EU CYBERSECURITY STRATEGY:

SECURITIZATION OF CYBERSPACE THROUGH A RHETORICAL LENS

By

Fran Stojaković

Submitted to

Central European University

Department of International Relations

In partial fulfilment of the requirements for the degree of Master of Arts

Supervisor: Professor Michael Merlingen

Word Count: 17 213

Budapest, Hungary

2018

Abstract

The advancement of information technologies has led to dissemination of security aspects needed to be addressed correspondingly. EU strives to build-up its cyber identity, a security realm which has become a profound expression of national interests, thus posing challenge to these supranational aspirations. Impediments of easier path to securitize cyberspace stand in a way, but can they be overcome?

This research adds to the literature focusing on EU actors dealing with cybersecurity, whether that be imposing vehement measures or influencing decision-makers in the securitization process. Taken initiatives embodied in political rhetoric are taken as an evaluation of creating (in)efficient cybersecurity strategy.

Acknowledgments

I would like to give my special gratitude to my supervisor, Professor Michael Merlingen for his continuous support and guidance, constructive criticism and encouraging feedbacks.

I am thankful for words of encouragement from my friends as well as understanding and empathy through all those sleepless nights from my girlfriend.

Most importantly, my expressions of love go to my sister and parents for having my back both at the Central European University and throughout my previous personal and professional development.

TABLE OF CONTENTS

Introduction

"*Now, it can reach our economies, it can reach our personal lives. It can reach our democracies. It is important there are concrete steps forward, so there is a common approach, better coordination to reinforce confidence for citizens and industries in member states*".
- Mariya Gabriel, European Commissioner for Digital Economy and Society

Internet has become not only a source of information, but a platform through which people do business, advertise, communicate and perform financial transactions. The internet has never been constructed to "track and trace the behavior of users", but to "link autonomous computers for resource sharing".[1] Alongside its abundant benefits, is serves as a platform for hackers as much as terrorists to gather information, recruit new people, and motivate or fund attacks. Cybersecurity is a vital part of individual's financial security as it protects the information that can affect "personal financial status".[2] Moreover, it is beneficial if each user knows how to protect himself from identity theft or online fraud, for it enhances the reliability and safety of cyber environment. In addition, businesses experience lack of resources and skills needed to tackle challenges. Consequently, it is more common to notice efforts of some countries and organizations in presenting permanent solutions or ambitious agendas. However, numerous frameworks and technologies, policies and ideas are arguably efficient in the long term. People tend to oversee or simplify some of the approaches needed for adequate cybersecurity strategy because of the fear of losing trade secrets or trying to reduce financial and reputation loss.[3] Government sector, on the other hand, owns a

[1] Goutam, R. (2015) 'Importance of Cyber Security' International Journal of Computer Applications, Volume 111, No. 7 Available at: https://pdfs.semanticscholar.org/5cfb/7a5bd2e6c181e8a69ebd49b1dadb795f493b.pdf (Accessed May 10, 2018)
[2] Ibid.
[3] Meyer, C. (2017) 'Measuring the Impact of Cyberattacks: Lost Revenue, Reputation & Customers) Available at: https://www.securitymagazine.com/articles/87778-measuring-the-impact-of-cyberattacks-lost-revenue-reputation-customers (Accessed May 10, 2018)

large amount of data and confidential information that are still number one target in the eyes of 'hacktivists'.

The term 'cyberspace' was invented in 1984 by the sci-fi novelist William Gibson, and it is safe to say that he certainly did not expect that this prominent academic metaphor would become a subject of study in further analysis of security field.[4] Cyberspace has become an unforeseeable dynamic environment with a potential to greatly influence the security of states. The threats that have emerged from a cyberspace are to be expected from both state and non-state source due to an "increasing interconnection of security trends and factors".[5] Recognizing the importance to address cyber threats and reduce their hostile effects, the European Union has started to develop a complex approach towards the cyber concerns. The harmony of the security environment has been shaken up by the intentions and means of new global actors. For these reasons, nation states decide to join larger alliances and supranational entities for having assurance of security and protection. Threats beyond the borders of the EU may have a direct impact on the security within the Union wherein core founding principles could be endangered. With this notion in mind, the Union has begun to thoroughly study the importance of cyberspace and empower its role of a cybersecurity actor by combating common threats and protecting its critical infrastructure for the sake of the EU citizens. The relevant actors along with institutions in charge of cyber matters acknowledged the challenges of information technology era and decided to act upon by assisting the progress of principles and instructions which together frame cybersecurity strategy; a crucial element of compliance with the concerns of citizens and challenges of dynamic security environment.

[4] Mazzini, F. (2014) 'Cyber-Cultural History: Some Initial Steps toward a Cultural History of Digital Networking', Universita di Padova, Humanities 2014, 3, 203

[5] Podhorec, M. (2012) 'Cyber security within the globalization process', Journal of defense Resources Management, Vol. 3, Issue 1., 1

Research Question(s) and Thesis Statement

"*Who are the actors who seek to securitize cyberspace and what arguments/frames do they use to achieve it?"*

"What are the obstacles that have prevented EU-level actors to give the EU a more significant role in cybersecurity?

This thesis attempts to offer plausible answers to these research questions by analyzing discourse of securitizing actors, their interests as well as their actions. The notion of cybersecurity is firstly being put in a wider context whereas transition between cyber enthusiasm and cyber criticism is being made. Consequently, the securitization theory of the Copenhagen School is applied upon the EU efforts to securitize cyberspace. The assumption of this thesis is that the securitization theory is applicable to the ongoing securitization process in the EU and has shown that the actors expressed their intentions by proposing policies, enacting laws, establishing institutions and enhancing cooperation on EU level for the process of securitization to be successful. In addition to the main question, the research has raised one sub-question that built up findings of this thesis.

This sub-question comprises:

- *How efficient are the efforts at EU level in comparison with the United States, a country where securitization of cyberspace has been successfully managed?*

Methodology

This qualitative research will deeply penetrate into the core reasonings provided by the relevant actors on the EU level by which they seek to depict cyberspace as a threatening realm of security. It starts off by overviewing historical context whereby cyber gradually becomes a subject of skepticism, and criticism consequently. *Wired* magazine along with other articles from the early 1990s serve as sources of cyber-enthusiasm that progressively vanishes away. Its transnational character and large-scale influence have turned it into a priority of political and security agendas. This is a turning point when it meets the securitization theory of the Copenhagen School. This research heavily relies on this theory and its components, thoroughly elaborated by Buzan et al. in

'Security: A New Framework for Analysis'. These respectable scholars reconceptualized security paradigm and opened up a debate within the School. In addition, Didier Bigo of the Paris School introduced the alternative method to approach securitization, focusing on routinized practices in his 'Security and Immigration: Towards a Critique of the Governmentality of Unease' which is a crucial component of this empirical study, and thus taken into account for further analysis. Therefore, an extensive literature review is provided to see matters from different perspectives. However, succeeding section introduces notable scholars who securitized cyberspace, a field securitized never before. Hansen and Nissenbaum assert the elements needed to be analyzed for having a complete securitization success, encouraging thus other scholars to deal with this field, and allowing students such as myself to apply these elements in empirical cases. Discourse analysis follows through wherein the theory is being applied. The discourse analysis looks at initiatives and proposals of the actors on EU level. The last subsection puts the EU securitization efforts into a comparative analysis with the US, for it enables to form a perception of success/failure of securitization, thus adding weight to its academic value.

Structure

The argumentation of this thesis is structured into four chapters: a historical overview of the initial cyber connotations, literature review of the cyberspace securitization, ongoing securitization in Brussels with its solutions and limitations and, lastly, long-term consequences that have emerged from the efforts to securitize cyber. The first chapter titled "Cyber: From Promise to Threat" gives a brief historical glimpse of the promising notions on cyber from the times of its appearance with regards to the societal and technological contexts, and the gradual development of skeptical views, some of which turned into critical ones. The successive chapter on "Cyberspace: Theoretical Perspective" provides a literature review on the securitization theory as well as the securitization

of cyberspace. It enables this research to be put into wider debate and signifies a gap in the literature on cyber securitization and counter-measures at the EU level. The third and most extensive chapter titled "Securitizing Cyber in Brussels" contains a discourse analysis of securitizing actors wherein their intentions and solutions are being identified and positioned within the theory. Moreover, this chapter sets up the limitations of further securitization and elaborates upon the elements of proposed cybersecurity strategy. The fourth and final chapter named "Aftermath: Effects of Cyber Securitization" presents outcomes of adequate cyber securitization, namely cyber identity building, and places the EU in comparison with the US; shortcomings of the EU side in contrast to the efficient cybersecurity strategy that has taken place across the Atlantic.

1. CYBER: FROM PROMISE TO THREAT

1.1. Cyber Forecast: Promising Beginnings

Cooperation between a man and computer, as seen from the perspective of one of the most innovative minds in computer science history, J.C.R. Licklider, was elucidated as a key to the development of future. One of his initial ideas underlined the importance of computers to be designed in a manner to "enable men and computers to cooperate in making decisions and controlling complex situations".[6] Increasingly fast innovation in information technology era over the course of past few decades brought revolution to the production and consumption of information wherein people are the ones who have wider access to information goods, enabled by the advancement of tools that compose significant share of cyberspace.[7] The biggest shift in the perception of home computing was brought along in the 1980s when computers were presented as a technology made to 'change the world'. Having these 'electronic brains' inside your home was a matter prescribed to science fiction and personal computing was limited to use only for tech-savvy enthusiasts.[8] Not long after that, society has begun to perceive that these wonders of information technology have the capacity to initiate a revolution in people's lives. As soon as the mainstream media realized how important and advanced are the things happening online, news about the internet were overflowing the society. One of the New York Times' report from 1994 was not different in any other way: "Increasing commercialization of the Internet will accelerate

[6] Bygrave, Lee A., and Jon Bing. 'Building cyberspace: a brief history of Internet', Oxford University Press, (2017). 32-37

[7] Jonnalagedda, Sreelata. 'Revenue generation in the information era: Opportunities and challenges', IIMB Management Review, (2011). 51-56

[8] Lean, T. (2016) 'Electronic Dreams: How 1980s Britain Learned to Love the Computer', Bloomsbury. Available at: https://www.historyextra.com/period/20th-century/a-brave-new-world-the-1980s-home-computer-boom/ Accessed May 15, 2018

its transformation away from an esoteric communications system for American computer scientists and into an international system for the flow of data, graphics, sound and video among businesses, their customers and their suppliers".[9] To illustrate the importance of cyber and frame of mind from the early 1990s, the following paragraph will be devoted to portraying the content of first editions of Wired magazine, whose objective is to clarify how emerging technologies affect the society.

