string to the chain.[98]

As anarcho-capitalist ethics argue for the right of private property, or community property or joint non-public ownership relation,[99] blockchain is the kind of enabling technology capable to deliver the trust in the business exchanges, in saving ownership or even social position to the blockchain ledger. Anarcho-capitalists see the state as an enemy because state capitalism does not offer truly free exchange between people but only provide a limited regulated capitalist-like environment. In this light, anarcho-capitalist are communicating radical ideology that if adopted through the enabling technologies can at least lower the power to regulate of certain people behaviours by the authority of a state. Here, we argue that observing cyber space only as a space of possible clash of hackers and states is quite limited because just a success of particular technologies and their wide usage by citizens can begin fulfilling the ideological ends, the utopian radical visions of assumed freedom from states' oppression. However, it can also lead to more criminal activities perceived by anarcho-capitalists as their right, which can be then followed by others inspired by the utopian vision of ultimate liberation.

4.2.4 Cyber militias

Cyber militia are defined as "a group of volunteers who are willing and able to use cyber attacks in order to achieve a political goal." [100] The definition also encompasses the ways the members of a militia contact and gather: "the members communicate primarily via Internet and, as a rule, hide their identity". The anonymity is usually achieved by adopting hacker aliases. Cyber militias may be permanent or be formed ad hock. The definition emphasises the fact of the members being volunteers,

[97] Flood and Robb, "Trust, Anarcho-Capitalism, Blockchain and Initial Coin Offerings."

[98] Iansiti and Lakhani, "The Truth about Blockchain."

[99] Holcombe, "Common Property in Anarcho-Capitalism."

[100] Ottis, "Proactive Defense Tactics against On-Line Cyber Militia."

as they participate in the cyber militia of their own free will. They are not contractually obliged to it. Usually they do not receive any money for their actions. There are exceptions to this; sometimes the leaders of a cyber militia are paid through salaries.[101] In addition to this, a member of a cyber militia decides upon their level of commitment. They may also leave it whenever they wish. This is the main difference between the members of the cyber militia and the people who join a government-run cyber-attack unit. Ottis also indicates that the word "political" in the aforementioned definition "refers to all aims that transcend the personal interest of the volunteer. This includes religious views, nationalistic views, opinions on world social order etc."[102] According to Ottis, most cyber militias meet the following criteria:

- the communication within the militia is centralized; the communicating, planning and coordinating a cyber-attack campaign usually relies on on-line forums and instant messaging services,
- there is no direct state support or control of the militia. If there is direct state support, the unit should be considered an organic part of the state rather than the cyber militia,
- the members are loosely connected in real life; the leadership/core group may be personally acquainted, but the rest of the members usually do not know any other members or know a few of them.

Forum posts allow identifying the roles certain members play in the militia. They can be divided into two categories: "officer" roles – leaders, trainers, suppliers, etc., and "soldiers" and "camp followers". The leaders motivate to act, coordinate actions and give the directions of attacks. The trainers give instructions of all kind, including the ones concerning reconnaissance and attacks, as well as covering them. The suppliers are responsible for providing scanners, malware, attack kits, etc. "Soldiers" are the ones who take active part in attacks. They usually remain quiet on the forum or are ordered to report the results of their actions. Lastly, the camp followers follow the forum threads out of curiosity but do not take part in any campaigns. [103]

One of the most well-known cases of the employment of cyber militia is Estonia, where volunteer hackers were recruited to respond to cyber-attacks. Those civilian defence corps grew out of the aftermath of a 2007 attack, when banking, government, news and other websites were attacked online.[104] Cyber Defence League was later added to the 11.000 strong volunteer Estonian paramilitary army called Estonian Defence League, which was set up after the World War I.[105]

Although Vladimir Putin's government denied involvement in 2007 attacks, authorities blamed Russian operatives. According to experts, the attacks have been one of the worst cases of state-sponsored warfare to date. Although the Estonian cyber militia hackers are mostly civilians, they have been trained to handle this kind of assaults on hospitals, banks and military bases, as well as, on e.g. voting systems. Their commander, Andrus Padar, says that the threat is taken as a given: "We have a neighbour that guarantees we will not have a boring live". His militia consist of all kinds of white-hat types, including amateur IT workers, economists, lawyers and so on. Some of their actions include running drills with troops, doctors, air traffic controllers etc. and gauging officials' responses to realistic attacks, for example by sending out e-mails with sketchy links or dropping infected USB sticks. Allegedly, a CD labelled with a picture of Russian porn star in a bathing suit proved very effective bait for military officials. As a result, at present the country's military computers turn off after having detected an unknown disc or USB drive. Officially, the militia is part of Estonia's national guard.

[101] Drozdiak, "One of Russia's Neighbors Has Security Lessons for the Rest of Us."

[102] Ottis, "Proactive Defense Tactics against On-Line Cyber Militia."

[103] Ottis.

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

[105] Kramer, "Cyberpower Natl. Secur."

Estonian's cyber militia has inspired many security officials elsewhere, including countries like France, Latvia and the U.S. [106]

China has also relied heavily on cyber militias. According to researchers, the collective membership of cyber militias in China has already amounted to over 10 million people. Most probably, the goal of the cyber units is to provide logistic support and rear area security for active duty units – similarly to militias in general. One of the most well-known faces of the Chinese cyber militias are the infamous, popular, nationalism-driven "patriotic hackers". [107]

In the United States of America, one of the cyber militia, Missouri National Guard Team, has recently launched a non-profit organisation in order to share their network security monitoring system "built by cyber warriors for cyber warriors".[108] In Ohio, a bill has been introduced that is going to create a civilian cyber militia, the task of which would be to protect the state's critical government agencies and election systems. If the bill is passed, a new volunteer unit would be created under the authority of the Ohio adjutant general and operate at the same level as National Guard. The Ohio Cyber Reserve would recruit "individuals who are interested in improving Ohio's cyber posture".

In India, in 2011, Information Technology Minister Kapil Sibal called for a community of ethical hackers to help defend Indian networks. Reportedly, India has been considering using patriotic hackers for offensive operations, too.[109]

There is a lot of controversy surrounding cyber militia. Gady enlists the possible positive outcomes of employing the "members of the cyber militia, recruited among a pool of civilians with the requisite forensic and IT skills." He states that the rotation of people "through advanced cyber defence training, a state would not only create a large pool of experienced specialists for protecting critical information infrastructure, but it would also have significant spill over effects for the national economy by boosting innovation and entrepreneurship in the IT sector". He also believes, that "such a force would serve as both a best practice hub for cyber defence and a coordinating body for a whole-of-nation approach to massive cyberattacks". Lastly, he states that it could "help deter non-state actors and nation states from engaging in attacks. By employing a non-military "resistance" force, a country can suffer a decisive blow to its government and military systems but still wreak havoc on an adversary's economy and military logistics and personnel." On the other hand, Segal warns that addressing problems through the cyber militia might have a destabilizing effect on the region. It is true that one of their biggest selling points is their plausible deniability, as states can simply claim they know nothing about attacks. However, it is feared that the members of militias may use their skills and knowledge against other states with no authorization, or even turn them back on home networks. Militias may also ignore orders, especially during a crisis. As Segal sums it up, "patriotic geeks might be the answer to a lot of policy challenges. But in terms of cybersecurity, it may be best to either bring them completely into the fold, or keep them at arm's length."[110]

4.3 Criminals

"It is with no doubt that cyber-crime has started playing a significant role in our lives." A similar sentence can be seen across all relevant annual reports concerning the topic of cyber-crime from cyber security firms, law enforcement agencies or technology corporations that are dependent on solid security such as Microsoft or Apple. However, what is cyber-crime then? One definition would be *any criminal activity enabled by cyber means*. It might look like that we have criminals on the one bank of the river and law enforcement on the other. It is not clear as it may look like.

---

[106] Drozdiak, "One of Russia's Neighbors Has Security Lessons for the Rest of Us."

[107] Lyall, "China's Cyber Militias."

[108] Seffers, "Cyber Militia Launches Nonprofit to Share Technology."

[109] Segal, "The Rise of Asia's Cyber Militias."

[110] Segal.

Some activities such as the defacement of a webpage can be certainly understood by the geek community as a protest; even the DDoS attack on Estonia was by some people understood as a massive digital protest,[111] but clearly not as a means of cyber war. The right to protest is the first democratic liberty we possess.

In fact, for states some actions that can be meant as a protest are understood as a means of cyber war, for example by the political representatives of Estonia who wanted to trigger Article 5 of the Washington Treaty after the attacks of 2007.[112] Moreover, law enforcement agencies may understand a DDoS attack as a criminal offence against the liberty of the server's owner. The result might be a requirement on the attacker to repay the losses caused by the attack. Who is right? Is it a protest or a criminal act?

The damage is a debatable variable when it comes to data as it is in case when a peaceful protest takes place in the middle of the city. Is it damaging when one could not sell a burger on a street due to the mass protest taking place? The debate over losses caused due to the introduction of the Internet, especially in the music distribution business, is aligned in favour of how the business was made before the Internet. The music industry is a great example to demonstrate how the fraudulent digital distribution was a problem until the day producers found a way to distribute the content online as well. People not necessary commit "crime" on internet in order to get rich but because the illegal way is simpler. Academic databases prepaid by universities in comparison to Sci Hub is a good example of this argument. Especially when the academics are involved because the core question in academia is whether the publishers should make so much money on scientific publications while the scientists do not. This is ethical question and at least ethical assessment should precede the law if the law is broken massively.

Understanding DDoS attacks by hacktivists in that way might finally completely change the perspective of their security impact, whether as a national security concern or just as a crime causing damage. However, that does not apply to bank fraud, blackmailing people by encrypting their data with ransomware (kind of intelligently aimed to people including their postal addresses),[113] stealing credit card information on a seriously massive scale,[114] which is every year only getting bigger[115] or publishing the whole stolen national ID databases as in the case of Turkey on 4th April 2016.[116] Finally, it has not been a whole citizen database, but "only" about 50 millions.[117] The server with the link for torrents was very quickly down, but the torrent itself will live a long time as the technology is simply unbeatable[118] as it is still available three years later.

Some attack vectors are surprisingly simple. One can find vulnerabilities on desktop sharing software such as Teamviewer and scan the Internet with a bot for a running service on random IP addresses; if successfully detected, the hacker would take complete remote control over a computer and all security measures are for nothing. The digital ID, all passwords if saved in a browser, access to PayPal and other services could be leaked and the hacker could cause serious damage to one's life. All these actions can finally be done with automated bots. Not to mention that current phishing methods based on scam emails might quickly change to AI chatbots[119] learning from our own communication

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

[112] Shackelford, "ESTONIA THREE YEARS LATER: A PROGRESS REPORT ON CO."

[113] BBC News, "The Ransomware That Knows Where You Live."

[114] Palermo, "10 Worst Data Breaches of All Time."

[115] Kiesnoski, "5 of the Biggest Data Breaches Ever."

[116] Leyden, "Did Hacktivists Really Just Expose Half of Turkey's Entire Population to ID Theft? Entire Citizen Database? Probably Not."

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

[118] Paganini, "DB with Records of 50 Million Turkish Citizens Leaked Online. Are They Recycled Data?"

[119] Wakefield, "Hello, I Am BBCTechbot. How Can I Help?"

between family members about the meaning of life.[120] Risk of deception by artificial intelligence during our online lives is becoming closer than ever in that perspective.

4.3.1 Cyber-crime actors

The first problem that usually lies at the bottom of any classification is the overlapping terms and their fluid meaning. Cyber crime actors are usually all actors that operate in cyber space and perceived by law enforcement as those they should focus on. Following is the list of actors with respective motivations: *nation-states* with geopolitical motivations, *cybercriminals* seeking profit, *hacktivists* driven by ideological beliefs, *terrorist groups* spreading their hatred through ideological violence, thrill seekers fulfilling their satisfaction, *insiders* fighting their personal discontent.[121] However, some others might use another classification that delimit the criminal actors: *state sponsored actors* with geopolitical motivations tunnelled through so called cyber warfare, espionage, political, economic, critical knowledge or military agendas; *organized criminals* seeking profit that can for nation states paying for targeted espionage, *hacktivists* that are usually somewhere at the edge of the law and *lone wolfs* that can be whatever they want driven by varying motivations.[122] The second approach to classification better describes that all actors can actively pursue criminal acts for various gains, which not necessarily constitute national security issues.

Mixing nation states with state sponsored actors shows how the attribution problem casts a big problem on future cyber threat mitigation. International law cannot be applied if state is not attributable to the attack, however, states, especially with authoritative regimes, can be used as a proxy for interests of individuals to deliver significant economic or power benefits. This is another unconventional perspective arguing that not necessarily authoritative states are the threat, but the threat is the willingness of individuals exploiting their power through an actor – nation states – that has to be treated equally on the international level. Thus, cyber-crime empirical evidence should be the inspiration for future possibilities of nation states hijacked by individuals rather than doom scenarios of cyber pearl harbour imagined by people responsible for (conventional) national defence. We do not live in the world of 20th century and those easy comparisons to historical events is not producing clearer picture of the current situation. Analysing behaviour as cyber-crime provides us much better perspective what is in fact possible and what is a mere imagination of possibilities.

This argument, that the same activities can be perceived as cyber-crime by law enforcement agencies while the same activities are called a proof of ongoing cyber war by nation state actors, is crucial to understand the constructive message of critical security studies. The point is not to deny the possibilities but to lower the discursive impact of imaginations while building on empirical evidence which cyber-crime is providing.

4.3.2 Between crime and national security

The problem of securitization of cyber activities as national security agenda empowers national defence capacities that are often offensive, and which does not necessarily solve the growing problem. However, if these perceptions are directed to international cooperation tackling cyber malicious activities, they are becoming a case for law enforcement, which is about international cooperation and not international suspicion and common neorealist nonconfidence. Europol report could support this argument as it says that the problem of tackling cyber-crime is based on *"incomplete transposition of international instruments into domestic legislation*."[123]

---

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

[121] Security, "Cyber Threat and Cyber Threat Actors," 2018.

[122] Gargano, "Three Common Threat Actors and the One You Might Not Know About."

[123] EUROJUST & EUROPOL, "Common Challenges in Combating Cybercrime - As Identified by Eurojust and Europol."

International tensions thus end with international cooperation, apparently as everywhere, in cyber space as well. According to this Europol and Eurojust report the rising problems are prevalently in international cooperation, implementation of legal instruments on the national level, challenges to PPP projects and then loss of data and loss of location. The last challenge is caused by the rise of anonymization tools that, as argued above, these tools are nourished by the law enforcement itself. Cyber space is significantly changing the way we live and the balance between criminalization of old order and enabling the new one is all the time very thin. However, the point to the secure world is not in criminalization of activities destroying decades established business models, it is of course in securing everyday lives of people being hijacked in growing ransomware business but at the same time the politics need to reflect that geeks will continue to work for liberation of the society, that the development of liberalization/anonymization tools hampering investigations are also securing people from powerful actors that not necessarily have liberal order between their objectives. Corporation are one of them. Thus the proper analysis of power balance between various actors and their capability to shape our lives is important as the only legit actor to shape intentionally our lives is definitely the democratic one – the nation states.

4.3.3 Trolls as the actor between crime and national security

While some actors are following the principal agenda related to their role in the world, the others can be mercenaries – cyber mercenaries? Some would say that we can find cyber militias in China or that there are hackers gathering information to sell it as intelligence to nation states. Developers of tools by script kiddies or professional worm/spyware developers that can be used and misused for particular criminal purposes of other actors. Making any classification will remain tricky, however, we decided to add trolls because they precisely depict the division line between crime for revenue and crime that turns to national security agenda.

Although the idea of "trolling" has been known for many years, there is a lack of academic consensus on the matter, owing to the fact it is a complex phenomenon.[124] Generally speaking, the term "trolling" has been used to describe all types of malicious or harassing activities in the Internet, both verbal and behavioural ones, with the latter mostly happening in the sphere of online gaming.[125] However, beyond this basic agreement, almost every researcher has coined their own definition of trolling. For instance, Bishop defines trolling as the "act of posting a message (…) that is obviously exaggerating something on a particular topic", [126] "for the entertainment of oneself, others or both."[127] Herring indicates that it "entails luring others into often pointless and time-consuming discussions."[128] Another definition points it out that a troll "posts a deliberately provocative message (…) with the intention of causing maximum disruption and argument."[129] Cambria et al. define trolling as "emotional attacks on a person or a group through malicious and vulgar comments in order to provoke response."[130] Shachaf & Hara call trolling "repetitive, intentional and harmful actions that are undertaken in isolation and under hidden virtual identities (…) consisting of destructive participation in the community".[131] Hardaker says trolling is "the deliberate use of impoliteness/aggression, deception and/or manipulation (…) to create a context conductive to triggering or antagonising

[124] Cook, Schaafsma, and Antheunis, "Under the Bridge: An in-Depth Examination of Online Trolling in the Gaming Context."

[125] Cook, Schaafsma, and Antheunis; Jussinoja, "LIFE-CYCLE OF INTERNET TROLLS."

[126] Bishop, "Tackling Internet Abuse in Great Britain: Towards a Framework for Classifying Severities of 'Flame Trolling.'"

[127] Bishop, "The Effect of De-Individuation of the Internet Troller on Criminal Procedure Implementation: An Interview with a Hater."

[128] Herring et al., "Searching for Safety Online: Managing 'Trolling' in a Feminist Forum."

[129] Alien Entity, "Urban Dictionary: Troll."

[130] Cambria et al., "Do Not Feel The Trolls."

[131] Shachaf and Hara, "Beyond Vandalism: Wikipedia Trolls."

conflict".[132] Finally, Golf-Papez & Veer define it as "deliberate, deceptive and mischievous attempts that are engineered to elicit a reaction from the target(s), are performed for the benefit of the troll(s) and their followers and may have negative consequences for people and firms involved".[133] As one may notice, although older definitions of trolling concentrated on stirring up discussions mostly for fun and amusement, the newer ones point it out that trolling aims to do emotional harm. The most recent ones emphasize the disruptive and deceptive nature of the acts of trolling. It may be thus stated that Internet trolling has become much more serious, harmful and potentially dangerous than it initially used to be. In fact, its potential as a tool of spreading deceptive and made-up content has already been utilised by many individuals and organisations. In the recent years, a new sub-group of trolls have caught the media's attention: the political trolls. They are usually "user accounts whose sole purpose is to sow conflict and deception", their intent being "to harm the political process and create distrust in the political system,"[134] which is exactly the moment where malicious activities playing on the ground of common crime can turn into a serious national security agenda. Political trolls may be further divided into three groups: political bots masquerading as real users (spreading spam and harmful links), organized trolls (including hate and persecution campaigns) and the ones who spread "fake news." [135]

Recently, media have revealed several notorious cases of state-sponsored political trolling. For instance, before the 2016 U.S. presidential elections thousands of troll accounts injected false tweets or fake news in support or against certain candidates, aiming at creating discord and hate.[136] The accounts were traced back to Russia and allegedly funded by the Russian government.[137] Russian trolls were also highly active in Australia, in the years 2015-2017. Their actions included, e.g. spreading tweets undermining support for Australian government in the light of its response to the downing of flight MH17.[138] In 2016, Russia significantly influenced the way how Dutch people perceived the treaty with Ukraine, which was for example not about admittance to EU but was about helping Ukraine to direct its reforms towards working nation state based on rule of law, however, most Dutch people responded in the poll otherwise because of the fake news which were spread throughout the country before the referendum.[139] Another example how can a political power use trolls happened in August 2019. Polish Deputy Justice Minister Lukasz Piebiak resigned after it had been revealed he allegedly arranged and controlled a hate campaign and sought to discredit judges who were critical of the government's judicial reforms; it was done by planting media rumours about the judges' private lives. Then, the transcripts of alleged conversations between the minister and a woman known as "Emilia" were published. In them, they formulated plans to anonymously send out material with rumours about the judge who has been a prominent critic of the ruling party. Emilia acted as an intermediary between the ministry of justice and pro-government media and both posted the material online and sent letters, e.g. to judge's home. The report sparked a massive outcry in the country, because, as Anna Materska-Sosnowska, a political scientists at Warsaw University has put it, "This is dangerous for the state, for democratic order… especially because it affects judges and it is paid for with public money".[140]

---

[132] Hardaker, "'Uh. . . . Not to Be Nitpicky,,,,,But…the Past Tense of Drag Is Dragged, Not Drug.': An Overview of Trolling Strategies."

[133] Golf-Papez and Veer, "Don't Feed the Trolling: Rethinking How Online Trolling Is Being Defined and Combated."

[134] Addawood et al., "Linguistic Cues to Deception: Identifying Political Trolls on Social Media."

[135] Gorwa, "Computational Propaganda in Poland: False Amplifiers and the Digital Public Sphere."

[136] Gorwa; Pennycook and Rand, "Who Falls for Fake News? The Roles of Analytic Thinking, Motivated Reasoning, Political Ideology, and Bullshit Receptivity."

[137] Addawood et al., "Linguistic Cues to Deception: Identifying Political Trolls on Social Media."

[138] Sear and Jensen, "Russian Trolls Targeted Australian Voters on Twitter via #auspol and #MH17."

[139] Applebaum, "How Much Trouble Is Russia Causing in Europe?"

[140] Charlish, "Polish Deputy Minister Resigns over Judge Trolling Scandal"; Gf, "Onet.Pl: Deputy Justice Minister behind Campaign to Discredit Judges."

4.4 Corporations

The reason to add corporation on the list of actors is based in their undeniable role in cyber space security dynamics. Corporations are differing from SMBs mainly by their strict focus on profit as the central objective. Moreover, the profit is not limited to a particular territory, the profit is usually global and any SMB in cyber security experiencing success with its products becomes global very quickly.