Initial edition of Wired dealt with the new possibilities for the cyber future, implicating how technology has more to offer than just entertainment; as such it was a tool meant to liberate and enlighten.[10] Wired was a product of its era aspirations, socially transformative tool and proof of a time within which people had high hopes and expectations from cyber. Before the mass acceptance of the internet, Wired offered promising outlook, indicating how the electronic technology will reshape the way humans interact with one another and transform perception of known society.[11] The importance of cyber and the assumption of its relevance in shaping culture of the future was presented on the first pages wherein the founder of Wired indicated the mission of the magazine, that is to "discuss the meaning or context of social changes so profound that their only parallel is probably the discovery of fire".[12] In alignment with displaying such ambitious goal, magazine's intent was to intrigue the reader in perceiving "the soul of new society in wild metamorphosis".[13] Society was entering an era of improved communication, a period of coexistence between the New Economy capitalism and the technological revolution, in which the success of internet can be

[9] Singer, P.W. and Friedman, A. (2014) 'Cybersecurity and Cyberwar – What everyone needs to know', Oxford University Press, New York., 20-21

[10] Wiener, A. (2018). 'On Reading Issues of Wired from 1993 to 1995.' [online] The New Yorker. Available at: https://www.newyorker.com/culture/cultural-comment/on-reading-issues-of-wired-from-1993-to-1995 [Accessed 2 Mar. 2018].

[11] Raile, D. (2014). 'A look back at the first issues of Wired prompts the question: How far have we come?.' [online] Pando. Available at: https://pando.com/2014/07/15/a-look-back-at-the-first-issues-of-wired-prompts-the-question-how-far-have-we-come/ [Accessed 8 Mar. 2018].

[12] Ibid.

[13] Ibid.

prescribed to the openness of its character, where the people began to wonder how to assimilate to internet as much as how to integrate technology into their lives.[14]

The rapid advance of the US economy between 1995 and 1999 was nothing less than remarkable. High-tech revolution that spread throughout the business sector in the late 1990s led to growth of labor productivity and rise of gross domestic product at an annual rate of more than 4 percent.[15] American private sector has been furiously investing in information technology in order to reduce costs, to enhance and provide new forms of services and to have an efficient coordination of 'large-scale operations'. Many experts at that time believed that the productivity growth would be even more apparent which goes in favor of the claim how cyber-enthusiasm was a predominant notion of the 1990s, and how aspirations of that era were somewhat unrealistic and too optimistic. Stanford graduates, Page and Brin, founded Google in 1998 and introduced the world to search engines which was a major leap towards a new way of communication, entertainment and education. More importantly, the first IMP; first generation of gateways, today known as routers, was mounted at UCLA and is nowadays considered as the beginning of a cyberspace phenomenon.[16] In other words, emergence of the space of information delivered a different viewpoint on the knowledge and facts, as infinite as the human imagination. The revolution of technology generated the innovation of products that adapt to consumers. Simultaneously, lowering the cost of reproduction had stimulated proliferation of information, whereas the evolution of communication technologies facilitated smoother information sharing.[17] After

[14] Wiener.
[15] Oliner, S. and Sichel, D. (2000) 'The Resurgence of Growth in the Late 1990s: Is Information Technology the Story?', Journal of Economic Perspectives 14, no. 4, 1-3
[16] Bygrave and Bing. 36
[17] Jonnalagedda. 52

implying that the internet had inevitably enhanced the way of communication, connectivity and market externalities, it is time to gaze at the flip side of the coin.

As the society became more entangled with the internet and its features, the opportunities of technological development became more expanded, but so did the challenges. The proponents of cyber skepticism became more evident; arguing that society which is becoming more dependent on technology must bear in mind that there is more to cyber than just taking advantage of its great benefits.[18] By the opportunist character of cyberspace, it by itself became a platform for execution of cyber-attacks, industrial espionage and cybercrime. Experts and analysts progressively realized the necessity for cooperation in the field of mitigating attacks along with the exigency for awareness and education, emphasizing the lack of leadership as a key challenge in recognizing and taking precautionary measures for the sake of society in technologically savvy world.[19] In the course of cyberspace advancement, every piece of information is preserved and thus might be misused by the private companies or governments which is why it is in the interest of each individual to pay attention to privacy protection. The larger amount of information there is on disposal to cybercriminals, the greater are chances of abusing them and higher is the risk of unintentional maltreatment by third parties.[20] One of the founding principles in every societal and security context revolves around trust, as it is a platform for security-building process. Security builds up the trust between people and technology and is required to protect the foundation of trust upon the society depends. When did the cyber emerge as an issue and what are the societal changes that benefited to its problematization and, consequently, securitization?

[18] Wong, A. (2016). 'Cybersecurity: Threats, Challenges, Opportunities.' [online] Acs.org.au. Available at: https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf [Accessed 12 Mar. 2018].
[19] Ibid.
[20] Ibid.

1.2. Downsides: Growth of Cyber Skepticism

In contrast to the initial excitement of the cyber possibilities, dynamic and volatile nature of the cyberspace blended with increasingly complex information technology tools led to eventual inception of threats, main argument favorized by the skeptics, some of which turned into critics. Their observation consists of the implication that although networks keep enabling transfer of knowledge and information to the people using it, new vulnerabilities of cyberspace continue to emerge.[21] Not long after, downsides of cyber have begun to be a subject of a wider debate in which economic and political elements were put in focus along with security and integrity of individuals, businesses and states. The cyber phenomenon along with its issues was introduced to the international discussion forums in the 1990s.[22]

Conditional adoption of the information technology by the consumers and the private sector sparked notable alterations in a way of producing, using and consuming information. Forming the necessary foundations for technology and its transfer to commercial use without any significant obstacles, concrete and strong commercial interest in the Internet started to progress in the beginning of the 1990s whereas the "primary open questions were concerning business models of service and profitability of providing Internet access outside the academic community".[23] Regardless of the emergence of cyber notion in the 1990s, the concerns that were dispersed by it came into focus in recent years, starting from the realization that potential impacts caused by it have to be addressed, along with the necessity to build up a resilient system and actualizing cooperation on international level. Critical infrastructure and utilities, transportation and banking

[21] Kasper, Agnes. 'The Fragmented Securitization of Cyber Threats', Springer International Publishing, Switzerland, (2014). 157-170
[22] Ibid.
[23] Ibid.

are dependent on the operational capabilities of computer equipment, relying on its flawless functioning, adopting the information technologies as integral part of its purpose. Throughout the time, perks of information boom era have tended to blur whereby cyber environment became a place of crime, a pragmatic platform for criminals to access the critical information via computer viruses and other illegal gadgets needed for "accessing databases, bank accounts and management information systems".[24] Ubiquitous issue of cybercrime spanned all over the digitally reliant systems since increasing number of people engage in this kind of criminal action. Availability of the information has expanded exponentially along with the progress of internet. Simultaneously, the barrier between useful and malicious information has become blurred. As a result, people started having less confidence in objective knowledge and a more skeptical view on the reliance of information technologies.[25] Societal context shifted; from having a positive, impeccable outlook on cyber future, numerous predictions insisted on being cautious when debating the future that heavily relies on information technologies.[26]

Throughout the time, people started to be more dependent on technology, leading to a constant and rapid information flow wherein cyberspace has begun to serve as an illegal area of information maltreatment, bolstering the repercussions that came along in a form of challenges. Money laundering and terrorist financing appeared as notable concerns of the web downsides. Christine Lagarde, the IMF Managing Director, gave a speech in 2017 on the importance of combating these problems, indicating how it is of grave importance to be "deeply committed to supporting countries

[24] Eurasian Group. (2014). 'Cybercrime and Money Laundering.' [online] Available at: http://www.eurasiangroup.org/files/Typologii%20EAG/Tipologiya_kiber_EAG_2014_English.pdf [Accessed 14 Mar. 2018].

[25] Krimsky, S. (2007) 'Risk communication in the internet age: The rise of disorganized skepticism', Tufts University, Medford, Environmental Hazards 7., 157-164

[26] Burkeman, O. (2009) 'Forty years of the internet: how the world changed for ever' The Guardian. Available at: https://www.theguardian.com/technology/2009/oct/23/internet-40-history-arpanet Accessed, May 15, 2018

in building defenses against money laundering and the financing of terrorism through the international framework standards"[27] knowing that neither of these challenges may not be tackled by countries working alone. She stressed out the relevance of encountering the financing of terrorism due to its pervasive character, implying that financial flows must be halted in order to disable terrorists' intentions of harming communities and individuals.[28] Some academics argue that cybercrime is a new category of felony that requires an advanced 'comprehensive legal framework' to address a 'unique set of challenges' that do not fall under traditional crime, namely international cooperation and the difficulty of identifying the perpetrator. Moreover, they pose an idea that cybercrime displays a new form of business that will necessitate a 'fundamental paradigm shift' in policing.[29]

The most extensive committed cybercrimes are very much related to illegal and unauthorized fund-removals from bank accounts, card-payment frauds, sharing of computer viruses and interference with online banking systems.[30] Executors of these attacks most of the time have a mission to gain financial advantages from theft or extortion, either from stealing classified documents in governmental property, developing capabilities to perform attacks for the support of certain country's strategic objectives or by engaging in cyberattacks "as a form of non-state or state-sponsored warfare".[31] Cybersecurity emerged at the same moment when the attackers decided to test or probe weaknesses of the system, thus leading to an everlasting circumvention between them

[27] IMF. (2017). 'Working Together to Fight Money Laundering & Terrorist Financing.' [online] Available at: https://www.imf.org/en/News/Articles/2017/06/21/sp062217-working-together-to-fight-money-laundering-terrorist-financing [Accessed 19 Mar. 2018].
[28] Ibid.
[29] Jain, N. and Shrivastava, V. (2014) 'Cyber crime changing everything – An empirical study", International Journal of Computer Application, Issue 4, Vol. 1, 76-80
[30] Eurasian Group.
[31] Fischer, E. (2016). 'Cybersecurity Issues and Challenges: In Brief.' [online] Fas.org. Available at: https://fas.org/sgp/crs/misc/R43831.pdf [Accessed 19 Mar. 2018].

and the defenders. Majority of attacks do not significantly affect the targeted components due to their limited impacts, but a successful one can cause major malfunctions of critical infrastructure; affecting the national security, economy and safety of citizens.[32] Moreover, confidential data along with the integrity of an ICT sector can be jeopardized by exfiltration of financial and personal information oftentimes committed without the victim's awareness of it. Therefore, cyberattacks can be costly to the ones who are attacked, with severe economic repercussions, and that fact is additional reason going in favor of cyber skeptics' and critics' assessment, an appraisal in which they advocate for development of sophisticated cybersecurity system as well. Rob McCusker, A prominent scholar and cyber crime expert poses an assumption how traditional organized crime groups will not recoil from using the cyberspace to facilitate the operation or to 'disguise the illicit proceeds' of physical crimes. He believes that the attacks targeted to pursue extortion, transfer laundered funds and acquire pertinent personal information will continue to evolve and that the tension between logic and pragmatism continues to persist.[33] More precisely, logic dictates that traditional criminals would cope up with the cybercriminal endeavors as long as it is a profitable and low-risk activity, whereas pragmatism employs the notion that traditional crime groups do not necessarily take advantage of cyberspace due to a lack of capacities and knowledge.