Corporations can be divided into various sub actors. First actor, the cyber security companies, produce anti-virus or malware detection systems or other tools useful to deliver security in cyber space are making business on the perception of possibly insecure environment or on particular events considered as insecure. The problem of these companies is in fact that their interpretation or clear misinterpretation of numbers can significantly influence their business models. At the same time, our perception of security in cyber space is mainly dependent on information delivered by these companies. Even nation states can use their data to assess current dynamics in cyber space security and in a situation in which these companies have more global picture than nation states repeating the need of international collaborations, security delivered by nation states to their citizens is significantly influence by privatization and internationalization.[141] This is the kind of strategy that lies at the beginning of the post-Cold war era in foreign policy of president Clinton: *"Every dollar we take out of military R&D [research and development] in the post-Cold War era should go to R&D for commercial technologies, until civilian R&D can match and eventually surpass our Cold War military R&D commitment."*[142]

Business contracts for nation states cannot be clear of influence by the companies willing to deliver their products which is quite contrasting to the conventional national security issues. When it comes to national security perspective, the military contracts are more or less still dependent on strategies delivered by experts of particular nation states or collective defence entities such as NATO. However, this new privatisation dynamics has been studied form a different perspective, from privatisation of the security service delivered by companies deployed directly to the battlefield.[143]

Second actors can be the key players in current global business between which we can certainly list companies such as Apple, Google, Amazon, Microsoft and other titans. During the Snowden's revelations, some of those companies where marked as part of the global espionage efforts where nation states and companies blurred into a network of assemblage. Zygmunt Bauman, a renown sociologist, along with other well respected thinkers such as Didier Bigo wrote a paper, in which they point on a dynamics where private and public blurs into undistinguishable assemblage, while it is the nation states which have social contract to deliver security to its citizens.[144] Their principal message is a question what we finally be securing when the business interests merge with national security. The merge is understandably based on the shortcoming of expertise, knowledge, intelligence capability of nation states. Bauman et. al. ask: *"Apologists for more intrusive and secretive forms of security often invoke extremist narratives about the threats we may face, but it is not difficult to imagine equally extreme narratives about the evisceration of the forms of modern subjectivity and self-determination that give security agencies much of their legitimacy. What, after all, are they supposed to be securing?"* More security brings less democracy. If security is based on imagined threats made out by corporations, the state will lose its sense and function and we will lose democracy.

The case of Cambridge Analytica is a good example of fulfilling prophecy by Bauman that put emphasis on the change of intelligence method gathering from high degree of certainty about a small

---

[141] Cavelty and Brunner, "'Introduction: Information, Power, and Security—an Outline of Debates and Implications."

[142] Clinton, "Remarks at Wharton School of Business, University of Pennsylvania on 16 April 1992."

[143] Krahmann, *States, Citizens and the Privatisation of Security*.

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

amount of data to high degree of uncertainty about a large amount of data. The former was a traditional intelligence approach because we hadn't had means to analyse huge amount of data, however, the latter approach cannot omit unnecessary data of citizens unrelated to the intelligence objectives which has only a result in lowering confidence of liberal democracy because even liberal nation states such as US or UK were knowingly involved, as Snowden revealed. The shift from discipline to control, from ingenuity to Big Data management, the merge of private and public as the biggest Big Data analysts needs more capacities than a single ingenuine analyst understanding the problem raises technical, ethical and power distribution questions.[145]

Corporations will continue to play significant role in our lives and global society, however, since we have not global parliament, we still depend on how strong nation states will be capable to regulate corporations, whether they will be willing and able to refrain from authoritative tendencies useful for ethically disputed intelligence methods by nation states or whether nation states will be willing to regulate corporations collectively. One good example come from the European Union. During the time when Mark Zuckerberg was heard at the European Parliament about the case of Cambridge Analytica, he mentioned, that it is not going to be United States of America who will finally regulate Facebook but European Union.[146] Zuckerberg openly mentioned that he is not in (complete) power of his own company, which is pointing on self-evolution of huge corporations and draws possible future if these corporations are driven only by capitalist principles without regulation delivered by democratic entities.

Third kind of corporation is not necessarily related to cyber space as the internet titans and cyber security companies are. As a third kind can be considered all other companies that are using cyber space as means for interconnecting their appliances into a smart home – the whole category of internet of things.[147] Until today, we have been dependent on cyber space related technology in means that could not influence significantly our physical environment. Beginning IoT the problem of sophistically controlled homes interconnected over internet using same software carrying the same vulnerability can lead to direct sabotages. These classical alarmist predictions are usually denied by the critical security scholars, however, the enormous rise of sensors into billions, trillions or quadrillions will have to be delivered with certain level of security. Some of these sensors will be sold by newly emerging titans or companies will be adopting shared firmware to ensure compatibility, the threat of exploiting of these networks of sensors influencing directly our lives will certainly raise. Internet of Things will be the kind of shift that our everyday lives will be again more dependent on technology.

Not only GPS-like systems are providing us information about our position directly influencing our decision making in world orientation and navigation, these systems fully replaced other previously used methods to make decisions. Here, we would like to put emphasis on the fact that the threat itself does not only emanate from hacking of these appliances or sensors causing our refrigerator freezing all the stored food but also emanate from our capability to make the right decision.[148] Corporations will thus play more important role in our lives than they have played already until today, which is again a quest for legitimate actors influencing our lives – the nation states or European Union or even bigger entities if some elected emerge to tackle the problem of security internationalization.

Power and governance is another area of concern regarding the role of corporations in future cyberspace shape. The current situation of multi-stakeholder governance of Internet has emerged from historical contingent events. That influences how cyber security is governed. Any ideas of unified cyber security governance will have to focus first on Internet governance and all attempts to change

[145] Lyon, "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique."

[146] "Mark Zuckerberg Calls for Stronger Regulation of Internet."

[147] Sicari et al., "Security, Privacy and Trust in Internet of Things: The Road Ahead."

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

the current status quo have failed.[149] This dynamics also play against the ideas of authoritative nation states to centralise governance of their portion of Internet. They are to some extent successful when it comes to balkanisation of Internet, however, as argued any action to take away liberties of freedom of choice of people behind their computers will produce more liberation tools developed by other actors. That means, corporations from other parts of the world, can come and liberate these people from the oppression of their governments. The most visible tool of such dynamics is VPN service. However, such dynamics will move cyber space more towards market governance as depicted by crypto (anarcho) capitalist but then the tool considered one day as a tool of liberation can become the tool of control the day later. It is an interesting dilemma for users whether to believe their democratic entities or use tools to avoid them but become a hostage of other actors. Here, one would argue that open source approach to the software development will keep multi-stake holder governance through market principles, however, the idea that technology can be perfectly kept decentralized is fictitious – networks tend to produce centres, centres temp power-inclining actors.[150] Any centralised power produced my market principles lacks democratic values and focuses on profit whatever it costs. If a massively used technology influencing how cyberspace works is in hand of a global corporation, it will certainly gain significant power and lower the power of democratically legit actor.

In summary, the challenges created by corporations as actors in cyber space security can be listed as follows:

- the conflicting interest between delivering and consuming security by cyber security companies,
- privatization of security in cyber space leading to a situation that democratically elected representatives of actors (nation states or European Union) are heavily dependent on privately delivered knowledge and measures, which is not only making these actors less important but also produces skewed pictures of security situation in cyber space,
- huge corporations, the internet titans, are producing enormous amount of data shifting the methods of intelligence conducted by nation states leading to a situation of another dependence on private businesses but also rising ethical questions whether nation states based on liberal democratic principles should even use big data and leave intelligence analysis ingenuity to history and if so how ethically can be such approach defended if it can be,
- given the above mentioned dynamics, corporations will remain and probably deepen their role in our lives raising a question which entity should regulate them to keep their activities within the boundaries of liberal democracy,
- IoT companies will influence our lives not only by delivering us appliances and sensors on which will directly depend in our smart homes, but will deepen our dependence on the information they produce when we make critical decisions,
- massively used key technologies will outbalance current multi-stakeholder governance and can empower corporations that are driven market principles.

4.5 (Nation) states

The area where cyber meets national security is probably the one most discussed today. When banks are losing money in credit card frauds and facing DDoS attacks on a daily basis and the biggest corporations experience credit card number leaks of hundreds of millions of users from their databases, it seems legitimate to ask when national security will be threatened by hackers. The first problematic question is where crime ends and national security concerns begins. Usually this question is answered by adding the state as an actor with assumptions that the state is a special actor. It is special at least in the way of what language it uses to secure its interests – it is a national security concern – a concern of us all which we should address with whatever means we have available. One

[149] Ellis and Mohan, *Rewired: Cybersecurity Governance*.

[150] Barabási, *Linked: The New Science of Networks*.

single move towards identifying what constitute national security concern has been the introduction of the term *critical infrastructure.* Countries usually have had a term identifying *objects needed for the security of a state* or a similar term, however, the introduction of *critical infrastructure* or *critical information infrastructure* is observable around the time of cyber security introduction to the national security agenda. As Myriam Dunn Cavelty shown, the term was not used before the cyber discourse was introduced to national security and has come with alarmist discourse of cyber terrorism.[151] Critical infrastructure does not constitute seriousness of the cyber attack, it does constitute whether the attack was conducted against the state. Thus, if we take this constructivist perspective, then states are becoming actors in cyber space by defining what belongs to them and thus national security concern is not constituted by the attack but by the state itself. On the other hand, thinking critically should not discard all possible cyber enabled national security threats but what remains a question is what seriously can cause an event that would threaten national security and what constitutes *national security* as a strategic objective.

However, how can we deal with a situation where we expect security to be provided by a state? When it comes to cyber security against cyber crime frauds, decentralized networks or particular non-state actors private companies are much more effective in dealing with these fluid troubles which strategy and kill chain changes every day. Moreover, where does the responsibility regarding my credit card number as a client of a bank end and where does the responsibility of the bank to take care of the security of their customers begin? And where the responsibility of the state begins?

We expect a state to take responsibility over general security of our daily life, we expect electricity to be delivered, that transportation works without traffic jams, stable prices, that other states do not wage wars against us etc. However, do we expect to keep electricity running by military units guarding electric wires from our homes to servers' switches or do we depend on our state to manage regime that regulate private sector's behaviour to deliver the service? Is it really cyber that threatens our lives to be the first threat in NATO strategy?[152]

4.5.1 National and international perspective

There are two terms, which are intermingled or used in confusion when authors talk about cyber related threats to national security. *Cyber war* and *cyber warfare*.[153] The former usually deals with interstate conflict on a general level using cyber means, while the latter might sometimes thoroughly discuss mean of waging a cyber war. According to the NATO CCD COE online dictionary, which collects different definitions from sources such as national strategies, other dictionaries or academic literature, there is no clear distinction and the institution does not provide its own definition.[154] Moreover, it is not hard to find academic articles, which use both terms with no regard to their different meanings. For example, a book called *Cyber Warfare: A multidisciplinary analysis*[155] deals with both problems (if we take the above mentioned possible distinction) and deliberately use the word *warfare* while referencing to articles criticizing the exaggeration of possible *cyber war* by pointing on a specific kind of conflict in the future, in particular espionage, sabotage, and subversion. Especially the Rid's article called *Cyber War Will Not Come* and the subsequent book discussed at the beginning in the literature review that he does not deny the capabilities or means of conducting an attack using cyber means or using cyberspace,[156] Rid conversely tend to put attention on means of warfare by addressing what is in

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

[152] NATO, "Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization."

[153] I would like to specifically thank here to Alex Crowther from National Defense University for our inspirational debate in Baku, Azerbaijan where we both presented our thoughts regarding cyber security on January 2016 at NISA Winter Session.

[154] Dictionary of NATO CCD COE can be found at https://ccdcoe.org/cyber-definitions.html

[155] Green, *Cyber Warfare*.

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

his perspective the real problem we face. However, James Green, the author of introduction to the mentioned book on Cyber Warfare[157] cites Rid's thoughts as *"views of a minority of commentators who have downplayed the threat."* The one who has read Rid's thoughts carefully would never say that Rid *downplayed the threat.* He tried to seriously analyse the exaggerated term, which is in policy analytically flattened into *"an undisputable threat"* that may happen while a cyber-attack that causes serious trouble somewhere else by other means can proceed without significant attention. Rid falls into the group of scholars who through reconceptualization of a settled concept raises questions about our reaction on the novel security situation, which can be exaggerated by applying our experience in conventional war while downplaying the novelty of the threat which has not been sufficiently understood.

Cyber war referred in recent history to very different campaigns of cyber attacks. At the beginning, cyberpunk subculture fed the imagination of many imaginable futures during 80s and even 90s. However, when the first serious attack on a country took place in Estonia in 2007, everybody turned to the first visible attack. Estonian officials actively promoted the attack as an attack to national security. Minister of defence argued that the cyber attacks should be compared to the naval blockade,[158] which should consequently trigger the Article 5 of the Washington Treaty.[159] NATO finally decided not to trigger the Article because there was no consensus over what constitute cyber war and if so whether such cyber war constitute a use of force according to the humanitarian international law. The years to come were dedicated to such discussion, which actually gave NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) to Estonia. State representatives are open in discussions and mentions that the best gift of the 2007 attack was the establishment of such a critical centre in Estonia. Thus, in the end the story of ongoing cyber war gave Estonia importance within the alliance and everybody around the world that a mere DDOS attack can be used to paralyze a whole country regardless the fact that today DDOS attacks are significantly bigger and the one in 2007 simply caught the country fully unprepared on such an event.

Moreover, when it comes to the Estonia attack, immediately after the attacks Estonians became world-wide recognized experts on cyber security due to their first-hand experience as transactors or translators of expertise.[160] They were immediately invited to specific cyber related researches as being respected world-class experts on cyber security; Estonians were two out of four contributors from Europe.[161] Estonians even personally admitted that the process of this recognition was an amazing gift;[162] even the Minister of Defense admitted it.[163] Beside this geek-to-national security expert transaction, we can witness the opposite direction, which is probably due to the enlarging cooperation between states and the private sector. Microsoft launched a program called the Government Security Program (GSP) already in 2003 to let governmental officials check their source code for vulnerabilities. NATO was involved in this program later, in September 2015, reaching numbers of 44 agencies and 26 governments checking the code right now. DARPA is willing to add artificial intelligence exactly to this process of code checking. Quoting ambassador Sorin Ducaru, an assistant secretary general of NATO's emerging security challenges division, *"we see this signing as another step forward in the NATO-Industry Cyber Partnership, building a stronger cyber defence network today with Microsoft, but also with other industry partners across the world."*[164] Private global corporations are now part of the global

---

[157] Green, *Cyber Warfare*.

[158] Cyrus FARIVAR, "A Brief Examination of Media Coverage of Cyberattacks (2007-Present)."

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

[160] Latour, *Science in Action: How to Follow Scientists and Engineers Through Society*, 108–21.

[161] McAfee, *Virtual Criminology Report 2009: Virtually Here: The Age of Cyber Warfare*.

[162] Based on a personal discussion at the Ministry of Defense of Estonia in Tallinn with Siim Alatalu, 21st Novemebr 2013.

[163] Aaviksoo, "Cyberspace: A New Security Dimension at Our Fingertips."

[164] Tung, "Microsoft Signs Deal to Let NATO Check Its Products for Backdoors."

cyber defence campaign dealing with cyber war. The intermingling process between national security experts dealing with national defence and experts on computer security is inevitable; however, despite the fact that the Estonia case might never happen again as the computer experts took countermeasures to avoid the same scenario.[165] Not to mention that according to widely available sites such as digitalattackmap.com we are facing quite bigger attacks today if the load of traffic is a measure than we witnessed in the Estonian case. Yet, we are not witnessing any political consequences as we have observed since the Estonian DDoS attack throughout the whole world; in every single national cyber strategy, from Africa, through Europe to South America and Oceania.

The next phase in cyber war discussion was the Stuxnet attack in 2010 immediately considered as a "cyber weapon",[166] which showed the world that a cyber attack can turn into a sabotage tool with physical consequences.. The possibility of such tool in hands of terrorist deepen the alarmist discourse that now every hacker can hack nuclear installation,[167] which have been strongly criticised.[168] Stuxnet has been thoroughly studied from all meaningful perspectives.[169] The point I would like to make here is that Stuxnet proved the existence of cyber weapons in hands of states, supposedly. We were told that it was a cyber weapon, because with this piece of code we were able to avoid an airstrike: *"To some degree, this piece of software replaced a squadron of fighter aircraft that would have violated foreign airspace, dropped laser-guided bombs, and left a smoking crater in the Earth's surface."*[170] Stuxnet hit the Iranian nuclear program by implementing a piece of code into their systems causing the fluctuation of nuclear centrifuges spin speeds and thus physical destruction. No reason to lower the seriousness of the attack character, exactly the opposite. We cannot omit the fact that we live in an information age where some kind of conflict related to information is more than possible, but there are voices criticizing linking full-scale war to a targeted sabotage.[171] Stuxnet is a clear example of 21st century precise state sponsored sabotage sending a message to Iran that we do not want to see Iran with a nuclear bomb. Nothing else. However, the Stuxnet attack is ordinarily analyzed along with the Estonia attacks discussed above. The reiteration of alarming discourse production can be seen on making relations between easy-to-conduct attacks such as DDoS, which anyone can buy on the internet – not to mention that the scale we witnessed in Estonia is quite different at least in its orchestrated shape from what we can buy – with extremely sophisticated attacks such as Stuxnet: *"As demonstrated in the preceding paragraphs, cyber tools, like Stuxnet and the wide-scale DDoS attacks on Estonia, have the potential to inflict massive amounts of damage on a state computer network, or even a nuclear reactor."*[172]

The third phase in cyber war discussion turns into the hybrid warfare where information is used to sow distrust. It is true that Arquilla and Ronfeld wrote in their alarmist article back in 1993[173] that the future cyber war will have two forms, cyber war and net war, where the former depicts what Estonia or Stuxnet is about and the latter what the turn into hybrid warfare showed us. Cyber enabled hybrid warfare is about combining all available means to confuse the opponent, sow discord, influence elections and redirect the political development in particular country in the way favourable to the

[165] Based on a personal discussion at the Ministry of Defense of Estonia in Tallinn with Siim Alatalu, 21st Novemebr 2013.

[166] Collins and McCombie, "Stuxnet: The Emergence of a New Cyber Weapon and I."

[167] DW, "Cyber Attacks, Energy Security and Terrorism – A NATO Perspective on Emerging Security Challenges in the 21st Century."

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

[169] Nicoll, "Stuxnet: Targeting Iran's Nuclear Programme"; Nicolas Falliere and Chien, "W32.Stuxnet Dossier"; Collins and McCombie, "Stuxnet: The Emergence of a New Cyber Weapon and I"; Falkenrath, "From Bullets to Megabytes."

[170] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 188–225.

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

[172] Kirsch, "Science Fiction No More: Cyber Warfare And The Uni," 629.

[173] Arquilla and Ronfeldt, "Cyberwar Is Coming!"

attacker.[174] The concept has been also significantly criticised because it is questionable, as in other cyber related events, whether such events should be called *war.*[175] On the other hand, the discussion has changed significantly beginning the hybridization of conflict. As the principal aim is to avoid international law, the discussion whether such an attack constitute use of force diminished. At the same time, states are not taking Russian behaviour in the Western media space lightly and the institutional adaptation has been quite quick.[176]

Cyber war is usually used in exaggerated articles full of threat imaginations, which aim to make short bridges between conventional war and hypothetical cyber war or builds new images of possible future war on which we need to be prepared. Preparation means real activities in order to face imaginations. On the other hand, *cyber warfare* supposes to be used to describe measures, practices, methods or advancement in capabilities concerning using ICT to conduct an attack against an adversary, usually a state if it is used in relation to interstate conflict. There is no doubt that a strong state can possess critical knowledge and capabilities to conduct a specific operation leading to identification of a vulnerability on a critical system, exploit it and even physically destroy it. The Stuxnet event[177] would serve as an example of such capabilities demonstration. However, before discussing what is a threat to national security we should pursue a discursive formation of *cyber war* rather than a discussion of *cyber warfare* or dealing with the described confusion scholars like to multiply. Concerns behind the *radical uncertainty* which might happen is what matters in this discursive analysis. Making such a distinction helps us to avoid criticism that we are denying the existence of tools to conduct a kind of attack which can be credibly called an exercise of tools, measures, practices or methods related to cyber warfare. That brings us to the exact moment where Rid criticizes the usage of the concept *cyber war*, as this is a new kind of activity challenging national security, which is not similar or easily comparable to conventional war, but requires appropriate conceptualization to assess what all possible strategic advantages can be reached by cyber warfare means as the policy practices have changed after every single significant attach, which is not the kind of approach giving us a broad picture about what the novelty in our security environment or put it bluntly is going on in cyber space.

The overall problem of states inclusion to the cyber space related security matters lies mainly on traditional recognition of a state as the most important, most sensitive, most sovereign and most legitimate actor influencing our lives. However, applying the traditional security perspectives on cyber space leave us blind to the critical and constructive analysis of the ongoing events, produce nice but useless concepts such as the *attribution problem* telling us that cyber attack cannot be reliably attributed to a state leaving us in a situation that international law is hardly applicable. States tend to make cyber space important for the sense of a state existence, without such a sense, there will not be a social contract between states and citizens. When it comes to a debatable action, it is understandable that states are the best actors because they possess legitimacy provided by democratic elections. However, as the whole objective of critical security studies is about unveiling hidden intentions of the securitizing actor, we must be aware of the dynamics in which states will tend to deepen their power in cyber space which is not necessarily going to bring citizen better life. Moreover, as cyberspace does not have borders, or at least the technology was designed to spread globally for the practical reasons, identifying any threats as being a threat to national security emanating from a territory of another state and attributing the attack to another state cannot do anything good as such situation necessarily will lead to the escalation. National perspective on cyber space is a trap that will not bring security to any citizens on the planet.

---

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

[175] Caliskan, "A Critique of Hybrid Warfare in the Light of Russia-Ukraine Crisis and Military Strategy."

[176] Mälksoo, "Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of the EU and NATO."

[177] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War."

4.5.2 Intelligence / Law Enforcement

However, at the same time the most pressing cyber related threats that influence our everyday lives do not necessarily need to be attributed to a state but should be prosecuted as a crime. Cyber security is an interesting novel security phenomenon because it shows how a threat properly analysed can be understood as a *threat to a way of life* instead of being a threat *to national security.* If take the former perspective, commonly known as positive security,[178] we can significantly change the way we perceive cyber security. National security perspective is drawing doom scenarios emanating from the imaginations of what other nation states may do, while criminals are making money on a completely naked users browsing the internet and being infected with e.g. ransomware. All law enforcement agencies around the world are putting emphasis on the growing cyber crime that is multiplying every year and that they cannot beat the criminals without unprecedented international cooperation.

The interesting clash can be found between intelligence and law enforcement. While the former tends to defend the national security of a respected state, the latter more focus on the way how people live as law enforcement enforces laws that were adopted in a democratically elected parliament. From the perspective of positive security, it is clear that law enforcement who can stick to activities clearly delimited by law, while state can declare a state of emergency which will provide the actors significant more power and an opportunity to fulfil exceptional acts.