Security has always been a crucial component of traditional societies. After the Cold War ended, the concept of security has been widened to embody societal, global and individual security whereas the conceptions of internal and external security merged into a new 'field of security'.[34] Boundless cyberspace environment is a leading cause of the paradigm shift in security practice.

[32] Ibid.

[33] McCusker, R. (2006) 'Transnational organised cyber crime: distinguishing threat from reality', Crime, Law and Social Change, 46 (4-5), 257-273

[34] Diez-Nicolas, J. (2015) 'The perception of security in an international comparative perspective', Royal Institute, Working Paper 16., 2-12

The field of international relations opened new perspectives and conversations on the 'conflict space of the future', thus shifting the conceptual security understanding.[35] The traditional concepts of international relations have been contested by the emergence of cyberspace due to its growing relevance to an increasing number of political and social activities. "A great amount of scholarship in cyber security is focused on what might be considered realist theories or their variants, with the concern for power and balance dominating. The question of deterrence is ubiquitous in the domain."[36] The respective deviation within the IR field from the traditional security concepts of power, territory and sovereignty to cyberspace and cybersecurity is apparent, but that does not change the fact that the field of cyber can learn much from the perspectives of IR theory and ethics.

It is an inevitable fact that globalization left its mark on the evolution of new threats to the civilization, a process under which national perception of a threat along with threat itself drastically changed, evolved rather.[37] What was once inconceivable, nowadays is rational; strategic advantage went in favor of information and knowledge, leaving the geographical location advantages and fighting power behind itself. As the information technologies have been developing, people have been synchronously adopting them, which appeals the new coming opportunities for the savvy attackers, ready to take full advantage of cyberspace. It is the very cyberspace in which experts tend to believe escalation of conflicts and intelligence activities will occur, thus claiming how these issues are of a great concern to the international security.[38] Their stance on this topic revolves

[35] Woodward A., Williams P.A.H. (2015) 'An Uncomfortable Change: Shifting Perceptions to Establish Pragmatic Cyber Security'. In: Unger H., Meesad P., Boonkrong S. (eds) Recent Advances in Information and Communication Technology 2015. Advances in Intelligent Systems and Computing, vol 361. Springer, Cham., 1-8

[36] Valeriano, B. and Maness, R. (2018). 'International Political Theory and Cyber Security.' In the *Handbook of International Political Theory*. Oxford University Press., 265

[37] Duić, I. (2017). 'International cyber security challenges.' [online] Bib.irb.hr. Available at: https://bib.irb.hr/datoteka/878827.Duic_Cvrtila_Ivanjko_International_cyber_security_challenges_.pdf [Accessed 19 Mar. 2018].

[38] Ibid.

around the notion that attacks of this character will develop into increasingly common cyber phenomenon, causing large-scale devastation and inducing incurable consequences. Before devoting effort to critically evaluate and address cyber concerns by applying the securitization theory in which "diverging perceptions and intertwined interest of stakeholders"[39] are scrutinized, it is of crucial importance to problematize cyber on EU level for this topic to be completely comprehended. By understanding the efforts of securitizing actors and by applying the securitization framework in an empirical case, cyber has the base to be thoroughly elaborated while securitization serves as the ground for exceptional political measures.

[39] Kasper. 165

2. CYBERSPACE: THEORETICAL PERSPECTIVE

2.1. Theoretical Concept of the Copenhagen School

The comprehension of security was greatly complemented in the book 'People, States and Fear' by Buzan who extended the scope of national security fields to societal, economic and ecological problems while simultaneously insisting that the political-military field remains the governing feature of each state's security.[40] The Copenhagen School approach to security perceives security threats in one of these five (military, political, environment, economic, social) specific yet interconnected sectors.

The securitization theory of the Copenhagen School introduces securitization as an intersubjective and self-referential socially constructed process which is a shift from objectivist conception of security. The theory indicates how the success of securitization depends on the level of convincing the audience and their acceptance for securitizing actors to take extraordinary measures. However, extraordinary measures are not the case of this empirical case, which is why alternative interpretation of the Copenhagen School is provided in the following parts of this section, leading to assertion that this research will combine two approaches; extracting selectively assumptions of both. In CS authors' words, intention of the theory is defined as the following: "Based on a clear idea of the nature of security, securitization studies aims to gain an increasingly precise understanding of who securitizes, on what issues (threats), for whom (referent objects), why, with what results and, not least, under what conditions (what explains when securitization is successful)."[41] In the process of conviction, securitizing actors have the challenge to gain the

[40] Buzan, Barry. 'People, States, and Fear', London: Harvester Wheatsheaf, (1991). 134

[41] Buzan, Barry, Waever, Ole and de Wilde, Jaap. (1998) 'Security: A New Framework for Analysis', Boulder. Lynne Rienner Publishers., 32

confidence of audience to adjust the current rules for a limited time only. If the audience accepts securitization, actors have the right to proclaim their own actions legitimate and essential, but the audience does not have to embrace emergency actions *per se*. To fully grasp the process of securitization, one needs to have a notion of the terms 'speech act', 'functional actor' and the 'referent object' used by the authors.[42] The consciousness of security is conceived by a speech act that intents to securitize a certain issue as an existential hazard toward a referent object which is why the referent object is in acute need of protection from the specific threat. Speech act refers to the prime rhetorical tool used for illustrating the issue as a threat to society whereas various rhetorical concepts that deliver the notion of existential threat are being used. In addition, it constructs a certain way of observing existing reality through a security frame. The theory indicates that introduction of the threat by a speech act is perceived as a move for justifying the use of force and utilization of security measures by the securitizing actors. A referent object specifies the object that is being securitized, the concern that is being portrayed as existentially threatened and demands prompt securitization.[43] According to Balzacq, securitizing actors must apply terms that resonate with audience's experiences, and will always strive to target the audience that is directly connected to the referent object.[44] Lastly, a functional actor differs from the securitizing actor that labels something as existentially threatening and is the one who has a significant influence on the "decisions in the field of security".[45] The speech act is most commonly referred to a securitizing move; a move with the ability to ascend political issues outside the scope of normal politics, increasing the need to urgently react and encouraging immediate response. It serves as a medium

[42] Ibid. 30
[43] Ibid. 36
[44] Balzacq, Thierry. (2011) 'A theory of securitization: origins, core assumptions, and variants.' Securitization Theory: How security problems emerge and dissolve. New York: Routledge., 5-11
[45] Buzan et al. 36

to avoid the normal political practice and to swiftly receive attention for an issue, thus justifying measures to mobilize resources. Successfully securitized issue is the first concern and has a leading role over everything else on account of survival of the referent object, that relies on a quick and fortunate solving of the situation. Buzan and co-authors greatly enhanced the perception of societal security, underlining its increasingly relevant role as well as suggesting a reconceptualization of the security environment.

Classical understanding of the security concept has been oftentimes interpreted as a states' domain of activity in which states decide to act upon security matters and aspire to enable security conditions. Buzan, Waever and De Wilde challenged classical 'end-state' security approach arguing that security does not necessary have to be favored option. In light of this notion, security can still be a case of relentless conflicts, even though these situations are a product of adequate countermeasures for achieving a balanced situation.[46] The Copenhagen School's theoretical concept appeared as a blend of wider security conception and traditionalist approach. The authors of the theory purport how it is possible to escape traditionalist security approach, claiming that one needs to perceive "logic of security itself to find out what differentiates security and the process of securitization from what is merely political".[47]

Buzan and his fellow scholars introduced the term 'securitization' wherein they claim it is a "move that takes politics beyond the established rules of the game and that it frames the issue either as a special kind of politics or as above politics".[48] The narrowness of the Copenhagen School on the speech act is complemented by the Paris School that argues how security is a construction of

[46] Ibid. 4
[47] Ibid. 4-5
[48] Ibid. 23

routinized practices rather than just speech acts that enable emergency measures.[49] In this regard, Bigo claims that "to attend to the study of securitization is to focus on the creation of networks of professionals of (in)security, the systems of meaning they generate and the productive power of their practices".[50] This contends the Copenhagen School's assumption of security as a realm of dramatic emergency measures only. Additionally, Bigo asserts the assumption how elites' discourses of securitization continue to be so powerful that even when alternative voices are well known, they stand no chance in affecting political arena. Both Schools argue that securitizing actors possess specific authority to attract the interest of audience.[51] No one is excluded from attempting to securitize or "articulate alternative interpretations of security", however, the power structure within the security field implicates that state elites hold advantageous position over construing security threats.[52] Waever asserts the idea that "by definition something is security problem when the elites declare it so".[53] Moreover, Buzan et al. tend to underline how securitization is most importantly a practice that is self-referential; meaning that the securitizing actors add the prerogative 'existential' to a certain issue not because an actual existential threat prevails but because they stage it as such.[54] Additionally, securitizing actors do not necessarily feel threatened by the same political issues that they ascend into the securitization realm. Instead, by characterizing the threats as exceptionally threatening, actors seek to attract confidence and approval of the audience in taking measures to counteract. Therefore, whether the actual threat