When a group is driven by profit, it is a case for law enforcement. Groups are global, law enforcement agencies are not. As Heather Brooke puts it: *"The hacker community may be small, but it possesses the skills that are driving the global economies of the future."*[179] The hacker community is at least approached as mysteriously powerful with a bright future. You kill one head, and two more grows on that hydra. Sometimes the imaginative national security discourse is reaching an extent that might either cause panic or fascination: *"Cyber hackers are GREATER threat to UK security than nuclear weapons"* which is a title of an article citing *experts on cyber terror.*[180] Hackers and their special capabilities are causing extreme fear based on uncertainty as to what everything else these *lords of cyberspace* can do. As attacks conducted by a state cannot be easily attributable to the particular state, it is understandable that *hackers* are responsible for all the national security concerns emanating from cyberspace.

A map created by the National Security Agency reveals about 600 attacks on corporate, private or governmental targets[181] that had been victims of *Chinese Cyber Espionage*. Despite the huge arguments attributing industrial intelligence to China,[182] one may raise an objection that the attribution of these attacks to China – because they are emanating from the Chinese territory – is not fair as a country consisting of 1,3 billion people simply can house enough profit oriented hackers working for private companies, whose principal objective is profit and nothing more.[183] When it comes to interstate cyber espionage, a great example of that simplified threat depiction is Keith Alexander's famous claim that cyber espionage is the *"greatest transfer of wealth in history",* while it is not difficult to remember decades long US policy about the lawful technology transfer to poor countries, especially to China;[184] or the Snowden revelations, which depict China as a small player to US intelligence efforts, where the "nationalization" of what can be easily be private-to-private espionage is blossoming. Reactions to private-to-private espionage, can insist to call it transnational corporate crime, in shape of sanctions against a state can finally bring the whole nations on dangerously thin ice. These sanctions might in contrary cause more harm to both economies, international stability and thus real espionage

[178] Booth, *Theory of World Security*.

[179] Brooke, "Inside the Secret World of Hackers."

[180] Fielding, "EXCLUSIVE: Cyber Hackers Are GREATER Threat to UK Security than Nuclear Weapons."

[181] Windrem, "Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets."

[182] Puglisi, *Chinese Industrial Espionage*.

[183] Austin, "What the US Gets Wrong About Chinese Cyberespionage."

[184] Austin.

campaigns than ever.[185] Especially when intelligence in order to strengthen national security order services from third parties that participate on massive mammoth surveillance programs as PRISM; post-modern fluid dystopian chaos emerges.

The combination of objectives depicted in The Crypto-Anarchist Manifesto[186] and the sense of the unmanageability of the alleged power of hackers helps draw a pessimistic perspective of possible future actions with limited options of how to cope with them.[187] That is nothing new in cyberspace; however, the fact that cyberspace is a socially constructed space in its fluid shape does not help policymakers approach the problem with a solid perspective. The fluid of unperfect policies are flowing through fingers as any policy approach simply cannot cover each specificity of every single cyber incident combined with constantly deepening technological complexity. So, the reaction is developing an image of environment that is and cannot be not under control; that is where the exceptional politics of continuous and unsolvable insecurities begin. The non-governable technological development, which is moving forward out of control will have implications that noone is even able to imagine. However, everybody is able to draw a solid picture of the threat rhetorically.[188] The Crypto-Anarchist Manifesto[189] drives people in developing technologies that are hard to control by governments and governments draw dystopian images of futures as they are not in charge of such development. One may raise a question as to whether this techno-optimism behind the technology combined with techno-opposition to everything that represents *the establishment* would have emerged without political statements such as the Manifesto. Additionally, the opposite perspective from *the establishment* might be similar. One may raise a question as to whether without the Manifesto states would be so afraid as they are or whether the threat of politics helps them constitute their state-related power on exclusion caused by fear of the unknown[190] and a depiction of deviation.[191] The definition of deviation helps to define the normal state and prepare procedures to react to preserve that normalized state in a normalized way as Aradau and Munster proposes.[192] In that moment, when the desirable policy would be to define the state of the technology society is dependent on, national security authorities are harshly conducting super surveillance programs to catch each anomaly of the deviance from the enormous amount of data that leads to introduction of fantastical concept of *superhuman*[193] above everybody. The policy against catastrophe constructs the catastrophe itself.

The moments that might play a role on deepening the threat perspective on the side of states are certainly not only related to isolated events such as the biggest bank frauds in the history ranging to $1 billion (sub-titled *hunt for the hackers).*[194] Techno-geeks are making political moves that help institutionalization of cyberspace in uncertain ways as they are by principle decentralized; they produce more unknowns in an unknown environment.

4.5.3 The alarmist perspective

"The majority of intrusions we respond to can be attributed to nation-state actors, by nations that condone cyber attacks, or folks in uniform paid by sovereign nations to do intrusions," [195] said Kevin

[185] Pickrell, "A Dangerous Game: Responding to Chinese Cyber Activities."

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

[187] Perrow, *Normal Accidents: Living with High-Risk Technologies*.

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

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

[190] Wodak, *The Politics of Fear*.

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

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

[193] Weathers, "NSA's Massive Cyber-Spying Efforts Called 'Superhuman.'"

[194] Unauthored, "Biggest Cybertheft in History Hits Banks."

[195] Tao, "Nation-State Actors Responsible for Most Cyber Attacks."

Mandia, CEO of US-based cyber security company FireEye. How can he argue this way? Critical security scholars would immediately check who are his clients because this argument is exactly the one that is securitizing cyber space for some hidden intentions. Critical security scholars should not directly criticize because some "may" may fulfil and then the argument would fail. However, at the same time we can argue that his perception, as anyone else, cannot be biased by the direction he perceive cyberspace and companies still need to focus on their profit as a key objective.

Nation-state actors – highly motivated and with 'deep pockets'[196] another statement directly giving states the prime, however, it is hard to compare motivation of a state and successful criminal on the top of virtual cartel selling daily intelligence to nation states.

Some argue that nation-state actors are often the most sophisticated threat actors. That the sophistication can be used as a criterion for attribution.[197] Others argue they are true forces of "cyber soldiers" and agents who have generous budgets, dedicated resources, capabilities and personnel, and are equipped with sophisticated tools and present a high degree of technical expertise, to an unparalleled degree.[198] Some perception to nation states through the securitization discourse use the term *state-sponsored actors*, and in fact, such actors can be generously funded by a government entity. It comes both in the form of money and direction.[199]

Also, unlike some other malevolent actors, some argue that they are characterised by extensive planning and coordination.[200] A common term a 'licence to hack' is used, as they work for governments, i.e. take instructions from government employees, or members of armed forces, usually in order to compromise or disrupt target governments, organisations or individuals. Some also argue that state sponsored actors may also belong to a semi-hidden 'cyber army' or 'hackers for hire' for companies aligned with the goals of a government or dictatorship, which is the kind of attribution through possibilities that deepen the alarmist discourse.

When it comes to nation-state actors' tasks the alarmist discourse builds on arguments that they include gaining access to valuable data, intelligence and secrets from other nations via cyber means. In addition to this, they are often tasked with disrupting other nations, understandably as they are nation states, they wage wars with other nations, thus they must wage cyber wars. The incidents they reportedly create oftentimes have international significance.[201] Using the word "international" is usually used in context of making the case more serious because it crosses (non-existing) borders from a nation and there lie another nation, the implication is that the case becomes international and thus more serious. Nation-state actors are more calculated and measured than other actors because they are probably better organized, and are known to play 'the long-game', which means deploying tactics and attacks granting nation states access to systems and networks quietly; they may apparently hang around for months and years.[202] This is meant probably because nation states must be more sophisticated than organized cartel or decentralized network of hackers sharing hacking tools. It is so, as state-sponsored groups usually carry out attacks simultaneously, even after having already gained

[196] Wilczek, "Cybersicherheit: Hartes Jahr Für Die IT-Security-Teams Der Banken – Und Entwarnung Ist Nicht in Sicht."

[197] Guitton and Korzak, "The Sophistication Criterion for Attribution."

[198] Gargano, "Three Common Threat Actors and the One You Might Not Know About"; Security, "Cyber Threat and Cyber Threat Actors," 2018; Raytheon, "A Field Guide to Hackers"; Bae Systems, "The Nation State Actor Has a 'Licence to Hack' – and They Use It Target Their Adversaries."

[199] Gargano, "Three Common Threat Actors and the One You Might Not Know About."

[200] Williams and Fiddner, *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition*; Raytheon, "A Field Guide to Hackers."

[201] Bae Systems, "The Nation State Actor Has a 'Licence to Hack' – and They Use It Target Their Adversaries."

[202] Gargano, "Three Common Threat Actors and the One You Might Not Know About."

access to the infrastructure in question. Thus, the sensitive data can be collected over a longer time period; there is no need for them to perform a 'smash-and-grab' operation'.[203]

However, such a claim does not work in any other moments where the actors are not state sponsored but paid by state on a black market. That is the moment when one actor blurs over another but in order to make the event more serious any higher sophistication is attributed to a nation state to vindicate exceptional politics. This usually goes to escalation, not necessarily of a conflict but definitely of the volume of perceived seriousness.

The common arguments of alarmist discourse include that the nation-state actors are aware of what they engage in, that they are also aware of the fact that their actions are tacitly supported by their state and thus, they are able to work without fear or legal retribution – it is highly unlikely that their actions will get them arrested in their home country, which understandably make them a threat to another nation state in the national defence strategic perspective. Such a discourse is clearly what has been criticized on neorealist perceptions of strategic concepts including mutual assured destruction.[204] As nation-state actors are generally linked to the military, intelligence or state control apparatus, they are strategic rivals.

What tend to be less alarmist is the argumentation that in some cases, nation-state actors may also be selected for specific skills – whether it be language, social media or cultural ones – in order to engage in propaganda, espionage or disinformation campaigns given their cultural or language capabilities.[205] It is also said that they might influence other malevolent cyberspace actors, as they are usually the first to introduce new tactics, insights and attacks that are subsequently copied by others.

The nation-state actors' motivation can be nationalism and geopolitical issues, however, such an argument can be external in neorealist means as a threat to other nations or internal as a threat to its own liberal order by applying exceptional politics in case of successful securitization of imagined threat from other nation states. Another argument says that unlike other actors, to whom claiming credit can be part of the reward for their efforts, nation-state actors operate under cover and hardly ever acknowledge ownership of their actions. How such argument is different to any other actor in cyber space remains hidden. The zero possibility of attribution is usually used to argue that they may go extreme lengths to cover their tracks, thus making it as hard as possible for cyber security experts to trace their actions back to their country of origin. Again, how is that argument different to any other actors in cyber space remains hidden. They would sometimes even plant 'false flags' in order to mislead the efforts to attribute them.[206]

A typical nation-state actor is a specialist with a remit for specific assignments. Some of them may comprise of everything imaginable which is enough sophisticated to argue that the attack should be attributed to a nation states, these include:

- stealing industrial secrets or classified, sensitive or proprietary information[207]
- disrupting critical national infrastructure,
- listening in on policy discussions,
- taking down companies that leaders are not in favour of,
- conducting propaganda or disinformation campaigns, spreading fake news [208]
- carrying out distributed denial of service attacks (DDoS),
- spreading destructive wiper malware,

---

[203] "Proactive Defense: Understanding the 4 Main Threat Actor Types."

[204] Jervis, "Mutual Assured Destruction."

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

[206] Bae Systems, "The Nation State Actor Has a 'Licence to Hack' – and They Use It Target Their Adversaries."

[207] Raytheon, "A Field Guide to Hackers."

[208] Bae Systems, "The Nation State Actor Has a 'Licence to Hack' – and They Use It Target Their Adversaries."

- conducting cyber reconnaissance of critical infrastructure [209],
- carrying out advanced persistent attacks (APTs) (using continuous, clandestine and sophisticated hacking techniques to gain access to a system and remain inside)[210],

all of the above within or outside the borders of their country.

Bae Systems argue[211] that they are also known to have been employing social engineering in order to target vulnerable or high-profile persons, using carefully crafted spear phishing email messages. Another method employed by the nation-state actors is the so-called 'poisoning the well', i.e. using strategic websites to spread malicious software to their visitors, thus snaring their victims.[212] Social engineering can be used as well. For instance, nation states may create spoof social media profiles or compromise the supply chain of the target organisation, but it can be done by another actor as well, in case of nation states it is considered a national security issue. Furthermore, the nation-state actor, working as an extension of the state security apparatus, may be asked to track, disrupt or persecute activists or dissidents, which is a common activity of any authoritative state, however, it can also be the moment when the liberal democratic nations fall down and begin using authoritative methods. Lastly, some actors can be employed to form armies of trolls aimed at fighting back against unfavourable, controlled or biased media sources, trying to make their employer's reputation grow.

The alarmist discourse commonly argue that the damage those actions cause may be considerable. It can range from foreign nations being disrupted for political gain to targeting the power stations, petrochemical companies and electrical grids, leading to possible physical damage.[213]

Apart from governments, industry bodies, businesses, think tanks, etc. have also been the target of attack; it is said that it happens due to the level of trust they have with participants from business and government organisations.[214] Other targets of high rank (the so-called High-Value targets) cannot be safe, too, some say.[215]

The alarmist discourse goes on and use a language saying that it is clear that that the nature of warfare has changed from physical to online, leading to a deluge of state-sponsored cyber assaults.[216] While it may be believed that cyberspace is becoming more secure, the entrance of nation-state actors has reversed this trajectory. Hence, some argue that cyberspace has been made less secure and heavily contested.[217] Consequently, such said activities of nation-state actors spark controversy. The previous assumptions that nation-state-sponsored APTs are different from cyber-crime threats have been fundamentally flawed. In other words, some people claim the boundary between nation-state and cyber-criminal actors is increasingly becoming blurred.[218]

All in all, according to MI5 Security Service, the nation-state actors are the ones who are 'generally equipped to conduct the most damaging espionage and computer network attacks'.[219] Although recently much has been said about state-sponsored attacks and cyber espionage. State-sponsored attacks are far less common than cyber-crime and hacktivism. Nonetheless, such

[209] Gargano, "Three Common Threat Actors and the One You Might Not Know About."

[210] Kaspersky, "What Is an Advanced Persistent Threat (APT)?"

[211] Bae Systems, "The Nation State Actor Has a 'Licence to Hack' – and They Use It Target Their Adversaries."

[212] Thompson, "DNS Cache Poisoning Part 2."

[213] O'Flaherty, "Cyber Warfare: The Threat From Nation States."

[214] Bae Systems, "The Nation State Actor Has a 'Licence to Hack' – and They Use It Target Their Adversaries."

[215] Sandmeier, "Cybercrime Akteure."

[216] O'Flaherty, "Cyber Warfare: The Threat From Nation States."

[217] Kallberg and Thuraisingham, "State Actors' Offensive Cyberoperations: The Disruptive Power of Systematic Cyberattacks."

[218] Winder, "Boundaries between Nation-State and Criminal Actors More Blurred than Ever."

[219] MI5, "Cyber."

imagination, whether true or false, is still a real and concerning trend in the cyber-political discourse with its implications, which can be proved by the fact that NATO members recognised cyberspace as a fifth domain of operations 'in which NATO must defend itself as effectively as it does in the air, on land, and at sea', as 'nations are increasingly waging war through the Internet.'[220] However, it is almost certain that in the future governments are going to adapt to technological development and nation-states will be powerful actors, asserting themselves in cyberspace.[221] Until this happen, we should consider that we may also live in an imagined reality of possible cyber war that was born by this alarmist discourse.[222]

4.6 Citizens

We decided to add the citizens because we are convinced that if we have to treat cyber space as a space of general human interaction, the most innocent and least malevolent behaviour can be observed in the common citizens. Most people come and use internet for their daily routines, people begin living in cyber space not necessarily in physical means but their daily routines and habits are significantly influenced by the interaction with cyber space.[223]

Nation states exist because their citizens are ready to obey rules of the game laid down by the nation states – the common social contract principle. As Sheila Jasanoff argues, nation states are losing ground by their inability to adapt to the technological development.[224] The principal objective of liberal states is to deliver liberal democratic regime in which people can flourish.[225] To reach that objective, Booth argues that states should not focus on what may happen in order to lower privacy, freedom and thus ingenuity of people living under one political umbrella. States should focus on producing environment that is useful as a ground for further flourishing and named such security policy approach *security plus*.[226] Traditional school in critical security studies has been unveiling *hidden intentions* in the securitization process.[227] This is a process we used generally in comparing the critical and alarmist discourses above where we compared what some say about nation states and their possible capabilities in cyber space while the critical security scholars asks questions where does this discourse come from, what is the motivation behind such alarmist discourse and mainly what is going to be the result of exceptional politics reacting on possibilities. However, such approach is still oriented on state-to-state relations and does not pursue ethically desirable world in which one would necessarily like to live. This has been criticized by the scholars from Aberystwyth university, with Kenneth Booth as the front thinker.

The point is that the traditional critical security studies does not provide us with a guidance what is the proper, desirable or even functional policy because it usually deconstructs the position of a policy maker drawing a possible threat, which would be common defence of anybody supporting the alarmist discourse securitizing everything that may happen. At the same time, such approach also reflects only a policy that is trying to reach a state of the absence of the respected (imagined) threat by adopting effective policy. However, how can we realize that we altered the political reality to avoid the threat from fulfilling? We cannot because we have not even experienced it. This is the problem of terrorism, if society experience a single attack that is amplified by the media coverage, the exceptional

---

[220] "Proactive Defense: Understanding the 4 Main Threat Actor Types"; Eddy, "Cyber Warfare Is Still a Free-for-All"; Schaake, "A Rules-Based Order to Keep the Internet Open and Secure."

[221] Kristin and Sharp, *America's Cyber Future Security and Prosperity in the Information Age Volume Ii*.

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

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

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

[225] Booth, *Theory of World Security*.

[226] Booth, "Security and Emancipation."

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

politics is adopted, next threat may or may not be averted but the society truly changed by cutting general privacy. The orientation point should be a question whether we have made a better world to live. Thus the assessment of ethical consequences in relation to set of values of liberal democracy should be the guidance of liberal democratic nation states when they are adopting particular security policy.

However, what has the recent cyber security practices showed us is exactly the opposite behaviour of liberal democratic states. Edward Snowden may be a hero or a traitor, that does not matter in this analysis, Snowden showed practices liberal democratic states tend to have in order to reach certain level of assumed security by adopting methods that are definitely out of the line from what we would expect from liberal democratic states.[228] The shift that happened in intelligence practices is that we currently moved from high degree of certainty about a small amount of data to high degree of uncertainty about a large amount of data. This move necessarily use data of innocent people that are not involved in any activity related to (assumed) national security. The fact that Snowden revealed such practices led to a situation in which citizens of involved liberal democratic lowered their belief into the values and ideology of liberal democracy. You cannot defend principles that you do not use in such defence. We can clearly link Snowden revelations to the time during which populist movements surged elections in Europe, which is also nourished by the propaganda activities by Russia, however, which also target mainly the authorities of the liberal democratic states in order to lower confidence of their citizens in their governments and liberal democratic regime[229] in general, drawing it as hypocritic.

Adding citizens into the nexus of cyber space actors should be perceive mainly as the central orientation of the desirable policy aiming to secure cyber space. As we argue throughout the text, securing cyber space from an imagined threat of nation states by adopting military discourse interpreting similar possibilities in cyber space to conventional war that may or may not happen does not reflect the principal ethical condition of policy – to build a better world. However, it does omit the distribution of power of all actors which is important to even deploy effectively any policy and finally it does not reflect the fact that the absence of a threat is not necessarily the desirable outcome of the adopted policy.

Citizens will follow what will make their lives better and failed securitization of possible cyber threats will only empower other actors in cyber space because citizens will use their liberation tools to avoid state surveillance, to avoid finally any probes states need to tackle cyber crime to fulfil its principal role in securing citizen where the empirical proof of growing cyber-crime is clear. Cyber space turned the concept of national security upside down and the strategy of securitization of possible threats will not give back power to states because the key power – in the principle of social contract – lies in authority, in fact that citizens are pliable to obey rules of the sovereign.

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

[229] Pomerantsev and Weiss, "The Menace of Unreality : How the Kremlin Weaponizes Information , Culture and Money"; Lucas and Pomerantsev, *Defending and Ultimately Defeating Russia's Disinformation Techniques. Recommendatins. A Report by CEPA's Information Warfare Project in Partnership with the Legatum Institute*; Schmidt, "Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War."

4.7 Cyber terrorists

„What is required today is a sense that individually, we need to secure ourselves first, then rely on others for security. We should not assume that we live in a protected American cyber enclave; cyberterrorism must be treated as a threat equal to that of weapons of mass destruction, and given the same priority attention." [230]

Given the relatively stable international order of democratic states, terrorism has become a central issue of international security. However, the current apocalyptic wave of terrorism is by some understood as the fourth wave of terrorism [231], so it should not be perceived as a fully novel phenomenon. The cyber enabled terrorism is more a construction of policy makers' imaginations because until today we do not have a single attack that can be considered as a pure cyber terrorist attack.

However, as the communication technology enables actions with physical implications where territory and time does not matter, it is understandable that given the apocalyptic terrorist attacks we have been witnessing since 9/11, cyberterrorism has become a contested word. Its proponents are drawing doom scenarios while its critics are arguing that not a single attack happened and thus there is no legitimacy for exceptional political decisions. The alarmist discourse perceives these new technological possibilities as a real phenomenon, a newest manifestation of terrorism and thus created a new term for it – cyberterrorism. The term was probably coined in 1997 by Mark Pollitt, who defined it as 'the premeditated politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by sub-national groups and clandestine agents'. [232] It is necessary to said that we have not yet reach the point of a consensus over the term "terrorism". We can easily find dozens, up to two hundreds of seriously discussed definitions. We can find a flow of different perceptions of what terrorism is for state actors[233]. Thus, any application of this ungraspable phenomenon to comparably fluid and ungraspable cyberspace cannot lead to a solid description of cyberterrorism without exaggerating possible future threats.

It is important to mention here that cyber terrorism as a term has a performative character as it does not describe the world but effectively transforms social reality.[234] Traditional perception of security as known from strategic studies focuses on physical security from military power. Thus since telecommunication infrastructure has become crucial for national security and consists of physical wires, the imagination that a geek-driven hacking of critical systems can cause doom scenario has been tacitly received without single empirical evidence. The empirical evidence is not necessary for the term to have practical impact on the social world, politics, foreign policy and thus international security. However, the source of the disturbance is more the imagination of a possible threat rather than the threat itself.

4.7.1 The alarmist perception of cyber terrorism

Generally speaking, from the alarmist perspective, cyberterrorism may be conducted by either state or non-state actors. The state-sponsored cyberterrorism may be conducted in order to achieve goals established by the state's political leadership. State-sponsored cyber attacks, if one manages to trace back and attribute them to their network source, may allow determining the physical location of the perpetrators, within the boundaries of the state that commissioned the assault. In comparison to

[230] Anonymous, "Cyberterrorism: The Invisible Threat Stealth Cyber Predators in a Climate of Escalating Risk."

[231] Rappaport, "The Four Waves of Rebel Terror and September 11."

[232] Dziundziuk, "Stopping Cyber Terror Countries Must Work Together to Thwart Efforts of Internet Criminals."

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

[234] Balzacq, Léonard, and Ruzicka, "'Securitization' Revisited: Theory and Cases."

non-state actors, the likelihood of identifying those responsible for attacks is increased. An example would be the uncovering of the state sponsored group APT41 probably falling under the Chinese military, however, exactly this group shows that even China might have significant troubles to keep them under control making their operatives a common geeks with unmeasurable power. [235]

On the other hand, non-state terrorist organizations do not have to work in a uniform way. They are often motivated by ideologies that embrace martyrdom or present apocalyptic visions, either based on religion or a wish to overthrow a government. Thus, it is understandable that just a mere declaration by a terrorist organization of hiring a hacker can cause imaginations of their possible cyber terrorist capabilities because, as some argue, we cannot prove it or deny it.[236] The problem is also in the 9/11 attacks character. One would say that we have been caught in surprise, others will argue on the basis of post-attack investigation that the failure was in the communication of intelligence agencies. Such a situation leads to moments that academics are looking for traditional strategic concepts to understand cyber related threats and argue whether we can deter cyber terrorism or not and argue that even the most aggressive organisations seem to be functioning in a strategic and rational way.[237] Besides, the majority of terrorist attacks are not carried out for the purpose of monetary gain[238], the perception of possible cyber terrorist threat as national security issue is understandable as that reaction comes from state structures prepared to face terrorism. Some assessments argue that terrorist groups are usually at the lowest level of sophistication, relying on widely available tools that require little technical skill to deploy, similarly to hacktivists.[239] Whether this sophistication can change or not is reserved to our imaginations

Dziundziuk identifies three kinds of cyberterrorism: [240]

- Ordering terrorist acts using computers and computer networks; terrorism at its 'purest',
- Using cyberspace for terrorist groups' sake, but not directly; to commission the acts of terrorism and manage their activities,
- Commissioning acts in cyberspace that do not facilitate political aims; they present a threat to public or national security, though.

Taking those into consideration, one may redefine cyberterrorism as an intentional, politically motivated attack on information, a computer system, or a network, that jeopardizes the life and well-being of citizens. It can involve other disastrous consequences, including disrupting public safety, intimidating the population or government authorities or even provoking a military conflict. [241] So, it can be stated that in order to qualify as cyberterrorism, an attack ought to lead to violence against a person or property, to foment terror and demoralisation, or at least generate fear, or change domestic national or international events. This may be achieved e.g. by causing death or bodily injury, explosions, economic loss, extended power outages, airplane crashes, water contamination etc. There are acts and policies that link cyberterrorism to even more actions, such as disrupting (tele) communication infrastructure, banking or financial services, transportation, etc. [242][243] [244] Depending

[235] Murphy and Murgia, "Chinese Hacker Group That Works for Both Beijing and Personal Gain Identified."

[236] Wiemann, "Cyberterrorism: How Real Is the Threat?"

[237] Klein, "Deterring and Dissuading Cyberterrorism."

[238] Ahmad and Yunos, "A Dynamic Cyber Terrorism Framework."

[239] Security, "Cyber Threat and Cyber Threat Actors," 2018.

[240] Dziundziuk, "Stopping Cyber Terror Countries Must Work Together to Thwart Efforts of Internet Criminals."

[241] Dziundziuk.

[242] Ahmad and Yunos, "A Dynamic Cyber Terrorism Framework."

[243] Beggs, "Cyber-Terrorism in Australia."

[244] Mshvidobadze, "State-Sponsored Cyber Terrorism: Georgia's Experience."

on their impact, vicious attacks against critical infrastructures could be perceived as acts of cyberterrorism, too. If they disrupt non-essential services or are generally a costly nuisance, they are not cyberterrorism, though. [245] [246]

Cyberterrorists wish to maintain a permanent state of fear, in order to achieve their goals of any nature, or to just draw attention to an individual cyberterrorist or a terrorist organization. Thus, causing harm or threatening to cause it is a kind of warning that there exists the possibility of more catastrophic consequences should the cyberterrorists' conditions are not met. As regards the second kind of cyberterrorism, some scientists disagree whether using cyberspace by terrorist organization in order to carry out or make their activities public (but not to commit terrorist acts directly) is, in fact, cyberterrorism, as such actions can hardly be qualified as terrorism under criminal law.

Nonetheless, this kind of actions may be the sign of terrorist acts committed in the near future. They include using the Internet to:

- Collect data on possible targets, their location and characteristics.
- Make websites about terrorist movements, as well as their aims and purposes, giving information to people interested in supporting terrorists, etc.
- Address mass audiences to report on planned or future actions, using websites or mass e-mailing, also including claiming responsibility for the commission of terrorist acts. With the rise of social media platforms, it is now quick and simple to find support for almost any group or idea, including terrorism. [247] [248]
- Initiate the 'psychological terrorism', for informational or psychological effect, e.g. by sowing panic, misleading, spreading rumours, etc.
- Raise funds to support terrorist movements,
- Extort money from institutions and organizations, either to spare them from cyberterrorism acts or damaging their reputation.
- Draw (generally unsuspecting) accomplices into terrorist networks; people like hackers who are unaware of where their actions might ultimately lead.
- Set up websites that contain information about explosives, explosive devices, toxins, gases, etc. and how to produce them, addressed to terrorists,
- Send encoded messages (using e-mail, message boards, etc.) and communicate,
- Relocate training bases for terrorist operations, as they are no longer located within the target countries, nor confined to the territory in which the terrorists are hiding.

As regards the third kind of cyberterrorism, the actions may not even be committed by terrorists themselves. They may be performed by delinquents and vandals with no political objectives. However, they pose a considerable threat to public or national security, so they may be regarded as terrorism. These actions may include spreading viruses, 'Trojan horses', 'worms' and the like in an intentional way, paralyzing the operation of government or other institutions by intrusion, etc. [249]

Klein argues that, although cyberterrorism has been written about since the early 2000s, is still not fully understood as a strategic concept. It is also questioned whether such actions can be deterred; there are strategists and policy-makers who argue that some cyberterrorism acts may prove to be undeterrable. [250]

---

[245] Denning, "Cyberterrorism Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives."

[246] Klein, "Deterring and Dissuading Cyberterrorism."

[247] Bieda and Halawi, "Cyberspace: A Venue for Terrorism."

[248] Dziundziuk, "Stopping Cyber Terror Countries Must Work Together to Thwart Efforts of Internet Criminals."

[249] Dziundziuk.

[250] Klein, "Deterring and Dissuading Cyberterrorism."

Terrorists resort to the Internet as the cyber domain has several advantages, because it:

- is far cheaper than traditional methods; instead of guns and explosives one needs a computer and access to the Internet,
- is more anonymous than traditional methods, more difficult to track down and identify the perpetrators,
- can be conducted remotely, and
- the range of potential targets is infinitely greater than with traditional, kinetic actions. [251]

However, there is an ongoing discussion on several aspects of cyberterrorism. Firstly, the media are blamed for blurring the concept by confusing/misusing the terms 'hacker' and 'cyberterrorist'. Terrorism is a form of crime, but not every crime is terrorism; thus not every hacker is a terrorist. [252] The media are also accused of portraying not what cyberterrorism is, but what it could be: 'terrorists crafting digital attacks to take down traffic lights, make trains stop on a dime, and water pipes burst'. [253]

This relates to another controversy: it is difficult to believe, but according to many authors, to date, no such dramatic events have occurred; no single instance of real cyberterrorism on public facilities and systems has been recorded [254] [255] Naturally, the attacks on critical components do happen, but so far have not been carried out in a way to result in the damage that could classify as cyberterrorism. What is more, it is commonly believed that the potential threat of cyberterrorism is alarming, due to our reliance on electronic networking having expanded to a significant degree. [256] Thus, if, e.g. an attack on the emergency services system had coincided with a planned, real-world event, 'a Cyber Pearl Harbor' event may be an appropriate metaphor. [257] Despite this fact, many experts on computer security claim using the Internet to cause damage, injury or death on a large scale is not attainable. [258] It has even been argued that cyberterrorism does not exist and the so-called cyberterrorists are, in fact, 'ordinary' hackers. [259] Indisputably though, it has been confirmed that some terrorist organisations do use the Internet; but instead of conducting attacks via the web, they employ it mostly for communication, recruitment, fundraising and coordination of future attacks.

Finally, there is a heated argument that the use of social media by terrorist groups create a grey area between freedom of speech and crime and governments are struggling to decide how to tackle this issue within established, constitutional frameworks. [260] All in all, cyberterrorism has been an emotionally charged issue; it cannot be ignored and needs a proactive response and strategic preparedness. [261] [262]

---

[251] Klein.

[252] Dziundziuk, "Stopping Cyber Terror Countries Must Work Together to Thwart Efforts of Internet Criminals."

[253] Ablon, "The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data: Hearings before the Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, United States House, 115th Cong. 1."

[254] Ablon.

[255] Klein, "Deterring and Dissuading Cyberterrorism."

[256] Bieda and Halawi, "Cyberspace: A Venue for Terrorism."

[257] Theohary and Rollins, "Cyberwarfare and Cyberterrorism: In Brief."

[258] Klein, "Deterring and Dissuading Cyberterrorism."

[259] Sigholm, "Non-State Actors in Cyberspace Operations."

[260] Goldman, "Terrorism 2.0? New Challenges in Cyberspace."

[261] Klein, "Deterring and Dissuading Cyberterrorism."

[262] Anonymous, "Cyberterrorism: The Invisible Threat Stealth Cyber Predators in a Climate of Escalating Risk."

4.7.2 The critical perception of cyber terrorism

Critical scholars have been active since the term cyber terrorism has made its way to the general political discourse in cyber security. Cyber terrorism finally does not describe anything else than a mere possibility of a lone wolf or an organized network to conduct an attack comparable to conventional terrorist attacks. As we do not know how many attacks have been prevented by the intelligence. The same can be easily said to cyber terrorism if intelligence is equipped by a cyber team assumedly capable to stop possible cyber terrorist attack.

Critical scholars usually focus on the securitization language and how it is used. For example, Myriam Dunn Cavelty begins her critical article by citing National Academies Press publication saying: "We are at risk. Increasingly, America depends on computers… Tomorrow's terrorist may be able to do more damage with a key- board than with a bomb."[263] Cavelty argues that the logic of thinking is not binary but probabilistic. In order to reach a desirable state of security, critical scholars are arguing that we should not intentionally securitize probabilities but rather desecuritize them[264] and focus on threats that has empirical basis (cyber crime) or objectively perceivable characteristics (asteroid).

4.8 Artificial Intelligence

Artificial intelligence (AI) can be used for various tasks that are necessary especially in analysis of vast amount of data. AI can be used for learning during such analyses but at the same time AI can learn from the human behaviour. The common problem with AI is that the cloud of knowledge AI is creating during the deep learning processes usually stay hidden to the operator. The way how such cloud is saved is comprehensible to the AI only. However, there is no other way to analyse for example data packets coming to the router for some suspicious patterns, it is finally only method using AI that can be successful and patient enough to keep the analysis going constantly. AI can be also used for lowering complexity of the problem for the operator but at the same time it is AI which is making the decision what is in such process more or less important for the operator. The classical ethical problem arises when we decide to let AI make a decision whether to act against assumed attack or not, if we do so, who is responsible for the result? This can look as a banal question, however, when such decision is made on behalf of a nation state, the question is then translated to the discussion over state responsibility according to the international law.

DARPA has decided a couple of years ago[265] to fund a challenge in which teams competed in AI development that will be capable to patch vulnerabilities in software. There are also viruses online that already change their shape and code according to the interaction they experience to lower the probability to be detected.[266] Development of comparable tools that will alter the cyber space autonomously can lead to real dystopian futures rather than being a tool for our security.

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[267] 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.* [268] Thus the implications

[263] National Academy of Sciences (NAS), *Computer Science and Telecommunications Board: Computers at Risk: Safe Computing in the Information Age*.

[264] Waever, *Securitization and Desecuritization*.

[265] DARPA, "Cyber Grand Challenge."

[266] Kaspersky Lab, "What Is Metamorphic Virus?"

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

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

are not inevitable, they are constructed. Nonetheless, ideas that artificial intelligence can be used in automated defense against cyber-attacks has been forming recently.[269] 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, from geeks to artificial intelligence.

5. International law perspective

5.1 Malicious cyber activities in the context of international law: Actors

According to the World Economic Forum, cyber-attacks are a growing concern as the regional (and global) economy becomes more sophisticated and interconnected.[270] The combination of connectivity, mobility and data present almost boundless opportunities for hackers with a wide range of motives and tools. Thus, the need to effectively address the complexity associated with operating in cyberspace became one of the greatest challenges of our time. Today, cyber security is an important topic and a day-to-day struggle for both national governments and individuals.

Cyberspace is described as a 'global domain' lacking physicality and is virtual in nature.[271] Transboundary nature of cyberspace implies the relevance of international law. However, the absence of territorial borders in cyberspace makes an application of international law, build on traditional conceptions of territoriality and sovereignty (the Westphalian model of sovereignty), very challenging. Thus, this chapter seeks to explore the multifaced international law challenges faced by various actors in cyberspace.

A leading effort to develop shared understanding on how international law applies in cyberspace is *The Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* (the Manual).[272] Sponsored and produced under the auspices of the North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence, the Manual reflects the personal assessments of a group of international law specialists drawn from a wide variety of regions and legal traditions.[273] Moreover, cyberthreats have been increasingly analysed and discussed by the United Nations. Its resolutions as well as reports from various UN bodies represent a valuable source of information for better understanding of state's positions and interests.[274]

Despite the fact that cyber technologies develop at an unprecedented pace, cyber space must never be a lawless world. On the contrary, it should be an integral part of the rules based international order. When states and individuals engage in hostile cyber operations, they are governed by law just like activities in any other domain.[275] In this context states, as authors and subjects of international

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

[270] Dusek and Collins, "Regional Risks for Doing Business 2018."

[271] Schmitt, "Sovereignty."

[272] Schmitt, "Tallinn Man. 2.0 Int. Law Appl. to Cyber Oper."

[273] Koenders, "Foreword."

[274] Since 2004, five Groups of Governmental Experts have continued to study the threats posed by the use of ICTs in the context of international security and how these threats should be addressed. Three of these Groups have agreed on substantive reports with conclusions and recommendations that have been welcomed by all UN Member States. See United Nations Office for Disarmament Affairs, Developments in the field of information and telecommunications in the context of international security. More http://www.un.org/disarmament/ict-security

[275] Wright, "Cyber and International Law in the 21st Century (Speech)."

law, play an indispensable role. One of the greatest challenges for states is to ensure that international law keeps pace with evolving technologies.

With regard to individuals, their dependence on the internet is growing faster than their ability to forestall attacks. According to Edward Lucas, processing power, memory and connectivity have become astonishingly cheap and even the poorest people can aspire to send and receive data. However, the same features make the internet and consequently its users significantly vulnerable.[276] In this context, the UN General Assembly has emphasized that enhanced capabilities of governments, companies and individuals to undertake surveillance, interception and data collection, may violate or abuse human right, especially the rights to privacy and to freedom of expression and may contradict the tenets of a democratic society.[277]

Moreover, an identification of those responsible for hostile cyber activities due to blurring of the line between state actors and private individuals and entities in cyberspace remains one of the greatest challenges. There are practical difficulties involved in making any attributions of responsibilities because cyber operations are not limited by traditional territorial boundaries. It is worth mentioning that malicious cyber operations conducted by states are governed by different legal regime than malicious cyber operations conducted by non-state actors.

5.2 States

Since states are both authors and subjects of international law, they play an indispensable role in ensuring that international law keeps pace with evolving technologies. In particular, states can exercise their sovereignty and use various diplomatic tools and instruments of international law in order to effectively address transboundary nature of cybersecurity. Especially treaties, regimes and institutions are a way to better secure cyberspace and to make international law adequately adapted to the cyber realm.

Within their own jurisdiction, determined by national borders (with some exception), states have ultimate authority in the decision-making process and in the maintenance of order. In other words, a state is free to adopt any measure it considers necessary or appropriate as long as the adoption of such measure is compatible with state's international obligations.[278]

However, in their response to extraterritorial cyberthreats, states are significantly limited by the concept of state sovereignty.[279] The principle of state sovereignty can be traced to the Peace of Westphalia and constitutes the cornerstone of the UN Charter. Article 2 of the UN Charter reads as follows: "*The Organization is based on the principle of the sovereign equality of all its Members*" and "*Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state (…)".* The principle of sovereignty is further developed in the Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations. The declaration reiterates that no state has the right to intervene directly or indirectly in the internal or external affairs of any other state (the principle concerning the duty not to intervene in matters within the domestic jurisdiction of any state) and all states enjoy sovereign equality (the principle of sovereign equality of states).[280]

---

[276] Lucas, "Why We Are Not Ready for Cyberwar."

[277] United Nation General Assembly resolution 68/168, The right to privacy in the digital age, A/RES/68/167 (18 December 2013).

[278] Schmitt, "Sovereignty."

[279] Simma et al, *The Charter of The United Nations 3E, Vol 1*.

[280] United Nation General Assembly resolution 2625 (XXV), Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, A/RES/2625 (XXV), (24 October 1970).

5.2.1 External and internal dimension of state sovereignty

Internal dimension of state sovereignty is traditionally understood as an ultimate power within the state's territory and in its internal affairs. In principle, a state is free to adopt any measure it considers necessary or appropriate as long as the adoption of such measure is compatible with state's international obligations.[281] The Permanent Court of International Justice in the Lotus case, held that "*the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention*".[282] The principle concerning the duty not to intervene in matters within the domestic jurisdiction of any state is of particular relevance for this chapter, because it does significantly limit states in responding to malicious cyber operations having origins in other states.[283]

External sovereignty captures the relation of independence of sovereign States outside their national boundaries and their equal rights in their mutual relations. External sovereignty serves as a legal basis to enter into international agreements and affect matters located beyond their national jurisdiction. However, states, exercising their sovereignty, are only bound by those rules of law which they had agreed, either by the conclusions of treaties or customarily.[284] In other words, an act of a foreign state could only have a legal effect in another state, if it had been recognized by that latter state.[285] In other words, international law is built on a foundation of state consent.[286] However, according to Prof. Guzman, while consent protects the interests of states and supports notions of sovereign equality, it functions as a barrier to effective cooperation in a world of vastly divergent priorities and concerns, often frustrating attempts to solve global problems.[287]

Given the nature of potentially transboundary nature of malicious cyber activities, the principle of state sovereignty may rise significant legal questions. Especially, how territoriality operates in the interconnected ream of cyberspace has proved to be enormously contentious.[288] Therefore, Prof. Schmitt expects states to clarify their position on sovereignty in cyberspace and parts of the Manual dedicated to state sovereignty are most likely to be changed in the next five years.[289] Brian Egan, the former Legal Advisor of the U.S. Department of State, also argues that sates should publicly state their views on how existing international law applies to State conduct in cyberspace to the greatest extent possible.[290]

Addressing the tensions between the concept of state sovereignty and the transboundary nature of cyber space, authors of the Manual argued that the physical,[291] logical,[292] and social[293] layers of

[281] Schmitt, "Sovereignty."

[282] PCIJ, S.S. Lotus (Fr. v. Turk.).

[283] Besson, "Sovereignty."

[284] Simma et al, *The Charter of The United Nations 3E, Vol 1*.

[285] Simma et al.

[286] Guzman, "The Consent Problem in International Law Permalink"; International Court of Justice, "Case Concerning the Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain), Judgment of 5 February 1970"; ICJ, Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits; PCIJ, S.S. Lotus (Fr. v. Turk.).

[287] Guzman, "The Consent Problem in International Law Permalink."

[288] Watts and Richard, "Baseline Territorial Sovereignty and Cyberspace."

[289] Jensen, "The Tallinn Manual 2.0: Highlights and Inisghts."

[290] Egan, "International Law and Stability in Cyberspace."

[291] For instance, physical network components (i.e., hard- ware and other infrastructure, such as cables, routers, servers, and computers). See Schmitt, "Sovereignty."

[292] For instance, connections that exist between network devices, including applications, data, and protocols that allow the exchange of data across the physical layer. See Schmitt.

cyberspace are encompassed in the principle of sovereignty. Rule 2 of the Manual stipulates that state enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory. With respect to cyber infrastructure, it does easily fit with a notion of sovereignty confined within territorial borders. According to the Manual, "the fact that cyber infrastructure located in a given State's territory is linked to cyberspace cannot be interpreted as a waiver of its sovereignty".[294] However, cyber security can be hardly limited only to the infrastructure. Thus, the Manual addresses the logical and social layer of cyberspace as well. Internal sovereignty provides states with the right to regulate cyber activities such as e-services, communications between web services and browsers, and to criminalize certain online activities (for instance, child pornography). Moreover, states can restrict access to cyberspace (for instance, blocking of access to terrorist content on social medias).[295]

Whereas states exercise supreme control over their internal affairs, externally they are limited by sovereignty of other states. This limitation is reflected by Rule 4 of the Manual: "A state must not conduct cyber operations that violate the sovereignty of another state."[296] However, the obligation to respect sovereignty of other states may significantly affect capabilities of states to respond to cyber threats. Therefore, states, exercising their external dimension of sovereignty, should use both diplomacy and instruments of international law to create an international legal environment addressing abovementioned inability of the current regime to cope with transboundary cyber threats.

5.2.2 State as a target of malicious cyber activity

Since states enjoy sovereign authority with regard to the cyber infrastructure, persons and cyber activities located within their territory, any malicious cyber activity having purely national character (conducted by non-state actors whose operations are not attributable to other states) are to be addressed by national law. Domestic actors conducting "domestic" malicious cyber activities will fall under the law enforcement regime – criminal or administrative law.