[49] Bigo, D. (2002) 'Security and Immigration: Towards a Critique of the Governmentality of Unease', Alternatives 27 (Special Issue): 63-92
[50] C.a.s.e Collective (2006) 'Critical Approaches to Security in Europe: A Networked Manifesto', Security Dialogue 37(4): 443-87
[51] Buzan et al. 32
[52] Ibid.
[53] Wæver, O. (1995) 'Securitization and Desecuritization' In On Security, ed. Ronnie Lipschutz. NY: Columbia University Press., 54
[54] Buzan et al. 24

exists or not, securitization falls under the political choice due to the fact that securitizing actors decide if the threat is going to be depicted as existential or not. Having put the choices of securitizing actors into comparative perspective, the theory notes that threats are intersubjective, perceived differently by securitizing actors and for these same reasons is the securitization intersubjective and socially constructed.[55]

Finally, it is important to imply how not all the scholars believed that the School would add great value to the analysis and conceptualization of security. Walt argued that the expansion of security field would devastate its intellectual coherence and contribute to the difficulty of constructing solutions to any serious problem that agonizes global politics.[56] Others believed that it would be counter-productive because it "extends the call for state mobilization to a broad range of issues".[57] The persistent critique has been that it pays too little attention to the factors determining the success or failure of the securitization moves, and that it fails to address the normative implications located within the securitization theory. Williams, for instance, critiques the School for being "politically irresponsible and lacking any basis from which to critically evaluate claims of threat, enmity and emergency".[58] Aradau gives a critique on the ethical aspect of the securitization process, implying that it is a government's technique to establish fear of violent death; and as such fabricates "an existential threat which provokes experiences of the real possibility of violent death".[59] Her perception dictates that securitization is an ethical issue that is by its very nature labeled as bad. Coming into the twenty-first century, academics acknowledged the innovative and fascinating

[55] Ibid. 30
[56] Walt, S. (1991) 'The Renaissance of Security Studies.' International Studies Quarterly. Vol. 35, No. 2, pg. 213
[57] Buzan et al. 4
[58] Williams, Michael C. (2003) 'Words, Images, Enemies: Securitization and International Politics' International Studies Quarterly 47., 521
[59] Aradau, C. (2004) 'Security and the democratic scene' in: Journal of International Relations and Development (Vol. 7, No. 4)., 405

approach that the CS brought along, one of which stated that "The Copenhagen School is one of the most interesting developments in the contemporary study of security".[60] Additionally, Alker is assured that CS is qualified to open new channels for echoing alternative security concerns, claiming that the theory "responds constructively, discursively, to the transnationalizing of concerns and the broadening of possibilities for reconceptualizing threats".[61] The theory has shaken up security concepts within the IR field although the very nature of it puts a limit on its explanatory power; a component that was strengthened by Guzzini who enhanced the empirical theory and made implicit causal mechanism more explicit.[62]

2.2. Securitization Theory Meets Cyber

To what extent does the Copenhagen School engage the conceptualization of cybersecurity? A question that arises after overviewing the theory of securitization is how exactly does the cyber fit in the theory. Thought-provoking fact is that the securitization theory scholars did not believe that cybersecurity can be one of the existential threat to the nation states back in the 1990s due to a lack of sizeable effects on other security issues.[63] The occasions that drastically changed concern the reliance of humankind on critical infrastructure and the advancement of technology throughout the last few decades.

Before presenting additional arguments of the cyber securitization literature, next paragraph will deal with the ideas of the very first scholars of the Copenhagen School who successfully theorized cybersecurity as a distinct field within the securitization framework and provide the answers to

[60] Smith, S. (2005) 'The Contested Concept of Security'. In Critical Security Studies and World Politics, ed. Ken Booth, 37

[61] Alker, Hayward. (2005) 'Emancipation in the Critical Security Studies Project' In Critical Security Studies and World Politics, ed. Ken Booth., 198

[62] Guzzini, S. (2011), 'Securitization as a causal mechanism' in: Security Dialogue, Vol. 42, No. 4-5., 329-341

[63] Buzan et al. 25

'why' and how' it is manageable. The threats that the evolution of cyber space delivers within itself are no different than the economic ones; the impact is global and there are no borders that could be an efficient obstacle. Cyber threats are continuously challenging traditional security norms and alter the perception of conflicts which is why cyberspace serves as a foolproof relevant framework within the Copenhagen School. Moreover, we are witnessing multiple cases in which states securitize and sanction specific cyber acts. This is the reason why securitization theory is especially applicable for cyberspace securitization because it is perceived as a notion of security where discursive approach is present and when it has a "rhetorical structure and political effects".[64] An additional matter going in favor of the applicability of the theory is the fact that if the existential threat exists and receives the spotlight of the audience, then other areas of the society would be included in resolving the situation apart from the army.[65] In that case, joint action plan from all of the involved societal actors is a necessity, in order to have a suitable cyberspace securitization. Such an action of empowering persuasive shift between securitizing actors and the referent objects is the reason why the theory of securitization is a convenient approach to cyberspace. Securitization of cyberspace is an ongoing practice which effects the regular lives of individuals that are digitally reliant. Because of the experiences that each person is facing in form of the cyber threat, hazard sequence of events is directly linked to the everyday actions done by the people, which makes an individual the referent object of securitization.[66] Accessibility and pragmatism of the hacking apparatus makes the escalation of national catastrophe more plausible. [67] An individual can be both a victim or the perpetrator of the cyber-attack while at the same time being a

[64] Hansen, L. and Nissenbaum, H. (2009) 'Digital Disaster, Cyber Security, and the Copenhagen School', International Studies Quarterly. Vol 53, no. 4., 1156
[65] Hansen and Nissenbaum.
[66] Ibid.
[67] Dun Cavelty, M. 'Cyberthreats, in M.Dunn Cavelty and V. Mauer (Ed), The Routledge Handbook of Security Studies', London: Routledge, (2010). 180-189

fundamental aspect of the resistance to the cyber insecurity and accountability for the functioning of the cyber space, whether his act is intentional or not.[68] Regardless of having the scarcity of experience and knowledge of technicalities in the cyber field, political elites have become securitizing actors because of the complimentary discourses between them and the computer specialists. Moreover, it is feasible to make a distinction of the politics from the tech expertise in the cyber field, but both make their own contribution to the cyber securitization and try to depoliticize the cyber issue by labeling it as an existential threat. The following section will engage other scholars' works on cyber securitization and identify guiding points for a further empirical analysis.

Barnard-Wills and Ashenden implied that cyberspace is a way that "people and institutions think, understand and talk about this space"[69] which supports the claim how cyberspace is a social construction, which is an upgrade to the original notion of it as physical construction only. The authors pinpointed several problems in the discussion on cybersecurity. They start off by claiming how cyberspace is of anarchic character and thus cannot be governed.[70] In addition, due to the increasingly rapid progress of information technologies and the agile pace of developments it is much unlikely to foresee the upcoming threats which makes the cyber innately unknowable. The cyberspace is presented as something that "is unknown and potentially unknowable, shifting and protean, anonymous, and full of dark corners where threats may hide".[71] From theoretical perspective, cybersecurity consists of three elements, namely people, process, and technology which were discussed by Andress who claims that security is the outcome of interaction between

[68] Hansen and Nissenbaum.
[69] Barnard-Wills, D. and Ashenden, D. 'Securing Virtual Space: Cyber War, Cyber Terror, and Risk' in: Space and Culture (Vol. 15, No. 2), (2012). 111
[70] Ibid. 116-117
[71] Ibid.

all three.[72] According to him, people are the weakest link in this security chain but most important ones. On the other hand, as technology relies on the other two, it makes it the least important. Janes asserts a presumption that the process connects people and technology, and its relevance is in that that it encompasses policies and procedures.[73] Thus, exposure of any of these greatly threatens the system as a whole, as much as integrating all three benefits the policies of preserving security. Moreover, three grammars of securitization of cyberspace, introduced by Hansen and Nissenbaum, could significantly enhance the understanding of cyber securitization. Hyper-securitization is the first of them and is used to explain the process of securitization that exceeds a 'normal' level of threats and dangers, for justifying the use of extreme countermeasures.[74] Again, securitization is a self-referential, intersubjective process which makes it hard to objectively perceive the 'normal level' of threats. Secondly, everyday security practices make up the second grammar and are being used by securitizing actors (both from government and private sector) to bring the disaster scenarios closer to the people's minds: "to make hyper-securitization scenarios more plausible by linking elements of the disaster scenario to familiar experiences from everyday life".[75] Technification, third and last grammar explains how important is the role of technical experts, mostly securitizing actors that legitimize cybersecurity by themselves, approve hyper-securitization scenarios and talk to the public (audience) about the importance of its everyday practices.[76]

[72] Andress, A. (2003). 'Surviving Security: how to integrate people, process, and technology' 2nd. Boca Raton: Auerbach Publications., 5

[73] Janes, P. (2012). Information Assurance and Security Integrative Project: People, Process, and Technologies Impact on Information Data Loss. SANS Institute, Available at: https://www.sans.org/reading-room/whitepapers/dlp/people-process-technologies-impact-information-data-loss-34032 [accessed May 16, 2018]

[74] Hansen and Niessanbaum. 1163

[75] Ibid. 1165

[76] Ibid. 1169

Bendrath provides an empirical case assuming that the Clinton administration attempted to securitize cyberspace and protect US critical infrastructure by using the expression 'Electronic Pearl Harbor', a cyber threat of an impact similar to 1941.[77] However, author believes that the attempt to securitize cyberspace was unsuccessful in this case due to a perception of law enforcement agencies that cyber threats are more dangerous to the law and order than they are to the national security. The private sector complemented them, implying that cyber risk is a local problem and nothing more than an economic cost.[78] These conclusions, and real-life situations could easily be projected to the empirical analysis of this research due to the similarities in Western values and political agendas. One recent example from the times under Obama's administration draws a parallel between securitization of cyberspace and the protection of critical infrastructure. The Executive Order from the 2013 is an example of a speech act whereby it states: "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront".[79] Although Lewis has a skeptic view on the vulnerability of critical national infrastructure due to a large-scale cataclysmic cyber-attack[80], Schmidt argues that Obama's Executive Order is a clear example of efforts not to just improve cybersecurity, but to securitize cyberspace and enhance protecting critical infrastructure.[81] Regardless of the fact that there is a literature gap concerning the cyber securitization efforts at the EU level, both theoretical and empirical reasonings scrutinized above could be beneficial for this analysis to be conducted.