However, open, transnational and decentralized nature of the internet enables various actors to conduct malicious cyber activities from the territory of other states. In addition, malicious cyber activities may originate from a state or non-state actor.

5.2.2.1 A malicious cyber activity originates from a state or its attributable to a state: Violation of sovereignty, prohibition of intervention and use of force

Since no state has the right to intervene into the internal affairs of another state, a malicious cyber activity conducted by a state (or a non-state actor attributed to a state) may constitute a violation of state sovereignty. However, it should be emphasized that the principle of non-intervention into internal affairs applies only to the relations between states. In other words, only states are obliged to respect sovereignty of other states. A malicious cyber activity can violate state sovereignty only when it conducted by a state or it is attributable to a state.

The Manual provides the following example: "If an agent of one State uses a USB flash drive to introduce malware into cyber infrastructure located in another State, a violation of sovereignty has taken place."[297] According to Garry P. Corn and Robert Taylor, there are differences in how sovereignty is reflected in international law with respect to specific domains. For instance, in the case of the air domain, in any unconsented entry into the airspace of another state constitutes a serious violation of international law. On the other hand, repeated entries into and transit trough the territorial waters of another state are permissible. The authors conclude that dramatically different

[293] Understood as a social layer encompassing individuals and groups engaged in cyber activities. See Schmitt.

[294] Schmitt.

[295] Schmitt.

[296] Schmitt.

[297] Tallinn str. 19.

regimes underscore a clear understanding and application of the sovereignty principle.[298] In the context of cyberspace, it is questionable whether any cyber operation constitutes a violation of state's sovereignty. Prof. Schmitt argues that only remote operations that manifest on a state' s territory should be considered as a violation of state's sovereignty.[299] An assessment of the lawfulness should take into consideration the degree of infringement upon the target state's territorial integrity and whether there has been an interference with or usurpation of inherently governmental functions.[300]

In addition, based on the international law principle of sovereignty, states are prohibited from coercive intervention, whether through the use of force or not, into another State's *domaine reserve*. This principle has been understood to be fully applicable to cyberspace. Rule 66 of the Manual states: "a state may not intervene, including by cyber means, in the internal or external affairs of another state".[301] According to the Oxford Public International Law, the prohibition of intervention is a principle of customary international law codified under Art .2 (4) and (7) of the UN Charter and often recognized by the ICJ's decisions.[302] The prohibition of intervention is understood as a corollary of every state's right to sovereignty, territorial integrity and political independence.[303] State's *domaine réservé*, referrers to the "choice of a political, economic, social, and cultural system, and the formulation of foreign policy.[304]

Article 2(4) of the United Nations Charter provides that: "*All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations*." Thus, in the context of cyberspace, a malicious cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any state is unlawful.[305] The prohibition has been recognized as a norm of customary international law.[306] The UN Charter offers no criteria by which to determine when an act amounts to a use of force, however, the International Court of Justice held that a use of force need not involve the employment of military or other armed forces by the state in question. For instance, training a guerrilla force that is engaged in hostilities against another state qualified as a use of force.[307]

Taking into consideration specific nature of cyber operations, the authors of the Manual suggest following qualitative elements of a particular cyber operation to be assessed when deciding whether to characterise a cyber operation, as a use of force: *severity* (How many people were killed? How large an area was attacked? How much damage was done within this area?), *immediacy* (How soon were the effects of the cyber operation felt? How quickly did its effects abate?), *directness* (Was the action the proximate cause of the effects? Were there contributing causes giving rise to those effects?), *invasiveness* (Did the action involve penetrating a cyber network intended to be secure? Was the locus of the action within the target country?), *measurability of effects* (How can the effects of the action be quantified? Are the effects of the action distinct from the results of parallel or competing actions? How certain is the calculation of the effects?), *military character* (Did the military conduct the cyber

[298] Corn and Taylor, "Sovereignty in the Age of Cyber."

[299] This conclusion is supported by the European Court of Human Rights. See ECHR, Decision on admissibility delivered by a Chamber Weber and Saravia v. Germany (dec.), no. 54934/00, 2006.

[300] Schmitt, "Sovereignty."

[301] Schmitt, "Prohibition of Intervention."

[302] Besson, "Sovereignty."

[303] Jennings and Watts, *Oppenheim's International Law : Volume 1 Peace*.

[304] ICJ, Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits.

[305] See Rule 68 on Prohibition of threat or use of force. More: Schmitt, "The Use of Force."

[306] ICJ, Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits.

[307] ICJ.

operation? Were the armed forces the target of the cyber operation?), *state involvement* (Is the State directly or indirectly involved in the act in question? But for the acting State's sake, would the action have occurred?), *presumptive legality* (Has this category of action been generally characterised as a use of force, or characterised as one that is not? Are the means qualitatively similar to others presumed legitimate under international law?).[308]

5.2.2.2 Attribution

An accessibility of cyber technologies resulted in blurring of the line between state actors and private individuals and entities in cyberspace. An attribution of responsibilities when the action concerned is capable of crossing traditional territorial boundaries and sophisticated techniques are used to hide the identity and source of the operation is particularly difficult.[309]

The question of attribution has been addressed by the International Law Commission. In 2011, it adopted the Articles on State Responsibility for International Wrongful Acts reflecting customary international law on state responsibility.

Assuming applicability of the customary law of state responsibility applies to cyber activities, a state bears international responsibility for a cyber-related act that is attributable to the state and that constitutes a breach of an international legal obligation. Pursuant to the Articles on State Responsibility for International Wrongful Acts, following conduct shall be considered an act of that state under international law: a) conduct of organs of a state, b) conduct of persons or entities exercising elements of governmental authority, c) conduct of organs placed at the disposal of a state by another, d) conduct of organs placed a the disposal of a state by another state, e) conduct directed or controlled by a state (acting on the instruction of, or under the direction or control of, that state in carrying out the conduct).[310]

With regard to cyberspace, there was complete agreement among authors of the Manual that the customary law of state responsibility applies to cyber activities.[311] However, the Articles on State Responsibility for International Wrongful Acts do not address specific nature of cyberspace and it remains unclear how to deal with an "anonymity" in that the authors of cyber operations can hide their identity, the possibility of multi-stage action that computes operated by different persons and places in different jurisdictions can be used, and the speed with which operations can take place.[312]

5.2.2.3 A malicious cyber activity originates from a non-state actor: Due Diligence

International law governs primarily relations between sovereign states and, thus, a malicious cyber activity conducted by a non-state actor cannot violate state's sovereignty (if the conduct in question is not attributable to the state). Since states are obliged to respect state sovereignty of other states, non-state actors can be stopped from causing harm only by the state enjoying sovereignty with regard to particular malicious cyber activities. The key questions in this context is, whether a state is obliged to exercise due diligence in not allowing its territory under its governmental control to be used for cyber operations that produce adverse consequences for other states.[313]

Authors of the Manual argue that the due diligence principle is reflected in the rules, and interpretation thereof, of numerous specialised regimes of international law, such as international

---

[308] Schmitt, "The Use of Force."

[309] Wright, "Cyber and International Law in the 21st Century (Speech)."

[310] Interntional Law Commission, Text of the draft articles on Responsibility of States for internationally wrongful acts as part of the International Law Commission Report, A/56/10 August 2001.

[311] Jensen, "The Tallinn Manual 2.0: Highlights and Inisghts."

[312] Buchan, Roscini, and Tsagourias, "State Responsibility for Cyber Operations: International Law Issues Event Report."

[313] Shackelford et al., "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors."

human rights law, international environmental law, international investment law.[314] They also quote the International Court of Justice's judgment Corfu Channel, which observed that '*it is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States*'.[315]

Hence, the authors of the Manual concluded that once the territorial state acquires knowledge of the fact that its territory is being used for a malicious cyber activity causing serious adverse consequences for another state, the former must take all reasonably available measures to stop that cyber operation. However, the precise scope of action required by the due diligence principle remains unclear. By contrast, as Prof. Jensen points out,[316] according to the United Nations Group of Governmental Experts (UN GGE), states were only willing to admit that they "should" exercise due diligence, rather than that they "must" as the Rule 6 of the Manual states.[317]

The international community should focus on further development of the due diligence principle, especially its exact scope in order to prevent state sovereignty to server as a shield for malicious cyber operations.

5.2.3 External dimension of state sovereignty: International cooperation in law enforcement

The core problems encountered in the attempted prosecutions of international cyber criminals encompass: lack of criminal statutes, lack of procedural powers and lack of enforceable mutual assistance provisions.[318] First, the principle of *nullum crimen sine lege* requires that a person may only be found guilty of a crime in respect of acts which constituted a crime at the time of their commission.[319] Thus, the fight against cybercrime requires adoption of effective substantive criminal legislations addressing specific nature of cyberspace. Second, states often lack the resources and procedural tools necessary to effectively cope with cyber criminality.[320] Third, prosecution of cybercrimes is often frustrated by a lack of enforceable cooperation between state.[321]

Domestic laws are generally confined to a specific territory and, thus, not adequately equipped to address transnational/transborder crimes. In response to these difficulties, states tend to cooperate in matters having transnational character.[322] International cooperation in the investigation and prosecution aims at overcoming difficulties typical for investigation or criminal proceedings against persons suspected or participating in criminal activities when such persons are outside their territory or where key evidence, witnesses, victims are located outside the country's jurisdiction.[323] Since malicious cyber activities are often of transnational character, enhanced international cooperation in these matters is desirable.[324]

---

[314] Schmitt, "Due Diligence."

[315] ICJ, Corfu Channel Case (United Kingdom v. Albania); Merits.

[316] Jensen, "The Tallinn Manual 2.0: Highlights and Inisghts."

[317] United Nations General Assembly Resolution 68/69, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98 (24 June 2013)"; United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174.

[318] Schjølberg and Hubbard, "Harmonizing National Legal Approaches on Cybercrime," 10.

[319] Glaser, "Nullum Crimen Sine Lege," 34.

[320] Weber, "The Council of Europe's Convention on Cybercrime," 426.

[321] Weber, "The Council of Europe's Convention on Cybercrime."

[322] United Nations Office on Drugs and Crime, "International Cooperation in Criminal Matters: Counter-Terrorism."

[323] United Nations Office on Drugs and Crime.

[324] „Although as a general matter States are not obliged to cooperate in the investigation and prosecution of cybercrime, such cooperation may be required by the terms of an applicable treaty or other international law

At both regional and global level, several efforts have been made to ensure harmonization of national legal approaches on cybercrime under the auspices of various international organizations, including OECD,[325] United Nations, Council of Europe, International Telecommunication Organization[326] or League of Arab States.[327]

5.2.3.1 The United Nations

The United Nations has been involved in the development of cybercrime related policy since 90s, when it published the Manual on the Prevention and Control of Computer Related Crime examining a wide range of issues related to crime and cyberspace.[328] In 2000 and 2002 the General Assembly adopted the resolutions 55/63 a 56/121 on "Combating the Criminal Misuse of Information Technology".[329] The General Assembly acknowledged, *inter alia*, that states should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies. In addition, national legal systems should protect the confidentiality, integrity and availability of data and ensure that criminal abuse is penalized.[330]

Additionally, since the traditional means of formal international cooperation in cybercrime matters are not able to offer the timely response needed for effective tackling cyber criminality, the United Nations Office on drugs and Crime (UNODC) and the Commission on Crime Prevention and Criminal Justice seek to provide technical assistance in capacity building, prevention and awareness raising, international cooperation, and data collection, research and analysis on cybercrime.[331]

5.2.3.2 Council of Europe's Convention on Cybercrime

Origins of the Council of Europe's Convention on Cybercrime can be traced back to 1989, when the Council of Europe published a set of recommendations recognizing the importance of an adequate and quick response to the new challenge of computer-related crime.[332] A decade later, in 2001, the Council of Europe opened for signature the first international treaty on crimes committed via the internet and other computer networks - Council of Europe's Convention on Cybercrime, known as the Budapest Convention. The treaty reflects an awareness of the jurisdictional dilemma and abovementioned difficulties in coping with transnational cybercrime.

---

obligation." See Rule 13 – International cooperation in international law enforcement. Schmitt, "Jurisdiction."; Walden2004 page 322.

[325] Since 1983, an OECD' s expert committee has discussed computer-related crime and the need for changes in the Penal Codes. See Schjolberg, *The History of Cybercrime: 1976-2014*, 36–37.

[326] A harmonization on global cybersecurity and cybercrime legislation is actively addressed by the ITU. In 2007, the ITU launched the Global Cybersecurity Agenda (GCA) as a framework for international cooperation aimed at proposing solutions to enhance confidence and security in the information society. The GCA is built upon the following five work areas: a) legal measures, b) technical & procedural measures, c) organizational structures, d) capacity building and e) international cooperation. See International Telecommunication Union, "An Agenda for Change, A Global Strategy."

[327] Arab Convention on Combating Information Technology Offences adopted in 2010. It has been signed by all GCC countries and ratified by all of them except for Saudi Arabia. More: States, "Arab Convention on Combating Information Technology Offences."

[328] Westby, *International Guide to Cyber Security*, 82.

[329] United Nations General Assembly, "Combating the Criminal Misuse of Information Technologies A/RES/55/63"; United Nations General Assembly, "Combating the Criminal Misuse of Information Technologies, A/RES/56/121."

[330] United Nations General Assembly, "Combating the Criminal Misuse of Information Technologies A/RES/55/63."

[331] United Nations Office on Drugs and Crime, "Global Programme on Cybercrime."

[332] Council of Europe, "Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer Related Crime."

The objectives of the convention are two-fold. First, it seeks to harmonize cybercrime laws and assure the existence of procedural mechanisms to assist in the successful prosecution of cybercrimes. Second, it sets up a fast and effective regime for international cooperation.[333]

With regard to the substantive provisions, the Convention calls for criminalization of four categories of offences – a) offences against the confidentiality, integrity and availability of computer data and systems, b) computer-related offences, c) dissemination of racist or xenophobic materials through computer systems, d) offenses related to infringement of copyright and related rights.[334] Section 2 of the Convention is dedicated to the procedural aspects of criminal investigation and proceedings. It requires states to establish a minimum set of procedural tools at the national level such as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production orders, search and seizure of computer data, real-time collection of traffic data and interception of content data. In addition, the convention allows a state to assert jurisdiction in a computer crime involving a computer system within its territory (even if the perpetrator committed the offence from other contracting party) and grants a state jurisdiction over a citizen of that state who commits a covered offence outside of the state's boundaries.[335] With regard to international cooperation, the convention provides, *inter alia*, principles related to extradition, mutual assistance including mutual assistance regarding provisional measures or investigation powers.[336]

The Council of Europe's Convention on Cybercrime is by some scholars considered to be largely symbolic, because it ultimately failed to articulate a common set of crimes, lacks universal participation and reservations undermine harmonization.[337] On the other hand, the Council's Convention on Cyber Crime is undoubtedly an important step in the right direction. Comprising 63 member countries,[338] the Convention on Cybercrime is the most comprehensive international treaty dealing with cybercrime ever concluded and by many considered as a gold standard of international conventions in the area of cybercrime.[339]

5.2.3.3 Interpol

International Criminal Police Organization (INTERPOL) aims at ensuring and promoting the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries. For these purposes, all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes should be established and developed. Recognizing the principle of non-intervention, Article 3 of the Interpol Constitution reads as follows: "*It is strictly forbidden for the Organization to undertake any intervention or activities of a political, military, religious or racial character."* [340] Thus, INTERPOL serves as a worldwide information hub for law enforcement cooperation.[341]

Securing cyberspace for people and businesses is one of the INTERPOL's goals. In this context, INTERPOL seeks to establish partnerships to secure cyberspace; expand cybercrime investigative expertise; safeguard communities through standard setting, public education; and protect critical

[333] Council of Europe, "Explanatory Reprt to the Convention on Cybercrime," para. 16.

[334] Articles 7-10, Council of Europe, "Convention on Cybercrime."

[335] Weber, "The Council of Europe's Convention on Cybercrime."

[336] Articles 23-35, Council of Europe, "Convention on Cybercrime."

[337] Marion, "The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation," 702–7; Weber, "The Council of Europe's Convention on Cybercrime."

[338] Council of Europe, "Parties/Observers to the Budapest Convention."

[339] Burrus, "The Budapest Convention on Cybercrime – 15th Anniversary."

[340] Article 1, United Nations General Assembly, "Constitution of the ICPO-INTERPOL."

[341] INTERPOL, "The Strategic Framework 2017-2020."

infrastructure.[342] INTERPOL's Global Cybercrime Strategy acknowledges that the borderless nature of cybercrime means that law enforcement agencies face challenges in responding effectively due to the limits of cross-border investigation, legal challenges and diversity in capabilities across the globe.[343]

INTERPOL helps member countries to conduct investigations into cybercrimes and coordinates transnational cybercrime investigations and operations. It is worth mentioning, that INTERPOL launched the Cyber Fusion Centre bringing together cyber experts from law enforcement and industry to analyse all available information on criminal activities in cyberspace and provide countries with coherent, actionable intelligence.[344]

5.2.4 External dimension of state sovereignty: International cooperation and the role of international organizations

External sovereignty enables states to participate in the international system alongside others. External sovereignty plays a fundamental role in addressing tensions between the concept of state sovereignty and transboundary nature of cyber space. However, the principle of sovereign equality of states implies that states are only bound by those rules of law which they had agreed, either by the conclusions of treaties or customarily.[345] A consent of a state plays a pivotal role in generating legal obligation and, thus, international treaties are result of lengthy negotiations seeking to balance positions of states engaged. In this context, international organizations play an important role since they are engaged in preparatory works paving the way for legally binding international treaties.

5.2.4.1 The United Nations

The issue of information security has been on the UN agenda since 1998, when the General Assembly in its resolution 53/70 expressed concern over the malicious use of ICTs (Information Communications Technology), being potentially used for purposes that are inconsistent with the objectives of maintaining international stability and security.[346] In particular, the General Assembly called upon member states to promote the consideration of existing and potential threat in the field of information security, and included this issue it its agenda as an item entitled "*Developments in the field of information and telecommunications in the context of international security*".[347]

Since 2004, mounting challenges posed by growing cyber insecurities have been addressed by Groups of Governmental Experts (GGE) focused on the following topics: a) Existing and emerging threats, b) How international law applies in the use of ICTs, c) Norms, rules and principles of responsible behaviour of States, d) Confidence-building measures and e) Capacity building. Groups of Governmental Experts are established by the General Assembly in order to study or investigate emerging international security concerns and make recommendations. Reports published by GGE are non-binding, however, they are viewed as an important step toward establishing global norms.[348] GGE in 2004 and 2005 failed to produce a report because of a lack of consensus. By contrast and against the background of disruptive ICT incidents in Estonia and Georgia in 2007 and 2009, GGE established in 2009 finally captured global attention.[349]

---

[342] INTERPOL, "Our Seven Global Policing Goals Shape How the Law Enforcement Community Works Together to Create a Safer World."

[343] INTERPOL, "Global Cybercrime Strategy."

[344] INTERPOL, "Investigative Support for Cybercrime."

[345] Simma et al, *The Charter of The United Nations 3E, Vol 1*.

[346] United Nations Office for Disarmament Affairs, "Developments in the Field of Information and Telecommunications in the Context of International Security."

[347] United Nations General Assembly Resolution 53/79, "Developments in the Field of Information and Telecommunications in the Context of International Security, /A/RES/53/70 (4 January 1999)."

[348] Camino Kavanagh, "The United Nations, Cyberspace and International Peace and Security in the 21st Century," 16; Korzak, "International Law and the UN GGE Report on Information Security."

[349] Camino Kavanagh, "The United Nations, Cyberspace and International Peace and Security in the 21st Century."

Especially 2013 GGE report reached consensus on a number of important issues. GGE emphasized that malicious use of ICTs by actors who often operate with impunity is easily concealed and attribution to a specific perpetrator can be difficult. Importantly, the report confirmed that existing international law applies to cyberspace, notably that the Charter of the United Nations; and the international norms and principles constituting state sovereignty apply to state conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory. In addition, states should refrain from using proxies, prevent their territories from being used by non-state actors for unlawful use of ICT, and respect fundamental human rights and freedoms.[350]

The 2015 GGE report provided valuable insights into how international law applies to the use of ICTs by states: a) States have jurisdiction over the ICT infrastructure located within their territory; b) In their use of ICTs, states must observe, among other principles of international law, state sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other states; c) Existing obligations under international law are applicable to state use of ICTs; d) States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms; established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction; e) States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts; f) States must meet their international obligations regarding internationally wrongful acts attributable to them under international law, however, the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a state may be insufficient in itself to attribute the activity to that State.[351]

In December 2018, the General Assembly significantly intensified its effort in developing common understandings on the application of international law in cyber space.[352] In the period of 2019-2021, the issue of security in the use of ICTs will be analysed by two bodies – an Open-ended Working Group and GGE.[353]

Moreover, United Nations Secretary-General António Guterres has made the promotion of a peaceful ICT-environment one of his key priorities and in May 2018, he launched his Agenda for Disarmament, including actions points on ICT-security.[354]

5.2.4.2 NATO

Although NATO placed cyber defence on its political agenda at the Prague Summit in 2002, the first Policy on Cyber Defence was approved in 2008 in response to cyber-attacks against Estonia's public and private institutions. In 2014, NATO recognized cyber defence as part of the Alliance's core task of collective defence, declared that a cyber-attack may lead to the invocation of Article 5 of the Washington Treaty and adopted enhanced policy on cyber defence.[355]

Against the background of rapidly changing threat landscape, NATO acknowledged cyberspace as a domain of operation at the Warsaw Summit in 2016. [356]In the last decade, NATO has continuously

[350] United Nations General Assembly Resolution 68/69, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98 (24 June 2013)."

[351] United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174.

[352] Council on Foreign Relations, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased."

[353] United Nations General Assembly, "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/C.1/73/L.37 (18 October 2018)"; United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security, A/C.1/73/L.27/Rev.1 (29 October 2018)."

[354] The Secretary-General of the United Nations, "An Agenda for Disarmament."

[355] NATO, "Wales Summit Declaration."