[77] Bendrath, R. (2001), 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection' in: Information & Security. Vol.7., 16
[78] Ibid.
[79] Federal Register. (2013) 'Executive Order 13636: Improving Critical Infrastructure Cybersecurity' Available at: https://www.federalregister.gov/executive-order/13636.pdf (Accessed May 16, 2018)
[80] Lewis, J.A. (2002) 'Assessing the risks of cyber terrorism, cyber war and other cyber threats', Washington DC: CSIS
[81] Schmidt, H.A. (2011) 'The Administration Unveils its Cybersecurity Legislative Proposal' Available at: http://www.whitehouse.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal (Accessed May 16, 2018)

The empirics of this research uses both speech act theory of the CS and everyday practices assumptions of the Paris School for having a wider perception of securitization of cyberspace at EU level.

3. SECURITIZING CYBER IN BRUSSELS

3.1. Discourse Analysis

Social construction of security is analyzed through speech acts where threats are being "represented and recognized".[82] Statements are perceived as a performative activity that can change the conditions of a certain situation. Finding meaning through discourse analysis reveals the notion of threat images. Balzacq tries to offer an explanation on why students find it appealing to include discourse analysis in their research: "Discourse analysis helps students map the emergence and evolution of patterns of representations which are constitutive of a threat image. In this sense, discourse is a vehicle of meaning, a meaning which is rarely self-evident but has to be chartered by the analyst".[83] The following discursive reasonings of the securitizing actors will be taken as illustrations of cyber securitization in Brussels in which three elements of the process are evaluated: do the actors endeavor to depict a referent object as an existential threat; do they entail the right to take extraordinary measures to counter the threat; and how do they try to convince the audience that the proposed measures are justified.

Elissavet Vozemberg-Vrionidi, European Parliament's rapporteur on the fight against cybercrime gave a speech in Strasbourg on October 2, 2017 which will in this regard serve as the fitting example of securitizing 'speech act' in which cyber was socially constructed as an existential threat. She drew on her expertise as a lawyer in her home country and indicated that this is the issue she has dealt with actively. Ms. Vrionidi implied that it is not an easy task and that it requires a lot of preparation, ensuring a lot of legal arms, and that a clear, circumscribed definition of the

[82] Williams. 513
[83] Balzacq. 39

threat needs to be offered initially. "It is difficult to find an evidence of offense very often and sometimes criminals are ahead of us in terms of technologies that they are using. We have to look at EU legislation. It is certainly an area in which we would like to be more active and to tackle this threat that is a slap in the face to the rule of law, a risk that keeps undermining democratic societies."[84] Rapporteur used the figures in which she further elaborated on the importance to act, claiming that 50% of the crime happens online, and that in 2016 hacking within the EU increased by 22% which is a rapid increase in such activities. The need to formulate clear proposals to fill the gaps and shortcomings in the EU's legal system was communicated, wherein rapporteur called for an action in the area of prevention and data exchange along with sharing the experience between Member States and institutions, additional authorities and police forces.[85] European Union Agency for Network and Information Security (ENISA) was used as an example of Agency that is working very successfully, although its capacities must be built up by bringing in extra staff. This premise supports the claim that measures have to be taken to accordingly tackle cyber threats. "Criminals are always one step ahead of us, so if we can get our citizens more interested in digital technology to help us with the task of protection, that would be helpful, I think. This is a challenge, to protect the rights of citizens that placed trust in technology, and we also want to make sure to protect the rights of future generations."[86] Ms. Vrionidi explicitly referred to the audience to justify the measures that are being taken as well as the forthcoming ones. The report was concluded with the notion that the position of the Parliament is very much aligned with the Commission's one whereby children are the first ones that should be protected while simultaneously respecting human

[84] European Parliament. 'The fight against cybercrime plenary sitting', Recorded on October 2, 2017, 28:44. Posted in October 2017.
http://www.europarl.europa.eu/plenary/EN/vod.html?mode=chapter&vodLanguage=EN&startTime=20171002-19:35:39-573#
[85] Ibid.
[86] Ibid.

rights. Individuals are the case of a referent object in this speech act while source of threat remains the internet. In accordance to her statement, cyber threats are given much more attention due to a possibility that perpetrators possess advanced technologies and are most of the time few steps ahead of everyone else that may be threatened by their malicious activities.

Caterina Chinnici, Member of the Parliament, had a more vehement appearance claiming that cybercrime is one of the 'worst threats' facing us globally, and additionally implied how over the last year cyber-attacks had increased of up to 750%, reaching unprecedented levels.[87] In order to meet the challenge, she called for a European legal framework with clear definitions and forms of cybercrimes with cross-border guidelines and online risk management campaigns. Her notion was for a note brisker than the preceding one due to linking cyber decidedly to the existential threat. Humanity as a whole was described in her speech act to be a referent object while claiming that nature of the threats becomes more expanded and reaches stages not seen before.

European Commissioner for the Security Union, Julian King, referred to the cyber awareness as the key subject at that same hearing, echoing official stance of the Commission. His statement revealed that the cyber-attacks can be achieved at surprisingly low cost but with devastating effect, posing thus risk to security, democratic processes and institutions which is a rationale for promoting cybersecurity within the EU.[88] "We recognize the importance of Europol and ENISA", he added, "but we need to strengthen the work that they have been doing and strengthen cooperation between different agencies and instruments."[89] His speech announced how certain solutions will be carried out by the Commission, justifying all the necessary means to contest cyber threats. The Commissioner implied that referent objects are in this case Member States (their

[87] Ibid.
[88] Ibid.
[89] Ibid.

democracies and institutions) whereby cheapness of the attacks and easiness of their execution pose a threat to the security of the Union.

On 13 September of 2017, in the annual State of the Union Address**,** President of the European Commission, Jean-Claude Juncker, stated: "In the past three years, we have made a progress in keeping Europeans safe online. But Europe is still not well equipped when it comes to cyber-attacks."[90] His address contained the notion that further harmonization is inevitable, for the sake of EU citizens, and by this act attempted to convince the audience of the seriousness of cyber risks. In addition to that, he portrayed cyber-attacks as the matter of existential proportions, suggesting that cyber-attacks have the tendency to become "more dangerous to the stability of democracies and economies than guns and tanks".[91] Mariya Gabriel**,** Commissioner for the Digital Economy and Society, emphasized the necessity to build on the trust of EU citizens, underlining that high cybersecurity standards will become a new advantageous component of businesses that will thus easier tackle "large-scale cyber-attacks"[92] which are becoming more and more frequent. While his predecessors had tendency to illustrate cyber threats as existential, Andrus Ansip, Vice-President for the Digital Single Market, described measures and tools needed for consistent and healthy cybersecurity as the promotion of 'cyber-hygiene', calling for joint initiatives and strengthening of cooperation in this field.[93] His recommendation consisted of convincing the audience that proposed measures have to be taken in light of more efficient fight against criminals as well as to

[90] European Commission. 'State of the Union 2017 - Cybersecurity: Commission Scales up EU's Response to Cyber-attacks.' European Commission - PRESS RELEASES - Press Release - State of the Union 2017 - Cybersecurity: Commission Scales up EU's Response to Cyber-attacks. Accessed March 20, 2018. http://europa.eu/rapid/press-release_IP-17-3193_en.htm

[91] European Commission. 'President Juncker Delivers State of the Union Address 2017.' December 14, 2017. Accessed March 20, 2018. https://ec.europa.eu/commission/news/president-juncker-delivers-state-union-address-2017-2017-sep-13_en

[92] EC Press Release.

[93] Ibid.

intensify investment in innovation. Federica Mogherini**,** High Representative/Vice-President, was more focused on the outcomes of implementing the proposed policies, arguing how the EU will "pursue an international cyber policy promoting an open, free and secure cyberspace as well as support efforts to develop norms of responsible state behavior, apply international law and confidence building measures in cybersecurity."[94] The vision of a stable and protected cyberspace is taken as an example of possible and desired outlook in a case of effective fulfilment of law and policy requirements. All of the speakers put the EU citizens, individuals, in the focus of their referent object. Their perception on the nature of the threats revolves around frequency of the attacks and possibility of the threats to evolve into a first concern to the security of each MS.

The day after the State of the Union, EU Cybersecurity Conference was held in Tallinn, Estonia wherein experts from various cyber field gave insightful observations on the current cyber threat landscape. The nature of this conference was to discuss the future of cyber within EU in light of proposed initiatives and solutions. Jean Pierre Nordvik, Head of Cyber Security Unit in the Joint Research Centre (JRC), European Commission's independent science and knowledge service, stated that research and innovations are key components and essential ingredients in building strong cybersecurity in the EU.[95] Jarno Limnell, professor of cybersecurity at Aalto University, believes that experts can encounter remarkable speeches at the digital conferences until the moment when security experts start talking about the issue. He claims that he has been dealing with cybersecurity issues for more than twenty years and based on his experience, tends to think that everybody needs to be an ambassador of positive cyber thinking, arguing that cybersecurity is an 'added value component' in the digital Europe. According to him, cybersecurity is worrying in

[94] Ibid.

[95] EU2017EE. 'EU cyber security conference 2017 – 14 September' Filmed [September 2017]. YouTube video, 5:34:11, Posted [September 2017]. Accessed March 21, 2018. https://www.youtube.com/watch?v=uY9d1hpoOvc

respect to elections, notably foreign states trying to affect election systems in different ways; breaches, leaks, information influencing, fake news etc.[96] Krzysztof Silicki, Technical Director of Research and Academic Computer Network (NASK), tends to believe that the threats are growing rapidly each year. He consistently uses the phrase 'threat landscape' by which he depicts the civilian critical infrastructure, cyber-crimes and hybrid threats.[97] Gail Kent, Facebook's global security expert, claims that Facebook experiences attacks on daily basis on its infrastructure, system and users. Her belief is that the experts have to provide easy-to-use and flexible solutions whether it concerns medium-size government departments, small businesses or regular users. She provided the notion that cybersecurity community must work together and that the proposed solutions need to be easier to understand for all the involved communities.[98] The predominant sentiment of the conference was to provide as much explanations as possible to tackle the threat and to ensure the digital autonomy of EU. Moreover, the securitizing element of convincing the audience that every taken deed is necessity did not lack, although it was sometimes hard to notice any intent in symbolizing the cyber threat as the existential one.