[356] NATO, "Warsaw Summit Communiqué," para. 70.

developed national cyber defence capabilities of NATO member states through various initiatives to enhance cyber defence, as a matter of priority, such as a Cyber Defence Pledge.[357]

NATO supports its members by, for example:

- Sharing real-time information about threats through a dedicated malware information sharing platform, as well as exchanging best practices on handling cyber threats;
- Maintaining rapid-reaction cyber defence teams that can be sent to help Allies in addressing cyber challenges;
- Developing targets for Allies to facilitate a common approach to their cyber defence capabilities;
- Investing in education, training and exercises, such as Cyber Coalition, one of the largest cyber defence exercises in the world.[358]

5.3 Malicious cyber activities in the context of international law: Non-State Actors

Over a long period of time, human beings were under the exclusive control of states and for many centuries, there was no international human rights law regime in place.[359] What is more, national sovereignty and the principle of non-intervention have served as a shield for human rights violations. There were some tentative attempts to establish a human rights system under the League of Nations, however they all came to an abrupt end when the Second World War erupted. Hence, foundations of international human rights law were laid in 1945 and 1948 when the UN Charter and the Universal Declaration of Human Rights were adopted. For the first time in human history, an instrument of international law spelled out basic civil, political, economic, social and cultural rights that all human beings should enjoy. The Universal Declaration of Human Rights, adopted by representatives with different legal and cultural backgrounds from all regions of the world was proclaimed as *a common standard of achievements for all peoples and all nations*.[360]

During the second half of the 20th century, states have increasingly concluded agreements grating human rights to individuals within their jurisdiction. These treaties have been either concluded under the auspices of the United Nations, such as the International Covenant on Civil and Political Rights and its two Optional Protocols, and the International Covenant on Economic, Social and Cultural Rights, or in form of regional treaties the European Convention on Human Rights.

International human rights are granted to individuals directly by international rules and exists whatever the content of national legislation. Although most of the international treaties on human rights may be exercised by individuals within the domestic legal system, some of them provide for the right to petition with international adjudicatory body (for example, the European Court of Human Rights in Strasbourg).[361]

Against the background of the economic globalization and widespread use of internet, extraterritorial application of human right treaties has attracted the growing attention of the international community.

5.3.1 Application of human rights in the context of cyber activities

New technologies have not only the potential to assist states in ensuring respect, protection and fulfilment of their human rights obligations, but also risk undermining certain human rights, in particular the right to privacy.[362]

---

[357] NATO, "Cyber Defence Pledge."

[358] NATO, "NATO Cyber Defence."

[359] Cassese, *International Law*, 142–43.

[360] United Nations, "Human Rights."

[361] Cassese, *International Law*.

[362] United Nations General Assembly, "First Report of the UN Special Rapporteur on the Right to Privacy to the Human Rights Council, A/72/540."

In 2013, the UN General Assembly noted that "*the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights(…)*".[363] Bearing in mind that public security objectives may require and justify the gathering and protection of sensitive information, the UN General Assembly contended that states must ensure full compliance with their obligations under international human rights law.[364] In response to the abovementioned concerns, the General Assembly affirmed that the same rights that people have offline must also be protected online.[365]

In addition, the UN Human Rights Council repeatedly confirms that human rights apply to the internet via its resolutions on "The promotion, protection and enjoyment of human rights on the Internet". [366]

More specifically, principles, standards and best practices regarding the promotion and protection of the right to privacy in the digital age have be addressed and explored by the High Commissioner for Human Rights.[367] Moreover, in July 2015, the Human Rights Council appointed Prof. Joseph Cannataci as the first-ever Special Rapporteur on the right to privacy.[368]

However, although various UN bodies constantly acknowledge that human rights apply to the internet, understandings concerning the precise scope of certain human rights in the context of cyberspace vary.[369] According to Prof. Schmitt, different understanding of certain human rights is often caused by different political, economic, legal, social, cultural, historical and religious context. Additionally, not all States are Parties to the same international human rights law treaties.[370]

5.4 Relevant human rights

5.4.1 Freedom of expression

Freedom of expression is one of the most universally recognized and prominent rights in all democratic legal systems. As such, freedom of expression should be restricted only in very exceptional cases. At the international level, the right to free speech is recognized by both the United Nations' Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). The right to freedom of expression is included in vast majority of regional international human rights treaties, including ECHR,[371] AfCHR,[372] or ACHR.[373]

Pursuant to Article 19 of the ICCPR, everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of

[363] United Nation General Assembly resolution 68/168, The right to privacy in the digital age, A/RES/68/167 (18 December 2013).

[364] United Nation General Assembly resolution 68/168.

[365] United Nation General Assembly resolution 68/168.

[366] United Nations Human Rights Committee, "The Promotion, Protection and Enjoyment of Human Rights on the Internet,A/HRC/38/L.10/Rev.1."

[367] Human Rights Council, "The Right to Privacy in the Digital Age Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/27/37."

[368] United Nations Human Rights Office of the High Commissioner, "Special Rapporteur on the Right to Privacy."

[369] See Rule 34 „Applicability" of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations in Schmitt, "International Human Rights Law."

[370] Schmitt.

[371] Council of Europe., European Convention on Human Rightson Human Rights.

[372] Organization of African Unity, African Charter on Human and Peoples Rights.

[373] Organization of American States, American Convention on Human Rights.

frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

Although the ICCPR does not expressly address the internet (the covenant has been concluded in 1966), its wording "any other media" is broad enough to include even modern ways of communication. Applicability of the right to freedom of expression to the internet has been affirmed by the Human Rights Committee in 2011. Its General comment no. 34 reads as follows: "*Article 19 (2) protects all forms of expression and the means of their dissemination. Such forms include spoken, written and sign language and such non-verbal expression as images and objects of art. Means of expression include books, newspapers, pamphlets, posters, banners, dress and legal submissions. They include all forms of audio-visual as well as electronic and internet-based modes of expression*."[374]

With respect to limitations of the right to freedom of expression, the Human Rights Committee argued: "*that any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3*."[375] Pursuant to Article 19 (3) the exercise of the right to freedom of expression can may be subject to certain restriction, however, these have to be provided by law and necessary for the rights of others or for the protection of national security or public order or public health or morals.[376] The Human Rights Committee argued that generic bans of the operation of certain sites and systems are not compatible with Article 19.[377]

In this context, the former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression contended that decisions to regulate content, such as blocking web sites, must be taken by a competent judicial authority independent of political, commercial or other unwarranted influences.[378]

An interesting insight into the practice of OSCE participating states related to the content regulation on the internet can be found in the Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the internet in OSCE participating states. The report assesses whether and how access to and content on the internet are regulated across the OSCE region by examining existing laws and practices related to freedom of expression, the free flow of information.

An internet content regulation of the participating states usually addresses:

a) racist content, xenophobia and hate speech (80% of participating states)
b) denial, approval or justification of genocide or crimes against humanity (41% of participating states)
c) incitement to terrorism or terrorist propaganda (70% of participating states)
d) child pornography (77 % of participating states)
e) obscene and sexually explicit content (72% of participating states)
f) internet piracy (78% of participating states)
g) libel and insult on the internet (64% of participating states)
h) expression of views perceived to be encouraging extremism (36% of participating states)

[374] United Nations Human Rights Committee, "International Covenant on Civil and Political Rights, General Comment No. 34, CCPR/C/GC/34."

[375] United Nations Human Rights Committee.

[376] United Nations, "International Covenant on Civil and Political Rights by General Assembly Resolution 2200A (XXI) of 16 December 1966."

[377] United Nations Human Rights Committee, "International Covenant on Civil and Political Rights, General Comment No. 34, CCPR/C/GC/34."

[378] United Nations Human Rights Office of the High Commissioner, "Freedom of Expression Everywhere, Including in Cyberspace."

i) distribution of harmful content (34% of participating states).[379]

5.4.2 Privacy

Pursuant to Article 17 of the ICCPR, no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Although the ICCPR does not explicitly mention cyberspace, it is generally understood that the right to privacy should be protected also in digital communication. Similar provisions may be found in various regional human right treaties, such as ACHR,[380] ECHR.[381]

Expressing deep concern at the negative impact that surveillance and interception of communications may have on human rights, the General Assembly in its resolution 68/167 acknowledged that that the exercise of the right to privacy is important for the realization of the right to freedom of expression, one of the foundations of a democratic society.[382] Against the background of the enhanced capacity of governments, companies and individuals to undertake surveillance, interception and data collection, human rights may be threatened or violated, and in particular the right to privacy, set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights. Accordingly, the General Assembly called upon all states to respect and protect the right to privacy in digital communication.[383]

Moreover, the right to privacy in the digital age has been a subject of a report prepared by the High Commissioner for Human Rights.[384] The report revealed that any capture of communications data is potentially an interference with privacy and the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Although Article 17 of the ICCPR does not include any explicit limitation clause, interference with an individual's right to privacy is permissible under international human rights law if it is neither arbitrary nor unlawful. Such conclusions can be drawn from the practice of the Human Rights Committee. Additionally, any limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available.[385]

Since 2015, the right to privacy has been continuously addressed by the UN Human Rights Council and, especially, by a Special Rapporteur on the right to privacy.[386] The creation of his mandate was motivated by the wake of the revelations by Edward Snowden.[387] The Special Rapporteur has been tasked to focus on alleged violations of the right to privacy including in connection with the challenges arising from new technologies. In particular the mandate covered five thematic action streams addressing the challenges to privacy in the digital era, namely a better understanding of privacy; security and surveillance; big data and open data; health data; and the use of personal data by corporations.[388]

---

[379] OSCE, *Freedom of Expression on the Internet: A Study of Legal Provisions and Practices Related to Freedom of Expression, the Free Flow of Information and Media Pluralism on the Internet in OSCE Participating States*.

[380] Organization of American States, American Convention on Human Rights.

[381] Council of Europe., European Convention on Human Rightson Human Rights.

[382] United Nation General Assembly resolution 68/168, The right to privacy in the digital age, A/RES/68/167 (18 December 2013).

[383] United Nation General Assembly resolution 68/168.

[384] United Nations Human Rights Office of the High Commissioner, "The Right to Privacy in the Digital Age."

[385] Human Rights Council, "The Right to Privacy in the Digital Age Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/27/37."

[386] Human Rights Council Resolution 28/16.

[387] Human Rights Council, "Report of the Special Rapporteur on the Right to Privacy, A/HRC/37/62," para. 13.

[388] United Nations Human Rights Office of the High Commissioner, "Special Rapporteur on the Right to Privacy."

According to the UN Special Rapporteur, every day our digital activities produce about 2.5 quintillion bytes of data.[389] However, a great deal of data is gathered from ordinary users, resold or shared without their knowledge or consent. The main obstacle to protecting the right to privacy under surveillance, identified by the UN Special Rapporteur, is the lack of inadequacy of detailed rules and oversight mechanisms to ensure independent, reliable and efficient control of surveillance, both nationally and globally.[390]

The UN Special Rapporteur made following observations:

a) Government-led surveillance puts privacy of many individuals at risk.
b) In order to effectively protect the right to privacy in the context of cyberspace, a comprehensive legal framework providing both safeguards and remedies should be established.
c) Where a citizen is subject to surveillance by his/her own Government then the safeguards and remedies must normally be sought within domestic law. In this context, domestic law should require precautionary measures designed to ensure that surveillance cannot be initiated until or unless it is proved to an independent and competent authority that this surveillance is legal, necessary and proportionate to objective pursued.
d) Where a citizen is subject to surveillance by a State which is not his own, citizens options are very limited and include options provided by domestic law of the state conducting the surveillance and international human rights.
e) The UN Special Rapporteur found that more than 33 percent of United Nations Member States, i.e. over 70 countries, have no privacy law at all ,and more than 80 percent of the United Nations Member States do not have any law which protects privacy by adequately and comprehensively overseeing and regulating the use of domestic surveillance.[391]

5.4.3 Right to be forgotten

The internet is often portrayed as an information market allowing people access to a potentially unlimited amount of information with just a computer and connection. However, once information is uploaded, the internet stores it permanently. This "digital eternity" may infringing upon individuals' right to privacy.[392]

The right to be forgotten emerged in May 2014 from the CJEU's (Court of Justice of the European Union) decision in Google Spain SL v. Agencia Española de Protección de Datos and Mario Costeja González (Google Spain judgment).[393] In the case, Mr González argued that when an internet user entered his name in the search engine of the Google group, he would obtain links to two pages of La Vanguardia's newspaper of 1998, mentioning his name due to the repossession and auction of his home following attachment proceedings for the recovery of social security debts. He contested that the issue had been resolved for over a decade and required to remove or conceal the personal data relating to him so that they ceased to be included in the search results.[394]

The court held: *"(…) even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be*

[389] United Nations General Assembly, "First Report of the UN Special Rapporteur on the Right to Privacy to the Human Rights Council, A/72/540."

[390] Human Rights Council, "Report of the Special Rapporteur on the Right to Privacy, A/HRC/37/62."

[391] Human Rights Council.

[392] Alessi, "Eternal Sunshine: The Right to Be Forgotten in the European Union after the 2016 General Data Protection Regulation."

[393] Court of Justice of the European Union, "C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González."

[394] Court of Justice of the European Union.

inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed." Therefore, the court found that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible the EU directive 94/46 (Data Protection Directive) because that information appears to be no longer relevant or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased."[395]

According to the CJEU, the EU directive 94/46 ("DPD") should be interpreted in light of Articles 7 and 8 of the EU Charter of Fundamental Rights, guaranteeing the right to private life and the right to privacy of personal data, and concluded that the protection of those rights encompasses the "right to be forgotten".[396] Thus, the Court established a presumption that the right to privacy trumps the general public's right to access information as well as the economic interest of the search engine.[397]

In 2016, the General Data Protection Regulation (GDPR) replaced the EU directive 94/46. It contains a right to be forgotten that will likely be interpreted in light of Google Spain judgment. According to Prof. Post, the GDPR marks the triumph of a distinctive EU variant of the right to be forgotten that derives directly from data privacy and that can be expected to have massive international consequences since it sharply poses the general theoretical question of how fair information practices can be reconciled with freedom of expression.[398]

With respect to the right to be forgotten, the authors of the Tallinn Manual were of the opinion that, at present there is no customary international human rights law-based obligation of states to require third parties to remove personal data or links to that data from the internet on the basis of a 'right to be forgotten'.[399]

5.4.4 Obligation to respect and protect human rights

Since international human rights law is applicable to cyberspace, states must respect human rights of individuals and protect the human rights from abuse by third parties.[400] In other words, the authors of the Manual concluded that if the activities of a non-state actor or another state interfere with the ability of individuals to engage in cyber activities protected by international human rights law, states may shoulder an obligation to ensure that the individuals entitled to benefit from the rights in question can do so.[401]

An obligation to respect human rights is triggered always when a malicious cyber operation is attributable to a state. For instance, a state using proxy actors to engage in hostile cyber operations will be responsible for human rights violations that occur in the course of that operation.[402] Additionally, customary international human rights law applies beyond state's territory in situation when that state exercises power or effective control over territory or over individuals. For example, a

[395] Court of Justice of the European Union.

[396] Court of Justice of the European Union.

[397] Alessi, "Eternal Sunshine: The Right to Be Forgotten in the European Union after the 2016 General Data Protection Regulation."

[398] Post, "Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere," 987.

[399] Schmitt, "International Human Rights Law."

[400] See Rule 36 of the Tallinn Manual. Schmitt.

[401] Ali, "Derogation from Constitutional Rights and Its Implication under the African Charter on Human and Peoples ' Rights '."

[402] Schmitt, "International Human Rights Law."

state has effective control over foreign territory during a belligerent occupation. However, there is no general consensus on a clear definition of "power or effective control".[403]

With respect to particular international human rights law treaties, their extraterritorial application is determined by their jurisdiction clauses. These clauses identify the range of persons to whom states owe their human rights obligations under the treaty. Article 2(1) of the ICCPR stipulates that state parties to the covenant undertake to respect and to ensure to all individuals within its territory and subject to its jurisdiction.[404] Although commentators initially endorsed the literal reading of the article and limited the scope of its application to the territory of a contracting party, the Human Rights Committee abandoned this reading and concluded that the covenant must be available to those within the power or effective control of a state party outside its territory.[405]

5.4.5 Limitations and derogation from obligations arising from international human rights law

It is generally accepted, that the obligation to respect and protect international human rights, with the exception of absolute rights, should be balanced in relation to other international human rights or competing communal aims such as protection of the rights of others, public order, public health, public morals, and national security or the promotion of general welfare. The most common method to address conflict of values and interests is balancing.[406] As Basak Cali points out, balancing has become a key concept in qualifying human rights in the case law of the European Court of Human Rights and is spreading to domestic jurisdictions.[407] In practice, balancing of human rights aims at determining whether their implementation takes precedent over a communal interest.[408] By the same token, international human rights relevant in cyber context are to be balanced in relation to competing communal aims, particularly public order and national security.

Some human rights treaties permit states to derogate from the binding nature of certain obligations in times of public emergency. Treaties usually refer to time of war or public emergency threatening the life of the nation (See ICCPR, ECHR), or emergency threatening the independence or security of state parties (See Article 26 of the American Convention on Human Rights). Interestingly the African Charter on Human and Peoples' Rights does not include any derogation clause.[409] The precise conditions of individual treaties vary. Although a derogation is applicable to cyber activities,[410] states should take measures derogating from their obligations to extent strictly required by the

[403] Schmitt.

[404] United Nations, "International Covenant on Civil and Political Rights by General Assembly Resolution 2200A (XXI) of 16 December 1966."

[405] Dennis, "Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation," 122–23.

[406] Greer, "'Balancing' and the European Court of Human Rights : A Contribution to the Habermas- Alexy Debate Author (s): Steven Greer Source : The Cambridge Law Journal , Vol . 63 , No . 2 (Jul ., 2004), Pp . 41."

[407] Çali, "Balancing Human Rights? Methodological Problems with Weights, Scales and Proportions."

[408] Çali.

[409] Ali, "Derogation from Constitutional Rights and Its Implication under the African Charter on Human and Peoples ' Rights '."

[410] See Rule 38 of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Schmitt, "Tallinn Man. 2.0 Int. Law Appl. to Cyber Oper."

exigencies of the emergency situation.[411] Derogations relevant in cyber context include blocking access to internet or removing online posts that might exacerbate a situation of emergency.[412]

However, it is worth mentioning, that human rights treaties may except certain human rights from derogation. The ICCPR prohibits derogation from provisions protecting, *inter alia*, the prohibition of the arbitrary deprivation of life, the prohibition against torture and slavery, the right to recognition as a person before the law, and the right to freedom of thought, conscience and religion.[413] The European Convention on Human Rights prohibits derogation from right to life, expect in respect of death resulting from lawful acts of war, from the prohibition of torture, the prohibition of slavery, and the prohibition of punishment without law even during times of emergency.[414]

6. Conclusions

In this document , we have introduced a novel perception of cyber space that is not limited to a technical descriptions but rather provides an cultural background and etymological source that both can influence the way how we perceive it. We introduced various actors operating in cyber space with their objectives and dynamics with an intention to balance the alarmist and critical discourse. The objective of this document was not to create a comprehensive classification but rather to present what various scholars, business and governments think about the cyber space and cyber security.

The above depicted dystopian fiction of cyberpunk can be considered a source of inspiration to the geek communities, to those who develop liberation technologies (crypto-anarchists) or those who apply the technology to change the world order(ultra-libertarians/anarcho capitalists). However, there is a conflict within resistance as well: while the crypto-anarchists would give the knowledge for free completely, the libertarian anarcho-capitalists would make money on everything but are not consistent when it comes to knowledge. Even within the community that resists the authorities are fundamental antagonisms. It is needed to understand the cultural basis of these motivations as the imaginaries the fictitious stories inspire people to cooperate. As Aradau and Munster[415] influentially argued, the knowledge of possible catastrophes is important in order to react in a normalized manner. If we fall into dystopian visions drawing near future insecurities in clearly fictitious way, we will find ourselves deeply swallowed by the dystopian visions. Knowledge about the subculture helps to predict actions of respective actors, but they react in resistance. More regulation of cyberspace means more powerful resistance. Too much regulation seeking the utopian totalized solution will lead to uncontrollable resistance and will lower the credibility of liberal democratic societies. Ideas like the one of DARPA with artificial intelligence patching exploits as self-learning organism is not a dystopian vision, it is a consequence of these dystopian imaginations, it is real. It does not solve the problem; it constructs it in a much more tremendous and absolutely unpredictable shape of future.

We should mainly focus on the empirical data (cyber crime) and tackle what the criminal actors do. If a nation state uses criminal networks to buy intelligence, it should be still perceived as criminal act because the effective way is to tackle the actors conducting the attack by their hands rather than to punish a nation state in cyber space according to international law.

Cyber security analysed from the international law perspective revealed that only enhanced international cooperation and international law can adequately address transboundary nature of

---

[411] United Nations, "International Covenant on Civil and Political Rights by General Assembly Resolution 2200A (XXI) of 16 December 1966."

[412] Commissioner for Human Rights, "Arbitrary Internet Blocking Jeopardises Freedom of Expression"; Human Rights Watch and Not, "France : New Emergency Powers Threaten Rights"; Palfrey and Zittrain, "Access Denied: The Practice and Policy of Global Internet Filtering - Book Review."

[413] United Nations, "International Covenant on Civil and Political Rights by General Assembly Resolution 2200A (XXI) of 16 December 1966."

[414] Council of Europe., European Convention on Human Rightson Human Rights.

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

cyber threats. However, this will require increased effort in developing common understandings on the application of international law in cyber space.

7. Appendixes

7.1 Notable hacktivist groups

7.1.1 Anonymous

The group that, in fact, is responsible for defining modern hactivism. At first, 'Anonymous' was a collective name acquired by the users from the 4chan message boards, in the early 2000's. They would frequently band together when attacking targets out of sheer boredom, conducting "trolling campaigns" [416] for 'the lulz' – or in other words, fun or amusement, typically undertaken at the expense of others. [417] Their activities encompassed irritating, but relatively harmless pranks, such as ordering dozens of pizzas to one's house, as well as more vicious harassment, like online abuse, carrying out DDoS attack or doxxing other Internet users. The group is unique among others as it is faceless, amorphous, made up of multiple proxy organisations and affiliated hackers. There is no formal membership, internal structure or controlling body. Anybody can take part in its actions at will; the targets and attack vectors the group picks are determined by popular consensus among its members and fans. At first, Anonymous rather targeted Internet personalities and was not really focused on political or ideological issues. However, in 2008 they moved to political activism, when the members carried out a series of attacks against the church of Scientology. Before resorting to physical protests outside multiple Scientologist properties, the members performed a week long DDoS attack against the website of the church. [418] The whole operation was called Project Chanology. As the protesting Anonymous members wore the Guy Fawkes mask adopted from the graphic novel V for Vendetta, is has incidentally become the symbol of hactivism. Afterwards, the group has also been actively involved in several campaigns aimed at protecting Internet freedom. For instance, they broadly participated in fighting against the Stop Online Piracy (SOPA) and the Protect Intellectual Property Act (PIPA), accusing both of trying to censor the web. In 2012, in response to the Israeli military operation in the Gaza Pillar of Defence, the group performed a DDoS attack against several Israeli websites and exposed names, identification numbers and personal e-mails of 5 thousand Israeli Defence Force officials. In 2014, Anonymous launched two operations, Op Russia and Op Ukraine, subjecting Russian cyberspace to digital attacks. It was the response to the Russian manoeuvres in Crimea [419]. The group has also been known for persistently attacking the online arms of the terrorist group ISIS following the Islamic State attacks on Paris in 2015. Anonymous set out to dismantle the large network of IS websites and social media accounts, thus making spreading the terrorist propaganda more difficult. However, it has been said that although their motive was for social justice, their methods could have caused more damage than good and were brought into question. It is possible that the takedown of the alleged IS accounts and forums hampered intelligence operations of actual counterterrorism experts and the intelligence community employed to dismantle these terrorist tools, as it is highly unlikely that Anonymous has the skillset to properly vet these accounts. Recently, the group also targeted the 2016 presidential campaign of U.S. President Donald Trump and Ku Klux Klan's (KKK) websites. [420], [421]

7.1.2 Edward Snowden/ Wikileaks

He became famous when after leaving the United States in May 2013 he flew to Hong Kong and within several weeks he leaked thousand of documents to the media. Thus, he revealed extensive

---

[416] Richards and Wood, "Hacktivists against Terrorism: A Cultural Criminological Analysis of Anonymous' Anti- IS Campaigns."

[417] Coleman, *Hacker, Hoaxer, Whistleblower, Spy. The Many Faces of Anonymous.*

[418] Deseriis, *Improper Names: Collective Pseudonyms from the Luddites to Anonymous*.

[419] Ohlin, Govern, and Oxford, "Nicolò Bussolati ' The Rise of Non-State Actors in Cyberwarfare .'"

[420] Afifi-Sabet, "What Is Hacktivism?"

[421] Gargano, "Three Common Threat Actors and the One You Might Not Know About."

Internet and phone surveillance program by American intelligence agencies. Snowden illegally downloaded and collected the documents from the National Security Agency (NSA) to expose its surveillance practices that he believed violated the right to privacy of the American citizens. After many of the documents were printed by prominent newspapers, such as The Guardian or The Washington Post, the U.S. Department of Justice announced charges against him, including espionage and theft. Snowden, who has yet to be tried for his actions, was granted temporary asylum in Russia. [422]

7.1.3 LulzSec

The groups' name being the combination of "lulz" ("for laughs") and "security". They became famous after attacking the Fox.com website in 2011, because they were not particularly fond of some piece of news Fox had given, apparently. LulzSec found the weakness of the site and leaked the profiles and names of over 70 thousand X factor US contestants. Later they attacked the US broadcaster PBS and planted there a fake story about the dead rappers Tupac Shakur and Biggie Small being in fact alive and living in New Zealand; they hacked into game companies such as Nintendo and Bethesda Studios and into Playstation Network (stealing personal data of almost 25 million customers), forcing the company to take the network offline for several days. LulzSec called themselves "latter-day pirates" and boasted to be "gods". Their intention was just to "gain attention, embarrass website owners and ridicule security measures". However, although they argued that the sites they hacked were so insecure that they were a risk to their customers, the group caused problems that cost hundreds of thousands of dollars to fix, e.g. by putting private information online. The group's downfall began after its members knocked offline an FBI-affiliated website, thus bringing themselves to the attention of federal authorities in the U.S. Then, one of the members forgot to disguise his location when logging into a chat forum and was traced by the FBI back to his home. He was offered a choice – go to jail or cooperate. Owing to family reasons he chose the latter and came back online, with the FBI monitoring everything he did. This led to arrests and charges against several members of the group. [423][424]

7.1.4 Impact Team

The group who became famous after stealing the personal information of 32 (according to some sources – even 37) million users of the extramarital dating site Ashley Madison, the slogan of which being "life is short, have an affair". The hackers demanded that the website be taken down – only then they would not release its customers' data, which included names, passwords, addresses and even phone numbers of the users. The website's owners did not comply with the group's claims, releasing the statement that "this event is not an act of hactivism, it is and act of criminality. (…) The criminal, or criminals, involved in this act have appointed themselves as the moral judge, juror, and executioner, seeing fit to impose a personal notion of virtue on all of society. We will not sit idly by and allow these thieves to force their personal ideology on citizens around the world." The refusal resulted in Impact Team exposing the data and thus leading to potential consequences of the breach including public embarrassment, furious spouses and people becoming vulnerable to blackmail of fraud. The attack was most probably motivated by moral concerns, as the group publicly referenced to Ashley Madison's users as "cheating dirtbags [who] deserve no such discretion". [425] [426]

---

[422] Benton, "The Misinformers: Edward Snowden, Aaron Swartz and The Troubled Relationship Between Hacktivists, Mass Media and American Government."

[423] Arthur, "LulzSec: What They Did, Who They Were and How They Were Caught."

[424] Baraniuk, "Ten Hacktivists Who Shook the Web."

[425] Afifi-Sabet, "What Is Hacktivism?"

[426] Magal, "WHO ARE THE HACKTIVISTS?"

7.1.5 Redhack

A radical leftist, self-identified Marxist-Leninist hacktivist organization from Turkey. They diverge clearly from other hacktivist groups from that country, most of whom are „patriotic hackers" working for the sake of national causes [427]

7.1.6 Cyber Berkut

A pro-Russian hacker group that repeatedly attacked NATO and Ukrainian websites. [428]

7.1.7 The Red Hacker Alliance

One of the most well-known Chinese patriotic hacker groups, has been particularly active since the late 1990s. [429]

7.1.8 The Chaos Computer Club (CCC)

One of the earliest hacktivist groups. Its members did not just shut down websites, but also tried to disturb telecommunication infrastructures as a form of protest against censorship and nuclear testing (Anderson 2008, 5 in: [430]).

7.1.9 Worms Against Nuclear Killers

The hacktivist malware that was released into NASA's network to protest the launch of the nuclear-powered rocket, carrying the Galileo probe into orbit. Reportedly, according to officials, due to the attack the project lost half a million dollars in lost time and resources. [431]

7.1.10 Electronic Disturbance Theatre (EDT)

A group that supported the Zapatista movement in Mexico in 1998, using internet technologies.

7.1.11 The Electrohippies

Hackers who protested against the World Trade Organisation in Seattle in 1999. (Jordan and Taylor 2004, 71-79). [432]

7.1.12 Di5s3nSi0N

Muslim hacking collective. Amaq, the main online outlet and "official" news agency of terror organisation Isis/Daesh, sent a statement to its subscribers that after some earlier online attacks it had "imposed more stringent security measures on [its] systems" and bragged it could "handle email attacks or any other type of hack". Di5s3nSi0N tweeted a "challenge accepted" meme in response and three hours later sent an e-mail calling Isis cowards and dogs. The e-mail also contained a list of over 1700 e-mail addresses of real accounts belonging to Amaq newsletter subscribers. In addition, Amaq's website was taken offline for some time. [433]

---

[427] Dogan, "Contextualizing Hacktivism: The Criminalization of Redhack."

[428] Ohlin, Govern, and Oxford, "Nicolò Bussolati ' The Rise of Non-State Actors in Cyberwarfare ."'

[429] Dogan, "Contextualizing Hacktivism: The Criminalization of Redhack."

[430] Dogan.

[431] Afifi-Sabet, "What Is Hacktivism?"

[432] Dogan, "Contextualizing Hacktivism: The Criminalization of Redhack."

[433] McCallion, "Anti-Isis Hacktivists Compromise Terrorists' Website | IT PRO."

8. References

Aaviksoo, J. "Cyberspace: A New Security Dimension at Our Fingertips." CSIS Statesmen's Forum, 2007.

Ablon, Lillian. "The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data: Hearings before the Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, United States House, 115th Cong. 1," 2018.

Addawood, Aseel, Adam Badawy, Kristina Lerman, and Emilio Ferrara. "Linguistic Cues to Deception: Identifying Political Trolls on Social Media." In *Proceedings of the Thirteenth International AAAI Conference on Web and Social Media (ICWSM 2019)*, 2019.

Afifi-Sabet, Keumar. "What Is Hacktivism?," 2018.

Ahmad, Rabiah, and Zahri Yunos. "A Dynamic Cyber Terrorism Framework." *International Journal of Computer Science and Information Security*, 2012.

Alessi, Stefania. "Eternal Sunshine: The Right to Be Forgotten in the European Union after the 2016 General Data Protection Regulation." *Emory International Law Review* 32, no. 1 (2017).

Ali, Abdi Jibril. "Derogation from Constitutional Rights and Its Implication under the African Charter on Human and Peoples ' Rights '." *Law Democracy & Development* 17, no. June 1981 (2013): 78–110. https://doi.org/10.4314/ldd.v17i1.5.

Alien Entity. "Urban Dictionary: Troll," 2002.

Anonymous. "Cyberterrorism: The Invisible Threat Stealth Cyber Predators in a Climate of Escalating Risk." *Foreign Affairs* 89, no. 6 (2010). https://doi.org/https://pustaqa.com/cyberterrorism-invisible-threat-stealth-cyber-predators-in-climate-of-escalating-risk/.

Applebaum, Anne. "How Much Trouble Is Russia Causing in Europe?" Slate.com, 2016. https://slate.com/news-and-politics/2016/04/the-dutch-referendum-on-ukraine-shows-how-russia-is-influencing-europeans.html.

———. "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.

Arquilla, John, and David Ronfeldt. "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (1993): 141–65. http://www.tandfonline.com/doi/abs/10.1080/01495939308402915.

Arthur, Charles. "LulzSec: What They Did, Who They Were and How They Were Caught." *The Guardian*, May 2013.

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

Bae Systems. "The Nation State Actor Has a 'Licence to Hack' – and They Use It Target Their Adversaries." Accessed August 10, 2019. https://www.baesystems.com/en/cybersecurity/feature/the-nation-state-actor.

Balzacq, Thierry, Sarah Léonard, and Jan Ruzicka. "'Securitization' Revisited: Theory and Cases." *International Relations* 30, no. 4 (December 27, 2016): 494–531. https://doi.org/10.1177/0047117815596590.

Barabási, A L. *Linked: The New Science of Networks*. Cambridge, Massachusetts: Perseus Publishing, 2002.

Baraniuk, Chris. "Ten Hacktivists Who Shook the Web," 2013.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B J Walker. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8, no. 2 (2014): 121–44. https://doi.org/10.1111/ips.12048.

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

Beggs, C. "Cyber-Terrorism in Australia." *IGI Global*, 2008.

Benton, Brian. "The Misinformers: Edward Snowden, Aaron Swartz and The Troubled Relationship Between Hacktivists, Mass Media and American Government," 2015.

Besson, Samantha. "Sovereignty." Max Planck Encyclopedia of Public International Law, 2011.

Bieda, David, and Leila Halawi. "Cyberspace: A Venue for Terrorism." *Issues in Information Systems* 16, no. 3 (2015).

Bishop, Jonathan. "Tackling Internet Abuse in Great Britain: Towards a Framework for Classifying Severities of 'Flame Trolling,'" 2012.

———. "The Effect of De-Individuation of the Internet Troller on Criminal Procedure Implementation: An Interview with a Hater." *International Journal of Cyber Criminology*, 2013.

"Bitlegal Tracks the Evolving Regulatory Landscape of Cryptocurrency, Digital Assets and Distributed Ledger Technology around the World." Bitlegal.io, n.d.

Boas, Richard. "Sinister New Site 'Assassination Market' Enables Users to Contribute Bitcoins for Murder of US Officials." Coindesk.com, 2013.

Booth, Ken. "Security and Emancipation." *Review of International Studies* 17, no. 4 (October 26, 1991): 313–26. https://doi.org/10.1017/S0260210500112033.

———. "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.

———. *Theory of World Security*. Cambridge University Press, 2007.

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

Buchan, Russell, Marco Roscini, and Nicholas Tsagourias. "State Responsibility for Cyber Operations: International Law Issues Event Report." *State Responsibility for Cyber Operations: International Law Issues*, no. October (2014): 1–14.

Burrus, Gene. "The Budapest Convention on Cybercrime – 15th Anniversary." *Microsoft Security*, 2016.

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

Buzan, Barry, Ole Wæver, J de Wilde, and Jaap De Wilde. *Security: A New Framework for Analysis*. *National Bureau of Economic Research Working Paper Series*. Lynne Rienner Publishers, 1998.

Caldwell, Tracey. "Hacktivism Goes Hardcore." *Network Security*, 2015. https://doi.org/10.1016/S1353-4858(15)30039-8.

Çali, Başak. "Balancing Human Rights? Methodological Problems with Weights, Scales and Proportions." *Human Rights Quarterly* 29, no. 1 (2007): 251–70. https://doi.org/10.1353/hrq.2007.0002.

Caliskan, Murat. "A Critique of Hybrid Warfare in the Light of Russia-Ukraine Crisis and Military Strategy." Beyond the Horizon, 2017. https://www.behorizon.org/a-critique-of-hybrid-warfare/.

Cambria, Erik, Praphul Chandra, Avinash Sharma, and Amir Hussain. "Do Not Feel The Trolls," 2010.

Camino Kavanagh. "The United Nations, Cyberspace and International Peace and Security in the 21st Century," 2017.

Cassese, Antonio. *International Law*. Second Edi. Oxford University Press, 2005.

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

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

———. "Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat

Debate." *Journal of Information Technology & Politics* 4, no. 1 (2008): 19–36. https://doi.org/10.1300/J516v04n01_03.

Cavelty, Myriam Dunn, and Elgin M. Brunner. "'Introduction: Information, Power, and Security—an Outline of Debates and Implications." In *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, edited by Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia Krishna-Hensel, 8–9. Aldershot: Ashgate, 2007.

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

CCDCOE. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Edited by Michael N. Schmitt. New York: Cambridge University Press, 2013.

Charlish, Alan. "Polish Deputy Minister Resigns over Judge Trolling Scandal," 2019.

Choucri, N. *Cyberpolitics in International Relations*. Cambridge, Massachusetts and London, England: MIT Press, 2012.

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

Clinton, William J. "Remarks at Wharton School of Business, University of Pennsylvania on 16 April 1992." Philadelphia, 1992.

"CloudFlare." Accessed March 29, 2016. https://www.cloudflare.com/.

Coleman, Gabriella. *Hacker, Hoaxer, Whistleblower, Spy. The Many Faces of Anonymous.* London, 2014.

Collins, Sean, and Stephen McCombie. "Stuxnet: The Emergence of a New Cyber Weapon and Its Implications." *Journal of Policing, Intelligence and Counter Terrorism* 7 (April 2012): 80–91. https://doi.org/10.1080/18335330.2012.653198.

Commissioner for Human Rights. "Arbitrary Internet Blocking Jeopardises Freedom of Expression." Council of Europe, 2017.

Cook, Christine, Juliette Schaafsma, and Marjolijn Antheunis. "Under the Bridge: An in-Depth Examination of Online Trolling in the Gaming Context." *New Media & Society* 20, no. 9 (September 2018): 3323–40. https://doi.org/10.1177/1461444817748578.

Corn, Gary P., and Robert Taylor. "Sovereignty in the Age of Cyber." *AJIL Unbound* 111 (2017): 207–12. https://doi.org/10.1017/aju.2017.57.

Council of Europe. European Convention on Human Rightson Human Rights (1952).

Council of Europe. "Convention on Cybercrime," 2001.

———. "Explanatory Reprt to the Convention on Cybercrime." *European Treaty Series - No. 185*, no. 185 (2001): 60.

———. "Parties/Observers to the Budapest Convention," n.d.

———. "Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer Related Crime," 1989.

Council on Foreign Relations. "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased," 2018.

Court of Justice of the European Union. "C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González," 2014.

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

Cyrus FARIVAR. "A Brief Examination of Media Coverage of Cyberattacks (2007-Present)," n.d.

Czosseck, C., and K. Geers. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Ios Press, 2009.

DARPA. "Cyber Grand Challenge," 2016. http://www.cybergrandchallenge.com/site/index.html#about.

Deleuze, Gilles, and Felix Guattari. *Anti-Edipus. Capitalism and Schizophrenia*. *SubStance*. Minneapolis:

University of Minnesota Press, 1983. https://doi.org/10.2307/3684887.

Denning, Dorothy E. "Afterword to 'The Future of Cryptography.'" In *Crypto Anarchy, Cyberstates and Pirate Utopias*, edited by Peter Ludlow, 103. Cambridge, Massachusetts and London, England: MIT Press, 2001.

———. "Cyberterrorism Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives," 2000.

———. "The Future of Cryptography." In *Crypto Anarchy, Cyberstates and Pirate Utopias*, edited by Peter Ludlow, 85–101. Cambridge, Massachusetts and London, England: MIT Press, 2001.

Dennis, Michael J. "Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation." *The American Journal of International Law* 99, no. 1 (2005): 119–41.

Deseriis, Marco. *Improper Names: Collective Pseudonyms from the Luddites to Anonymous*. Minneapolis: University of Minnesota Press, 2015.

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

Dogan, Bülay. "Contextualizing Hacktivism: The Criminalization of Redhack." *CARGC Papers* 10 (2019).

Drozdiak, Natalia. "One of Russia's Neighbors Has Security Lessons for the Rest of Us." *Bloomberg Businessweek*, 2019.

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.

Dusek, Mirek, and Aengus Collins. "Regional Risks for Doing Business 2018," 2018.

DW. "Cyber Attacks, Energy Security and Terrorism – A NATO Perspective on Emerging Security Challenges in the 21st Century." *Deutsche Welle*, April 10, 2014. http://www.dw.com/en/cyber-attacks-energy-security-and-terrorism-a-nato-perspective-on-emerging-security-challenges-in-the-21st-century/a-17533087.

Dziundziuk, Dr. Viacheslav. "Stopping Cyber Terror Countries Must Work Together to Thwart Efforts of Internet Criminals." *Per Concordiam, Journal of European Security and Defense Issues* 2, no. 2 (n.d.).

ECHR. Decision on admissibility delivered by a Chamber Weber and Saravia v. Germany (dec.), no. 54934/00 (n.d.).

Eddy, Max. "Cyber Warfare Is Still a Free-for-All." *PC Magazine*, 2019.

Egan, Brian. "International Law and Stability in Cyberspace." *Berkeley Journal of International Law* 35, no. 1 (2017): 169–80. https://doi.org/10.15779/Z38CC0TT2C.

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

Elias, Herlander. *Cyberpunk 2.0. Fiction and Contemporary*, 2009.

Ellis, R, and V Mohan. *Rewired: Cybersecurity Governance*. Wiley, 2019.

EUROJUST & EUROPOL. "Common Challenges in Combating Cybercrime - As Identified by Eurojust and Europol," 2019. https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime.

Falkenrath, Richard A. "From Bullets to Megabytes." *New York Times, The (NY)*. Accessed January 1, 2028. http://www.nytimes.com/2011/01/27/opinion/27falkenrath.html?_r=1.

Farwell, James P., and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." *Survival (00396338)* 53 (2011): 23–40. https://doi.org/10.1080/00396338.2011.555586.

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

Flood, John, and Lachlan Robb. "Trust, Anarcho-Capitalism, Blockchain and Initial Coin Offerings." *SSRN Electronic Journal*, December 6, 2017. https://doi.org/10.2139/ssrn.3074263.

Foucault, Michel. *Discipline & Punish: The Birth of the Prison*. Vintage. Knopf Doubleday Publishing Group, 2012.

Fowler, Kevvie. *Data Breach Preparation and Response*, 2016.

Gargano, Francesca. "Three Common Threat Actors and the One You Might Not Know About." https://www.lookingglasscyber.com, 2019. https://www.lookingglasscyber.com/blog/three-common-threat-actors-and-the-one-you-might-not-know-about/.

Geers, Keneth. *Strategic Cyber Security*. Tallinn: NATO CCD COE Publication, 2011.

Gf. "Onet.Pl: Deputy Justice Minister behind Campaign to Discredit Judges," 2019.

Gibson, William. "Burning Chrome." *Omni*. Omni, July 1982. http://www.voidspace.org.uk/cyberpunk/burning_chrome.shtml#burning.

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

Glaser, Stefan. "Nullum Crimen Sine Lege." *Journal of Comparative Legislation and International Law* 24, no. 1 (1942): 29–37.

Goldman, Zachary K. "Terrorism 2.0? New Challenges in Cyberspace." *Georgetown Journal of International Affairs*, 2015.

Golf-Papez, Maja, and Ekant Veer. "Don't Feed the Trolling: Rethinking How Online Trolling Is Being Defined and Combated." *Journal of Marketing Management* 33, no. 15–16 (October 2017): 1336–54. https://doi.org/10.1080/0267257X.2017.1383298.

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

Gorwa, Robert. "Computational Propaganda in Poland: False Amplifiers and the Digital Public Sphere." Working Paper No. 2017.4, 2017.

Green, James A. *Cyber Warfare*. Abingdon, UK: Routledge, 2015.

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

Greer, Steve. "'Balancing' and the European Court of Human Rights : A Contribution to the Habermas-Alexy Debate Author (s): Steven Greer Source : The Cambridge Law Journal , Vol . 63 , No . 2 (Jul ., 2004), Pp . 41." *The Cambridge Law Journal* 63, no. 2 (2004): 412–34.

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

Guzman, Andrew. "The Consent Problem in International Law Permalink." *UC Berkeley Berkeley Program in Law and Economics, Working Paper Series*, 2011.

Hardaker, Claire. "'Uh. . . . Not to Be Nitpicky,,,,,But…the Past Tense of Drag Is Dragged, Not Drug.': An Overview of Trolling Strategies." *Journal of Language Aggression and Conflict* 1, no. 1 (2013): 58–86. https://doi.org/10.1075/jlac.1.1.04har.