Rand Corporation published a research where several recommendations were issued, namely developing cybersecurity standards and certifications to improve the security of online transactions, implementing a bill of user's rights and enhancing information sharing between public and private sector.[99] These solutions were seen before, however, this thank-tank put consumer and stakeholder in the focus of a referent object. Research implies that consumers should be educated on cyber risk via public awareness campaigns. Primary concerns of this paper are

[96] Ibid.
[97] Ibid.
[98] Ibid.
[99] RAND Corporation. (2016) 'A framework for exploring cybersecurity policy options', Published Research, Available at: https://www.rand.org/pubs/research_reports/RR1700.html (Accessed May 16, 2018)

massive data breaches that can compromise financial system, and malicious actors who have found a way to exploit vulnerabilities of cyberspace.

Clingendael, a Netherlands Institute of International Relations, published an article on evolving cyber threats. Article asserts a notion that classification and unification of threats is not possible due to a wide range of cyber-attacks. However, it emphasizes individuals and society as the referent objects.[100] Main idea is to concentrate on cybersecurity in the near future, because it will become a key topic in international politics. In accordance to the article, all forms of cyber threats will become more aggressive and ways of dealing with them are embodied in deterrence, defense and diplomacy, whereby diplomacy is the only option that offers a long-term solution.

Some of the theoretical arguments provided by Hansen and Nissenbaum, namely three grammars of cyber securitization could be noticed in some of these utterances. Firstly, securitizing actors did not use hyper-securitization whatsoever due to a lack of any efforts to illustrate the 'exaggerated threats' both in public speeches and written recommendations. Everyday security practices were evident in a way that actors have cultivated fear in everyday life and used it to enhance securitization. Lastly, technification, seen as a speech act that can "construct an issue but requires technical expertise of the subject" was apparent in many occasions, thus providing authority and legitimacy to the experts for employing their knowledge.[101] It is hard to find a radically contrasting view on the importance of cyber. The EU strategy on cybersecurity was set up based on the opinions of the securitizing actors (political elites) and lobbyists; 'functional actors' of the securitization theory, experts who both influence and raise concerns on certain policies, programs

[100] Van der Meer, S. (2016) 'Defence, deterrence, and diplomacy: Foreign policy instruments to increase future cyber security' Available at: https://www.clingendael.org/sites/default/files/pdfs/book_securing-cyberspace-chapter_July2016.pdf (Accessed May 16, 2018)

[101] Hansen and Nissenbaum. 72

and projects;[102] making up a vital part of the European security agenda which is why interests of securitizing actors complement one another.

3.2. Proposed Solutions

The following paragraphs will address the policy, legal and institutional solutions proposed by the relevant EU securitizing actors by which they intend to introduce means for combating the cyber concerns and thus add weight to the cyber securitization argument. The constantly upgrading tools and EU policies are contributing to a proactive approach towards protecting the society, prosperity and its founding values by countering the existing and future cyber-threats correspondingly. Ensuring that the EU develops and expands vital capacities stays the primary concern of EU's strategic interest, not only to secure digital economy and democracy but to protect critical infrastructure as well as to provide cybersecurity services of grave importance. The EU's affection to the rising weight of cybersecurity started off as an economic concern, and while still having significant impact to shaping of economic policies, its area of influence drastically expanded.[103]

3.2.1. Policy Solutions

European Commission and its High Representative of the Union for Foreign Affairs and Security Policy, currently held by Federica Mogherini, addressed the European Parliament and Council in the Joint Communication document issued in 2017[104], and as such can serve as one of the most advantageous form of discourse between high ranking officials, ergo institutions. The document

[102] Boros, Crina. "[Investigation] How the EU Cosied up to the Defence Lobby." EU Observer. December 20, 2016. Accessed March 23, 2018. https://euobserver.com/investigations/136310

[103] Carrapico, H., & Barrinha, A. (2017). 'The EU as coherent (cyber) security actor?' Journal of Common Market Studies, *55*(6), 1254–1272

[104] European Commission. (2017). 'Joint Communication to the European Parliament and the Council', Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. High Representative of the Union for Foreign Affairs and Security Policy, JOIN (2017) 450 final. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450

explicitly implies that policies of the Union are designed to approach the constantly evolving challenge of promoting cyber stability accordingly while at the same time going in favor to Europe's strategic cyberspace-autonomy.[105] Moreover, it indicates how the malicious acts in cyber sphere threaten the economy of each Member State, their very own democracies, guiding values and freedoms, and the Digital Single Market and that it is of vital importance to ensure that EU has tools against cyber-threats by which it would preserve and secure civilian infrastructure and military capacity, both relying on secure digital systems.[106] The predominant rhetoric implications of this Communication signify that the EU works exhaustingly on prioritizing international cybersecurity issues in its international engagements, putting respect for human rights in front of its agenda and cultivating its core values. The Commission has recently proposed establishment of an EU cybersecurity certification framework, which aims to provide "trustworthiness and security of information technology products" whereas it would contain of technical requirements, comprehensive set of rules, standards and procedures.[107] After the framework has been initiated, stakeholders of relevance will be invited by the Commission to fixate on security of systems that EU citizens depend on in customary activities; from cars and airplanes to power plants and medical devices; all of which are interconnected and are becoming digital to a great extent.[108] Commission tends to display that adopting the framework will affirm EU's international position and stimulate additional efforts of development of high-security standards recognized world-wide.

3.2.2. Legal Solutions

Not until recently, the European Union has been notably slender in terms of legally binding agreements touching upon cyber, which can be prescribed to the notion of how cyber securitization

[105] Ibid.
[106] Ibid.
[107] Ibid. 4
[108] Ibid. 5

has begun taking its toll on both political and economic fields. In fact, The Directive on security of network and information systems (the NIS Directive) which was adopted in 2016 is the first EU-wide legislation on cybersecurity.[109] This set of legal measures aims to ascend the overall cybersecurity level by making sure that Member States are prepared to be equipped in accordance to the Directive, that inter-state cooperation leads to exchange of information on EU level, and that culture of security prevails across the critical infrastructure sectors.[110] Furthermore, the NIS toolkit favors the appropriate security measures that businesses will have to take as well as notify future incidents to their national authorities. The legislation intends to deliver easily understandable provisions and provide insightful observation on how these provisions should work in practice.[111] However, due to its explanatory character, European Standards Organization (ETSI) recommends that the objectives of Directive are too technical and have a tendency to become obsolete at a rapid pace. Additionally, Directive is, in ETSI's view, partial and lacks some of the core cybersecurity issues and more importantly, businesses should adopt Directive, but market players are the ones who define levels of assurance.[112] EU Directives, unlike Regulations, are non-binding legislative acts that set out goals for each MS to achieve. It is then up to each MS to devise their own laws on how to achieve these goals. After adoption, The NIS Directive leaves up the space for each country to set out objectives and priorities of national strategy by establishing governance framework. Legal solutions enable Member States to take a lead in the integration process of cybersecurity legislations. Therefore, for the European Union to enhance its cybersecurity and increase its power

[109] Dekker, Marnix. "2018: The Year of the NIS Directive." Help Net Security. January 08, 2018. Accessed March 25, 2018. https://www.helpnetsecurity.com/2018/01/03/nis-directive/
[110] Ibid.
[111] Ibid.
[112] ETSI. (2018) 'Position Paper on Draft Regulation 2017/0225 "Cybersecurity Act"' Available at: http://www.etsi.org/images/files/ETSI_position_paper-CyberAct_20180206.pdf (Accessed May 17, 2018)

at the supranational level, direct decision of States' governments is to be made first.[113] These notions are prescribed to liberal intergovernmentalism, which poses a theory that periods of radical change in the EU are a result of converging governmental preferences whereas periods of inactivity come after diverging national interests. Legal solutions implementation process within the securitization theory of cyberspace fits into this theory.

3.2.3. Institutional Solutions

The European Commission progressively pushes forward its institutional solutions arguing how they will play a major part in helping to prevent and in some cases to eradicate newly developed existential threat. In this regard, EC points out that having a collective and extensive approach to formidable cyber resilience, promotion of cybersecurity and response to cyber threats on intra-state levels needs to be efficiently carried out on equal level as it is executed in the EU's institutions, bodies and agencies.[114] Institution-wise, Commission shares belief that Europol leads the way of becoming a center of expertise for cyber-related crimes. Since May of 2017, Europol has been officially recognized as the European Union Agency for Law Enforcement Cooperation whose Director is directly appointed by the Council. Members of the Parliament adopted a new regulation in 2016 which gave additional powers and authority to Europol for intensifying efforts in encountering cybercrimes. [115] This regulation precisely empowered Europol by allotting it a significant proportion of attention and resources for it to tackle securitized cyber issue. Additional argument for it to be a component of a larger securitization process is the fact that Europol on its

[113] Moravcsik, A. (2002) 'In Defence of the Democratic Deficit: Reassessing Legitimacy in the European Union', Center for European Studies, Working Paper No. 92, Journal of Common Market Studies, Vol. 40, Issue 04., 603-624

[114] EC Joint Communication. (2017)

[115] Europol. "About Europol." March 01, 2018. Accessed March 26, 2018. https://www.europol.europa.eu/about-europol

official website underlines its goal of securing the Member States from 'large scale' criminal and terrorist networks that pose a 'significant threat' to the safety of the EU citizens as well as the internal security of the Union.[116] The Joint Communication document points out that The European Union Agency for Network and Information Security (ENISA) serves as a focal point in providing information and knowledge for Member States, institutions of EU and businesses in the cybersecurity community, encouraging the cooperation among actors and strengthening cyber resilience within the Union. Having this fact in mind, Member States are the ones that must magnify the availability of cybersecurity tools for the private sector, using the ENISA as a backup platform.[117] Preceding Agency calls out Member States to step up and reshape their cybersecurity strategies by 'prioritizing' actions to improve overall security level. It also encourages public-private partnerships and information sharing; arguably extraordinary means used in the name of security, that in regular occasions has less chances to succeed. The Commission proposed to reform ENISA into the EU Cybersecurity Agency of stronger capacities, giving it a permanent mandate and a larger amount of resources. What will change then? The role of ENISA was to provide expertise instead of handling the cybersecurity operationally, which will be the case as soon as the Member States start applying the NIS Directive that is predicted to take place in May 2018.[118] The European Commission stands behind the establishment of public-private partnerships and collaboration on every level by introducing dedicated projects such as the Online Fraud Cyber Centre and Experts Network (OF2CEN) which serves as the standard model of information sharing, analyzing and addressing cyber-crime risks.[119] Nature of these solutions falls under