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

Herring, Susan, Kirk Job-Sluder, Rebecca Scheckler, and Sasha Barab. "Searching for Safety Online: Managing 'Trolling' in a Feminist Forum." *The Information Society* 18, no. 5 (October 2002): 371–84. https://doi.org/10.1080/01972240290108186.

Holcombe, Randall G. "Common Property in Anarcho-Capitalism." *Journal of Libertarian Studies* 19, no. 2 (2005): 3–29.

Hughes, Rex. "A Treaty for Cyberspace." *International Affairs* 86 (2010): 523–541. https://doi.org/10.1111/j.1468-2346.2010.00894.x.

Human Rights Council. “Report of the Special Rapporteur on the Right to Privacy, A/HRC/37/62,” 2018.

———. “The Right to Privacy in the Digital Age Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/27/37,” no. June (2014).

Human Rights Watch, and Powers Not. “France : New Emergency Powers Threaten Rights,” 2015.

Iansiti, Marco, and Karim R. Lakhani. “The Truth about Blockchain.” *Harvard Business Review*, 2017.

ICJ. Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits (1986).

———. Corfu Channel Case (United Kingdom v. Albania); Merits (1949).

Inkster, Nigel. “China in Cyberspace.” *Survival* 52, no. 4 (November 2010): 55–66. https://doi.org/10.1080/00396338.2010.506820.

International Court of Justice. “Case Concerning the Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain), Judgment of 5 February 1970,” 1970.

International Telecommunication Union. “An Agenda for Change, A Global Strategy,” n.d.

Interntional Law Commission. Text of the draft articles on Responsibility of States for internationally wrongful acts as part of the International Law Commission Report, A/56/10 August 2001 (2001).

INTERPOL. “Global Cybercrime Strategy,” 2017.

———. “Investigative Support for Cybercrime,” n.d.

———. “Our Seven Global Policing Goals Shape How the Law Enforcement Community Works Together to Create a Safer World,” n.d.

———. “The Strategic Framework 2017-2020,” n.d.

Jasanoff, Sheila. *States of Knowledge: The Co-Production of Science and Social Order*. Routledge, 2004.

Jeff Shantz, Jordon Tomblin. *Cyber Disobedience: Re-Presenting Online Anarchy*. Hants: Zero Books., 2013.

Jennings, Robert, and Sir Arthur Watts. *Oppenheim’s International Law : Volume 1 Peace*. Oxford University Press, 2008. https://doi.org/10.1093/law/9780582302457.001.0001.

Jensen, Eric Talbot. “The Tallinn Manual 2.0: Highlights and Inisghts.” *Georgetown Journal of International Law* 43, no. 3 (2017): 735–78.

Jervis, Robert. “Mutual Assured Destruction.” *Foreign Policy*, no. 133 (2002): 40. https://doi.org/10.2307/3183553.

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

Jussinoja, Terho. “LIFE-CYCLE OF INTERNET TROLLS.” UNIVERSITY OF JYVÄSKYLÄ, 2018.

Kaiser, Robert. “The Birth of Cyberwar.” *Political Geography* 46 (2015): 11–20.

Kallberg, Jan, and Bhavani Thuraisingham. “State Actors’ Offensive Cyberoperations: The Disruptive Power of Systematic Cyberattacks.” *IT Professional* 15, no. 3 (May 2013): 32–35. https://doi.org/10.1109/MITP.2013.20.

Kampmark, Binoy. “Cyber Warfare Between Estonia And Russia.” *Contemporary Review* 289 (2007): 288–93.

Kaspersky. “What Is an Advanced Persistent Threat (APT)?,” n.d.

Kaspersky Lab. “What Is Metamorphic Virus?” Accessed August 28, 2019. https://www.kaspersky.com/resource-center/definitions/metamorphic-virus.

Kellner, Douglas. *Media Culture: Cultural Studies, Identity and Politics between the Modern and the Postmodern*. London and New York: Routledge, 1995.

Kelly, Brian B. “Investigating in a Centralized Cybersecurity Infrastructure: Why ‘Hacktivism’ Can and Should Influence Cybersecurity Reform.” *Boston University Law Review* 92, no. 5 (2012): 1663–1711.

Kiesnoski, Kenneth. "5 of the Biggest Data Breaches Ever." cnbc.com2, 2019. https://www.cnbc.com/2019/07/30/five-of-the-biggest-data-breaches-ever.html.

Kirsch, Cassandra M. "Science Fiction No More: Cyber Warfare And The United States." *Denver Journal of International Law & Policy* 40 (2012): 620–47.

Klein, John J. "Deterring and Dissuading Cyberterrorism." *Journal of Strategic Security* 8, no. 4 (2015).

Koenders, Bert. "Foreword." In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., xxv–xxvii. Cambridge: Cambridge University Press, 2017. https://doi.org/DOI: undefined.

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

Korzak, Elaine. "International Law and the UN GGE Report on Information Security." Just Security, 2015.

Krahmann, Elke. *States, Citizens and the Privatisation of Security*. New York: Cambridge University Press, 2010.

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

Kristin, M. Lord, and Travis Sharp, eds. *America's Cyber Future Security and Prosperity in the Information Age Volume Ii*, 2011.

Kuehl, Daniel. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 35:24–42. Potomac Books, 2013.

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.

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

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

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.

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

Libicki, Martin. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press, 2007.

Lohrman, Dan. "Hacking For Cause: Today's Growing Cyber Security Trend," 2015.

Lucas, Edward. "Why We Are Not Ready for Cyberwar." *The Security Times - The Special Edition of the Atlantic Times for the 51th Munich Security Conference*, no. February (2015).

Lucas, Edward, and Peter Pomerantsev. *Defending and Ultimately Defeating Russia's Disinformation Techniques. Recommendatins. A Report by CEPA's Information Warfare Project in Partnership with the Legatum Institute*. Center for European Policy Analysis, 2016.

Ludlow, Peter. *Crypto Anarchy, Cyberstates, and Pirate Utopias*. Cambridge, Massachusetts and London, England: MIT Press, 2001. https://doi.org/10.1108/14636690232094299 5.

Lyall, Nicholas. "China's Cyber Militias." *The Diplomat*, March 2018.

Lyon, David. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society* 1, no. 2 (2014): 205395171454186. https://doi.org/10.1177/2053951714541861.

Magal, Paula. “WHO ARE THE HACKTIVISTS?,” 2019.

Mälksoo, Maria. “Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of the EU and NATO.” *European Security* 27, no. 3 (2018): 374–92. https://doi.org/10.1080/09662839.2018.1497984.

Mansfield-Devine, Steve. “Hacktivism: Assessing the Damage.” *Network Security* 2011, no. 8 (August 2011): 5–13. https://doi.org/10.1016/S1353-4858(11)70084-8.

Marion, Nancy. “The Council of Europe’s Cyber Crime Treaty: An Exercise in Symbolic Legislation.” *International Journal of Cyber Criminology* 4, no. 1/2 (2010): 699.

“Mark Zuckerberg Calls for Stronger Regulation of Internet.” The Guardian, 2019. https://www.theguardian.com/technology/2019/mar/30/mark-zuckerberg-calls-for-stronger-regulation-of-internet.

May, Timothy C. “The Crypto Anarchist Manifesto.” In *Crypto Anarchy, Cyberstates, and Pirate Utopias*, edited by Peter Ludlow, 61–63. Cambridge, Massachusetts and London, England: MIT Press, 2001.

McAfee. *Virtual Criminology Report 2009: Virtually Here: The Age of Cyber Warfare*. Santa Clara, CA, USA: McAfee, 2009. www.mcafee.com.

McCallion, Jane. “Anti-Isis Hacktivists Compromise Terrorists’ Website | IT PRO.” *ITPro*, 2017.

Melnitzky, Alexander. “Defending America Against Chinese Cyber Espionage Through The Use Of Active Defenses.” *Cardozo Journal of International & Comparative Law* 20 (2012): 537–70.

Melzer, Nils. “Cyberwarfare and International Law,” 2011. http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

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

MI5. “Cyber.” Security Service, 2019.

Morris, Laura C. “Contextualizing the Power of Social Media: Technology, Communication and the Libya Crisis.” *First Monday* 19, no. 12 (2014): 1. https://doi.org/10.5210/fm.v19i12.5318.

Mshvidobadze, K. “State-Sponsored Cyber Terrorism: Georgia’s Experience.” *Presentation to the Georgian Foundation for Strategic and International Studies*, 2011.

Murphy, Hannah, and Madhumita Murgia. “Chinese Hacker Group That Works for Both Beijing and Personal Gain Identified.” Financial Times, 2019. https://www.ft.com/content/965ceffc-b8ea-11e9-8a88-aa6628ac896c.

Nakamoto, Satoshi. “Bitcoin : A Peer-to-Peer Electronic Cash System,” 2008, 1–9.

National Academy of Sciences (NAS). *Computer Science and Telecommunications Board: Computers at Risk: Safe Computing in the Information Age*. Washington D.C.: National Academies Press, 1991.

NATO. “Cyber Defence Pledge,” 2016.

———. “NATO Cyber Defence,” 2019.

———. “Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.” Lisbon, 2010. http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf.

———. “Wales Summit Declaration.” Press Release 120, September 5, 2014. http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

———. “Warsaw Summit Communiqué,” no. July (2016): 1–30.

NCTA. “How Google Tracks Traffic.” National Cable & Telecommunications Association, 2014. https://www.ncta.com/platform/broadband-internet/how-google-tracks-traffic/.

Nicolas Falliere, Liam O Murchu, and and Eric Chien. “W32.Stuxnet Dossier.” Cupertino, 2012. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Nicoll, Alexander. “Stuxnet: Targeting Iran’s Nuclear Programme.” *Strategic Comments* 17 (2011): 1–3.

https://doi.org/10.1080/13567888.2011.575612.

O'Flaherty, Kate. "Cyber Warfare: The Threat From Nation States," 2018.

Ohlin, David, Kevin Govern, and Claire Finkelstein Oxford. "Nicolò Bussolati ' The Rise of Non-State Actors in Cyberwarfare ,'" 2015.

Organization of African Unity. African Charter on Human and Peoples Rights (1981).

Organization of American States. American Convention on Human Rights (1969).

OSCE. *Freedom of Expression on the Internet: A Study of Legal Provisions and Practices Related to Freedom of Expression, the Free Flow of Information and Media Pluralism on the Internet in OSCE Participating States*, 2012.

Ottis, Rain. "Proactive Defense Tactics against On-Line Cyber Militia." In *ECIW2010-Proceedings of the 9th European Conference on Information Warfare and Security*, 2010.

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

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

Palfrey, John, and Jonathan Zittrain. "Access Denied: The Practice and Policy of Global Internet Filtering - Book Review." *Oxford Internet Institute, Research Report*, 2007. https://doi.org/10.1109/tpc.2009.2032378.

PCIJ. S.S. Lotus (Fr. v. Turk.) (1927).

Pennycook, Gordon, and David G. Rand. "Who Falls for Fake News? The Roles of Analytic Thinking, Motivated Reasoning, Political Ideology, and Bullshit Receptivity." *SSRN Electronic Journal*, 2017. https://doi.org/10.2139/ssrn.3023545.

Perrow, Charles. *Normal Accidents: Living with High-Risk Technologies*. Princenton: Princeton University Press, 1984.

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

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

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

Pompon, Ray. "Doxing, DoS, and Defacement: Today's Mainstream Hacktivism Tools." *Application Threat Intelligence*, 2017.

Post, Robert C. "Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere." *Duke Law Journal* 67, no. 5 (2018): 981–1072.

"Proactive Defense: Understanding the 4 Main Threat Actor Types," n.d.

Puglisi, William C. Hannas James Mulvenon Anna B. *Chinese Industrial Espionage*. Routledge, 2013.

Ranger, Steve. "The New Art of War: How Trolls, Hackers and Spies Are Rewriting the Rules of Conflict." techrepublic.com, 2016. http://www.techrepublic.com/article/the-new-art-of-war-how-trolls-hackers-and-spies-are-rewriting-the-rules-of-conflict/.

Rappaport, David. "The Four Waves of Rebel Terror and September 11." *Anthropoetics 8*. Department of Political Science, University of California at Los Angeles, 2002. http://www.anthropoetics.ucla.edu/ap0801/terror.htm.

Raytheon. "A Field Guide to Hackers," 2019.

Reid, Fergal, and Martin Harrigan. "An Analysis of Anonymity in the Bitcoin System." In *Security and Privacy in Social Networks*, 1–28, 2013. https://doi.org/10.1007/978-1-4614-4139-7_10.

Richards, Imogen, and Mark A. Wood. "Hacktivists against Terrorism: A Cultural Criminological

Analysis of Anonymous' Anti- IS Campaigns." *International Journal of Cyber Criminology* 12, no. 1 (2018): 187–205. https://doi.org/10.5281/zenodo.1467895.

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.

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

Samadashvili, Salome. "Muzzling the Bear Muzzling the Bear. Strategic Defence for Russia's Undeclared Information War on Europe." Brussels, 2015.

Sandmeier, Claudio. "Cybercrime Akteure," 2018.

Sanger, D E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. Crown Publishing Group, 2012.

Schaake, Marietje. "A Rules-Based Order to Keep the Internet Open and Secure." *Georgetown Journal of International Affairs*, 2018.

Schjolberg, Stein. *The History of Cybercrime: 1976-2014*. Books on Demand, 2014.

Schjølberg, Stein, and Amanda M. Hubbard. "Harmonizing National Legal Approaches on Cybercrime." *WSIS Thematic Meeting on Cybersecurity Background Paper*, no. June (2005).

Schmidt, Nikola. "A Sociological Approach to Cyberspace Conceptualization and Implications for International Security." In *Perspectives on Cybersecurity*, edited by Jakub Drmola, 70–77. Brno: Muni Press, 2015.

———. "Critical Comments on Current Research Agenda in Cyber Security." *Defense and Strategy* 14, no. 1 (2014): 29–38. https://doi.org/10.3849/1802-7199.14.2014.01.029-038.

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

———. "The Birth of Cyber as a National Security Agenda (PhD Thesis)." Charles University, 2016.

Schmitt, Michael N. "Due Diligence." In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., 30–50. Cambridge: Cambridge University Press, 2017. https://doi.org/DOI: 10.1017/9781316822524.008.

———. "International Human Rights Law." In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., 179–208. Cambridge: Cambridge University Press, 2017. https://doi.org/DOI: 10.1017/9781316822524.012.

———. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." *Harv. Int'l L.J. Online* 54 (2012). http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/.

———. "Jurisdiction." In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., 51–78. Cambridge: Cambridge University Press, 2017. https://doi.org/DOI: 10.1017/9781316822524.009.

———. "Prohibition of Intervention." In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., 312–27. Cambridge: Cambridge University Press, 2017. https://doi.org/DOI: 10.1017/9781316822524.019.

———. "Sovereignty." In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., 11–29. Cambridge: Cambridge University Press, 2017. https://doi.org/DOI: 10.1017/9781316822524.007.

———. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., i–ii. Cambridge: Cambridge University Press, 2017. https://doi.org/DOI: undefined.

———. "The Use of Force." In *Tallinn Manual 2.0 on the International Law Applicable to Cyber*

Operations, 2nd ed., 328–56. Cambridge: Cambridge University Press, 2017. https://doi.org/DOI: 10.1017/9781316822524.020.

Sear, Tom, and Michael Jensen. "Russian Trolls Targeted Australian Voters on Twitter via #auspol and #MH17," 2018.

Security, Canadian Centre for Cyber. "Cyber Threat and Cyber Threat Actors," 2018.

———. "Cyber Threat and Cyber Threat Actors," 2018. https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors.

Seffers, George I. "Cyber Militia Launches Nonprofit to Share Technology." *SIGNAL AFCEA*, 2019.

Segal, Adam. "The Rise of Asia's Cyber Militias." The Atlantic, 2012.

Shachaf, Pnina, and Noriko Hara. "Beyond Vandalism: Wikipedia Trolls." *Journal of Information Science* 36, no. 3 (June 2010): 357–70. https://doi.org/10.1177/0165551510365390.

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

Shackelford, Scott J, Scott Russell, Andreas Kuehn, Scott J ; Shackelford, and Scott ; Russell. "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors." *Chicago Journal of International Law* 17, no. 1 (2016): 7–8.

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

Sicari, S., A. Rizzardi, L. A. Grieco, and A. Coen-Porisini. "Security, Privacy and Trust in Internet of Things: The Road Ahead." *Computer Networks* 76 (2015): 146–64. https://doi.org/10.1016/j.comnet.2014.11.008.

Sigholm, Johan. "Non-State Actors in Cyberspace Operations." *Journal of Military Studies* 4, no. 1 (2016): 1–37. https://doi.org/10.1515/jms-2016-0184.

Simma et al. *The Charter of The United Nations 3E, Vol 1*. Oxford University Press, 2013. https://doi.org/10.1093/law/9780199639762.001.0001.

Snegovaya, Maria. "Putin's Information Warfare in Ukraine," no. September (2015): 28.

Sorell, Tom. "Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous." *Journal of Human Rights Practice* 7, no. 3 (2015): 391–410.

States, League of Arab. "Arab Convention on Combating Information Technology Offences," 2010.

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

Tao, Ai Lei. "Nation-State Actors Responsible for Most Cyber Attacks," 2017.

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

The Secretary-General of the United Nations. "An Agenda for Disarmament," 2018.

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

———. "Over to the Dark Side." *10th June*, 2013.

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

———. "The Terrorist in the Data." *28th November*, 2015.

———. "Uber Is Now More Popular than Taxis or Car Rental with Business People." *22nd January*, 2015.

———. "Unfriended." *12th December*, 2015.

Theohary, Catherine A., and John W. Rollins. "Cyberwarfare and Cyberterrorism: In Brief," 2015.

TheWhiteHouse. "International Strategy for Cyberspace," 2011.

http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

———. “The National Strategy to Secure Cyberspace.” Washington, DC., 2003.

Thompson, Jeff. “DNS Cache Poisoning Part 2.” alienvault.com, 2019. https://www.alienvault.com/blogs/security-essentials/dns-cache-poisoning-part-2-1.

Tung, Liam. “Microsoft Signs Deal to Let NATO Check Its Products for Backdoors.” *Zdnet.Com*, September 25, 2015. http://www.zdnet.com/article/microsoft-signs-deal-to-let-nato-check-its-products-for-backdoors/.

Unauthored. “Biggest Cybertheft in History Hits Banks.” *WND*, February 16, 2015. http://www.wnd.com/2015/02/biggest-cyber-theft-in-history-hits-banks/.

United Nation General Assembly resolution 2625 (XXV). Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, A/RES/2625 (XXV), (24 October 1970) (n.d.).

United Nation General Assembly resolution 68/168. The right to privacy in the digital age, A/RES/68/167 (18 December 2013) (2013).

United Nations. “Human Rights,” n.d.

———. “International Covenant on Civil and Political Rights by General Assembly Resolution 2200A (XXI) of 16 December 1966,” 1966.

United Nations General Assembly. “Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/C.1/73/L.37 (18 October 2018),” 2018.

———. “Combating the Criminal Misuse of Information Technologies, A/RES/56/121,” 2002.

———. “Combating the Criminal Misuse of Information Technologies A/RES/55/63,” 2001.

———. “Constitution of the ICPO-INTERPOL,” 1956.

———. “Developments in the Field of Information and Telecommunications in the Context of International Security, A/C.1/73/L.27/Rev.1 (29 October 2018),” 2018.

———. “First Report of the UN Special Rapporteur on the Right to Privacy to the Human Rights Council, A/72/540,” 2017.

———. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 12404 § (2015).

United Nations General Assembly Resolution 53/79. “Developments in the Field of Information and Telecommunications in the Context of International Security, /A/RES/53/70 (4 January 1999),” 1999.

United Nations General Assembly Resolution 68/69. “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98 (24 June 2013),” 2013.

United Nations Human Rights Committee. “International Covenant on Civil and Political Rights, General Comment No. 34, CCPR/C/GC/34,” 2011.

———. “The Promotion, Protection and Enjoyment of Human Rights on the Internet,A/HRC/38/L.10/Rev.1,” 2018.

United Nations Human Rights Office of the High Commissioner. “Freedom of Expression Everywhere, Including in Cyberspace,” 2011.

———. “Special Rapporteur on the Right to Privacy,” n.d.

———. “The Right to Privacy in the Digital Age,” n.d.

United Nations Office for Disarmament Affairs. “Developments in the Field of Information and Telecommunications in the Context of International Security,” n.d.

United Nations Office on Drugs and Crime. “Global Programme on Cybercrime,” n.d.

———. “International Cooperation in Criminal Matters: Counter-Terrorism,” 2007.

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

Waever, Ole. *Securitization and Desecuritization*. Centre for Peace and Conflict Research Copenhagen, 1993.

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

Watts, Sean, and Theodore Richard. "Baseline Territorial Sovereignty and Cyberspace." *Lewis & Clark Law Review* 22, no. 3 (2018): 803–72.

Weathers, Cliff. "NSA's Massive Cyber-Spying Efforts Called 'Superhuman.'" *AlterNet*, February 17, 2015. http://www.alternet.org/civil-liberties/nsas-superhuman-cybersurveillance-network-exposed.

Weber, Amalie M. "The Council of Europe's Convention on Cybercrime." *Berkeley Technology Law Journa* 18, no. 1 (2003): 425–46.

Westby, Jody R. *International Guide to Cyber Security*. American Bar Association, 2005.

Westwood, Sallie. *Imagining Cities: Scripts, Signs, Memory*, 1997. https://doi.org/10.4324/9780203397350.

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

Wiemann, Gabriel. "Cyberterrorism: How Real Is the Threat?" Washington, D.C., 2004. www.usip.org/sites/default/files/sr119.pdf.

Wilczek, Marc. "Cybersicherheit: Hartes Jahr Für Die IT-Security-Teams Der Banken – Und Entwarnung Ist Nicht in Sicht." IT Finanz magazin, 2019. https://www.it-finanzmagazin.de/cybersicherheit-hartes-it-security-banken-88529/.

Williams, Phil, and Dighton Fiddner. *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition*. Strategic Studies Institute (U.S.), 2016.

Winder, Davey. "Boundaries between Nation-State and Criminal Actors More Blurred than Ever." *SCMagazineUK.Com*, 2018.

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

Wodak, Ruth. *The Politics of Fear*. SAGE Publications, 2015.

Wright, Jeremy. "Cyber and International Law in the 21st Century (Speech)." 2018.