[116] Ibid.
[117] EC Joint Communication. (2017)
[118] European Parliament. "Legislative Train Schedule." March 20, 2018. Accessed March 26, 2018. http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-eu-cybersecurity-agency-and-cybersecurity-act
[119] EC Joint Communication. (2017) 16

supranational category, namely for the following reasons: ENISA is a regulatory agency that is financed by the EU budget while performing duties under first pillar and has the highest possible legal personality; even in the legal systems of the Member States.[120] Knowing that ENISA remains supranational institution, and recognizing efforts of securitizing actors to strengthen its capacities and give larger amount of resources, solutions of these kinds are of supranational character. Coherence of involved institutions could be observed as the "optimal alignment of procedures, policy outputs, instruments and actors, necessary to tackle security threats that are not bound by national borders".[121] A common approach of all securitizing actors has been consistently developing by enhancing the cooperation among them, advancing the instruments and adjusting the policies. In addition, institutional coaction is highlighted in this regard since European cybersecurity governance is decentralized with equal share of bodies in both public and private sectors.[122]

Given the fact that 80 percent of companies within the EU experienced cyber-attacks with an estimated cost of 265 billion euros every year, it was an imperative to form cybersecurity policies.[123] Taken initiatives by the actors are unquestionably a big leap forward the creation of unified cyber strategy. Things cannot change overnight, and there is certainly a large gap between the securitization incentives and real-life threat scenarios. Fragmentation between Member States, information sharing between public and private sectors and other securitization barriers do not go

[120] Zbiral, R. (2009) 'Agencies of the EU: The Emerging Network of Supranational Administrative Bodies' Contemporary Administrative Law Studies, Vol. 4, No. 1., 173-173

[121] Brattberg, E. and Rhinard, M. (2012) 'The EU as a Global Counter-Terrorism Actor In The Making'. European Security, Vol. 21, No. 4, pp. 557–577

[122] European Commission (2006) 'Communication from the Commission to the European Council of June 2006: Europe in the World- Some Practical Proposals for Greater Coherence, Effectiveness and Visibility', COM (2006) 278 final, 8 June.

[123] Di Matteo, B. (2017) 'New EU cyber strategy leaves key security gaps' Available at: https://globalriskinsights.com/2017/10/new-eu-cyber-strategy-leaves-key-security-gaps/ (Accessed May 17, 2018)

in favor of addressing cyber-threats accordingly. Digital single market is yet to be implemented. Much more is to be changed and overcome for having a truly effective cybersecurity strategy. After comprising the policy incentives suggested, if not asserted, by the securitizing actors, legal conditions under which securitization is being processed, and institutional solutions and reforms needed for the securitization of cyberspace to be fully conducted, the succeeding section will deal more thoroughly with the obstacles to these proposals, ergo securitization of cyberspace.

3.3. Obstacles to Adequate Securitization

After tackling down initiatives and proposals of relevant securitizing actors, this section will address the obstacles to effective securitization, an unavoidable 'handicap' in any further discussion. EU is facing numerous challenges, of which inter-institutional coordination occupies the first place, limiting its operational capacity embodied in human resources and financial investment. [124]

3.3.1. Resources and Classification

In January 2018, the head of the EU's cybersecurity agency, Udo Helmbrecht gave a speech at the conference hosted by the EESC wherein he devalued the outlined ambitions of the agency's aspirations in ongoing mandate implying how the agency's financial strength will continue to be limited due to the lack of additional resources needed for proper functioning of the agency. The European Commission itself admitted how ENISA "was not equipped with proportionally sufficient resources" whereas Mr. Helmbrecht affirmed these claims with the following statement: "My biggest challenge as executive director for the last years is prioritization… We will fulfil

[124] Christou, G. (2016) 'Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy', London: Palgrave.

everything which is in the proposed regulation. Full stop. But the regulation is very, let's say, 'generic'".[125]

EU does not classify cyber as a conventional threat, as the US does for instance. It is unlikely that EU army will be established any time soon, but it would be a significant shift towards defense of critical infrastructure, territory and integrity of the Union, far beyond the aspirations of the current Common Security and Defense Policy (CSDP) that does not cover collective defense of the EU territory. Moreover, there are arguably more difficulties securitizing cyber if not classifying it in the same category as weapons of mass destruction or global terrorism. This strategy of convincing the audience that cyberspace particularly is and continues to be an existential threat would be a more reliable option. Member States would find it challenging to cede their sovereignty on defense policy; as an illustration, David Cameron depicted such an idea impassable, claiming that "suggestions of an EU army are fanciful: national security is a national competence, and we would veto any suggestion of an EU army".[126] Necessity for creating an EU army is an ongoing debate and it surely does not mean that it would ease up the securitization of cyber in case of identifying it with the conventional threats, and new questions would arise: how will the cyber domain connect with classical military activities and will the military forces be in charge of cyber operations or will the new types of military forces be created? Excluding these limitations, there are far more fundamental concerns standing in securitizing actors' way.

[125] Teffer, Peter. "[Focus] EU Cyber Chief Says Expectations Exceed Resources." EUobserver. January 09, 2018. Accessed March 25, 2018. https://euobserver.com/digital/140481

[126] Besch, Sophia. (2016) "An EU Army? Four Reasons It Will Not Happen." Centre for European Reform. Accessed May 04, 2018. https://www.cer.eu/insights/eu-army-four-reasons-it-will-not-happen

3.3.2. Supranational – Intergovernmental Dichotomy

The Union does not hold responsibility for national security of each Member State, but rather serves as a platform for providing support to develop efficient national cybersecurity capabilities. At the same time when the EU-level capacities are being built, cybersecurity persists to be "almost exclusively a national prerogative".[127] However, uniqueness of this security-type, its complexity and transnational effects, has encouraged EU to take matter in its own hands and thus facilitate integration in every MS. EU believes that the legislation would make it easier for countries to receive security certification, which then becomes a practice with a potential to spread from one state to another trouble-free. Lower costs for firms and avoiding expensive application processes are guaranteed.[128] Additional impediment, from the Brussels perspective, revolves around the idea of convincing the Members to forge ahead with integration in this area. To some extent, a partial contradiction emerges; EU continues to insist on having a 'parent's role' stressing out the transnational nature of cyber issues and imposing legislative acts, while simultaneously encouraging decentralized organization of cybersecurity governance where the EU would have a secondary role of supporting capacity building, ensuring consistency and facilitating coordination and outreach.[129] The lawmakers of certain Member States have firmly opposed to a proposal that advocates pan-EU certification scheme that is superior to national ones. For instance, Germans dismissed parts of such proposal indicating how they would rather support a complementary European scheme which could be as beneficial for the sake of strengthening cybersecurity. The

[127] Renard, T. (2014a) 'Partners in Crime? The EU, its Strategic Partners and International Organised Crime', ESPO Working Paper No. 5, European Strategic Partnership Observatory., 13

[128] Stupp, C. (2018) 'Commission should 'walk the walk' on cybersecurity, German chief says' Available at: https://www.euractiv.com/section/cybersecurity/interview/commission-should-walk-the-walk-on-cybersecurity-german-chief-says/ (Accessed May 17, 2018)

[129] Ramunno, G. (2014) 'EU Cyberdefence Strategy'. European Union Military Committee, Vol. 6, May 2014., 1

French senate openly defied any motion that disproves exclusive competence of national authorities to deal with protection of Europeans in the cyber sphere, implicating thus how ENISA does not have competence to initiate certification schemes. Lastly, Czechs announced how ENISA "should primarily complement activities of the Member States in the area of cybersecurity and should not be aimed at taking over their competences in this area".[130] Clarifying background behind these statements (among others) lies in the fact that lawmakers are assured that the Commission's proposal to create a new system for certification would be slow and inefficient and that the better way to approach this matter would be by staffing up security teams tasked with protecting its internal systems against perpetrators instead of instructing MS what to do.[131]

Article 5 of the Lisbon Treaty plays a major role in cybersecurity discussion whereas its undeniable relevance needs to be thoroughly elaborated. The field of cybersecurity falls under direct control of its Member States whereas EU acts only if objective cannot be sufficiently achieved. To be expressed in a precise manner, principle of proportionality, stressed out in Article 5, declares that the content of EU activity must not go beyond what is necessary to achieve the objectives of signed Treaties. The succeeding one, principle of subsidiarity, asserts itself as a main legal compliance in the area that does not fall under exclusive competence of EU, claiming that the EU can only act if a certain proposed action cannot be achieved sufficiently under the scope of Member States; in which case preceding actions are conducted at EU level.[132] It is an everlasting battle between proponents of intergovernmentalism and supranationalism. Proponents of the first theory believe that states are uniquely powerful for having a legal sovereignty and political legitimacy as the only

[130] Teffer.
[131] Stupp.
[132] The Lisbon Treaty. "The Lisbon Treaty." Accessed March 27, 2018. http://www.lisbon-treaty.org/wcm/the-lisbon-treaty.html

democratically elected stakeholders in the integration process. The latter ones agree that intergovernmentalism does not reflect political reality as the EU institutions with all their law-making powers could offer a solution to intense cooperation and integration, cybersecurity included.[133]

3.3.3. Public-Private Partnership?

Digital-world infrastructure and its features are mostly privately owned, which can be problematizing for effective law enforcement mechanisms. Out of this, starting concerns emerge; do the public and private sector share the same notion of cybersecurity threats, per se? Are their interests overlapping enough for them to find common ground on subjects of major concern? In light of these questions, recent experiences regarding Facebook data breach incident gave EU lawmakers an additional reason to enact General Data Protection Regulation (GDPR), a binding legislative act. Facebook CEO, Mark Zuckerberg, went so far and claimed how GDPR will serve as an extension of the company's data privacy rules globally.[134] GDPR constitutes a major overhaul of privacy rules that includes all companies possessing personal data, and while being unique in the world, this regulation has a potential to set up a global standard, for it applies to "any Internet company that targets European consumers".[135] As this is a positive example of shared interests between private and government sectors, there are still some debatable issues concerning the expectations of each actor. The main responsibility of the state stays "generating security for citizens",[136] referring to its responsibility to cybersecurity as highly improbable for passing it to

[133] Wang, R (2007) 'The Fate of the European Union. Global Politics.' Available at http://www.global-politics.co.uk/issue2/archive.htm (Accessed May 17, 2018)
[134] Teffer, P. (2018) 'New EU privacy rules to benefit Facebook users globally' Available at: https://euobserver.com/science/141520 (Accessed May 17, 2018)
[135] Ibid.
[136] Carr, M. (2016) 'Public-private partnerships in national cyber-security strategies'. International Affairs, Volume 92, Issue 1., 44

the private sector. Expectations in terms of roles and authority tend to differ, as responses to cyber-threats seem to disperse remarkably, leaving the results of collaboration in cybersecurity governance patently limited.[137] Cybersecurity information-sharing between public and private sectors represents a noticeable obstacle due to a governments' lack of intention to distribute sensitive data for fear of compromising national security. Going further, private counterpart has a fear of unfolding business information, risking reputation and breaching data protection rules.[138] Pragmatic character of business policies relies on obtaining and selling information, rather than sharing it. Therefore, there is a long way ahead in a sense of strengthening public-private partnership; mutual trust and reverence is yet to be accomplished in favor of obtaining comprehensive and profound cybersecurity strategy.

3.3.4. Heterogenous National Perspectives

Things that tend to be mutual to all Member States in forming their own cybersecurity strategy are embodied in forms of identical threats and concerns. In contrast, dissimilar responses of Member States to these threats become visible when actualizing different levels of cybersecurity development within each one and the lack of trust among them.[139] Due to the lack of coherent European understanding of what notion of cybersecurity is, national actors possess disparate models of cybersecurity coordination at national level, which aggravates the choice of a model for information exchange. For instance, Estonia experienced one of the biggest cyber-attacks in modern history which is why today they are considered to be one of the most computerized nations with an emphasis on securing cyberspace and information systems for the sake of its citizens.

[137] Carrapico.
[138] EC Joint Communication. (2017), 7
[139] Carrapico. 1266

Experience taught them to develop measures of a civil character whereas UK, on the other hand, focuses its strategy on economy of innovation, investment and quality in the cyber field, for it allows them to fully exploit cyberspace.[140] Sharing the substantial information does not come natural to all Member States, which is an additional reason to proclaim cybersecurity as the sensitive area of cooperation; posing a significant challenge to securitizing actors. [141] National authorities managing the field of cybersecurity lack the coordination skills due to a dissimilar level of preparedness among MS, wherein important gap between rhetoric and practices continues to persist. Swift information exchange mechanism between all the institutions and connected actors affirms itself as crucial, and clarity on responsibilities and respective roles is required with the EU in aspiring role of the unifying security actor.[142] The OECD initiated a study in 2012[143] in which it described common features of national cybersecurity strategies. The report suggested how states do agree that cyber has become major priority of national security and that governments mostly tend to believe that the Internet and ICT are crucial for each national critical infrastructure as well as economic development and social prosperity. Moreover, international cooperation and coordination on both operational and policy levels is being emboldened while the need for flexibility is put as an additional priority. But, components such as political regime, economic development as well as sociocultural traditions were cited as the factors of influence for a nation to act upon cybersecurity matters. Political elites of some countries are constrained in regard to perception of differences between traditional threats and cyber-threats. Particularly, cyber-attacks

[140] Sliwinski, K. (2014) 'Moving beyond the European Union's weakness as a cyber-security agent' Contemporary Security Policy 35.3., 468-486
[141] Carrapico. 1267
[142] Argomaniz, J. (2009) 'When the EU Is the "Norm-taker": The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms'. Journal of European Integration, Vol. 31, No. 1, 125
[143] OECD. 'Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the Internet economy' 2012, Accessed March 29, 2018. https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

have a potential to be conducted on a scale impossible in the physical world (traditional attack able to impact one or two targets, cyber-attack hundreds or thousands), can be executed from anywhere in the world with a far more reach (far more data can be extorted in the digital world than ever possible in the physical world) and have a massive speed (single code that can target numerous sites in a matter of minutes).[144] The idea was that perceptions and actions on these delicate issues tend to differ from state to state whereby absence of forceful coordination is the catalyst of diverse understandings. Different national dispositions towards cyber thus alludes to be the last obstacle to effective securitization in this section.

[144] PGi. (2016) 'What is the difference between cyber crime and traditional crime' Available at: http://www.pgitl.com/explore/article/what-is-the-difference-between-cyber-crime-and-traditional-crime (Accessed May 17, 2018)

4. AFTERMATH: EFFECTS OF CYBER SECURITIZATION

4.1. Cyber Identity Building

EU has set up a goal to build up a resilient and sustainable future by protecting and investing in critical information infrastructures. This chapter is devoted to analyzing the effects of policies and initiatives taken by the actors and seeing how they contribute to implementation of cyber strategy. Overall approach of the EU is then put in comparison with the United States, a case wherein US is being construed as advanced and well-built cyber resilient country.

European Agenda on Security has a priority to ensure consistent and continued action in the field of cybersecurity, among terrorism and organized crime.[145] It focuses on improving information exchanges and operational cooperation between law enforcement authorities, thus greatly complementing cyber securitization efforts. The notion is that the EU can bring added value to support MS in ensuring security while nurturing collective European identity, in words of Juncker: "Combatting cross-border crime and terrorism is a common European responsibility".[146] All of the proposals in previous chapter serve to boost up security agenda but some of the initiatives within the Union, whether they are being conducted by political elites or by institutions, deserve a spotlight in this section. EU ministers of defense adopted Cyber defense policy framework in 2014 which emphasizes areas of high importance for developing cyber defense.[147] The agenda of this

[145] European Commission. (2018) 'European Agenda on Security' Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en (Accessed May 18, 2018)
[146] European Commission. (2015) 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions' Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf (Accessed May 18, 2018)
[147] Darmois, E. and Schmeder, G. (2016) 'Cybersecurity: a case for a European approach' Human Security Study Group, SiT/WP London., 15 Accessed May 1, 2018. http://www.securityintransition.org/wp-content/uploads/2016/02/WP11_Cybersecurity_FinalEditedVersion.pdf

framework that was developed by EC, EDA and EEAS includes prevention, detection, protection and information sharing, all the terms and phrases commonly used and often heard by the political elites and other relevant actors without further top-down specification of each suggestion and initiative. It is highly problematic to approach cyber concerns seriously without having a thorough elaboration on a certain issue, set expectations of a target group and a certain deadline. One of the other priorities discussed in the policy initiative concerns the enhancement of protection of "communication networks used by EU entities" whereas efforts should prioritize a unified doctrine of cybersecurity and defense covering all missions and operations.[148] Efforts of this framework are focused on the development of a unified doctrine of cybersecurity and defense covering all CSDP missions and operations at the strategic planning level. This could be a significant achievement in securitizing cyberspace as the audience could grow an idea of existentially threating concern. The EU Military Staff has already initiated the revision process of the EU concept for cyber to integrate in military affairs.[149] Actions like this are a sign of construing an identity, a cyber identity that has a productive and attainable strategy. The initiatives and policies as parts of security agenda do indeed assert the notion of enhancing the cyber strategy but can pose a risk of being awfully ambitious, and thus unattainable. For having a successful substantiation of proposed measures, proportional efforts in both theory and practice are to be made. An extensive set of legal, practical and supporting tools are being put in procedure, but the fact that EU still heavily relies on the success of information-sharing between stakeholders, cooperation, trust and mutual recognition of all MS, institutions and agencies, implementation of policies has a risk of being partly completed. This would mean that some time has to pass before EU establishes itself as a leading cybersecurity actor. Therefore, an attempt to build up a coherent and collective cyber identity is existent,

[148] Ibid. 16
[149] Ibid.

securitization of cyberspace is at its peak and we are yet to witness discussed initiatives push forward a cyber strategy of high efficacy.

Moving away from the adopted framework, over the course of last year (2017) European Union Institute for Security Studies (EUISS) formed a partnership with the Commission with a specific goal to promote strategic cyber capacity building among EU stakeholders. The purpose of this formed coalition is to convert ambitious guiding initiatives into "operational guidance for any EU external cyber capacity building action".[150] In doing so, the EUISS initiated the Cyber Capacity Building Task Force whose work is directed towards building functional and liable institutions to deliver enhanced cyber resilience of each Member State. Although the same ideas are recycling within EU policy propositions, and priorities do not tend to change, namely strengthening cooperation and effectiveness in cyberspace, forming a task force of experts could be a major leap for fostering international understanding of a common threat. Capacity building in cyber domain puts a focus on securing free, reliable and interoperable cyberspace while, more importantly, respecting human rights and the rule of law.[151] The gaps regarding EU cyber security do not only exist in literature on securitization of cyber but in methodology work of cyber capacity building as well, which is why this partnership has listed methodology as a top concern of its operational agenda. Additionally, the Task Force noted that handful of stakeholder consultations will be organized annually to have an input of each policy actor, practitioner and expert on cybersecurity for delivering concrete guiding solutions for further capacity-building actions.[152]

[150] European Union Institute for Security Studies. 'The Eurasian Customs Union: The Economics and the Politics | European Union Institute for Security Studies' March 26, 2018. Accessed May 01, 2018. https://www.iss.europa.eu/content/cyber-capacity-building-task-force-0
[151] Ibid.
[152] Ibid.

The efforts of European Defence Agency's (EDA) capability development plan have been recognized as well. The Agency has been actively developing cyber defense capabilities and research & technology, focusing on supporting MS and ensuring the availability of proactive cyber technologies.[153] Its agenda poses attention to both civil and military sector, giving advantage to R&T program which will be on military's disposal. Although cyber-threats rarely rise to a level where military's intervention is needed, companies tend to outsource cyber concerns to the military sector sometimes. Although it could be a positive trend in further securitization, it poses a risk of relying heavily on the armed forces to act on cybersecurity issues and thus reducing the incentives for business sector to develop lasting solutions. On EU level, these things do not occur due to a lack of armed forces. Instead, EU deals with cybersecurity issues by proposing and elaborating upon coherent cybersecurity policies.

Unquestionably, EU has set up an ambitious agenda to follow where the focus is put on building cyber capacity based on its internal experience. EU Member States remain in charge of creating their own national cybersecurity policies which partly contribute to enhancing joint cyber capability of the Union while having support of both Europol and ENISA. In the process of adjustment of each actor dealing with cyber, the Union has enacted legal changes needed for the securitization to fully succeed. For the agenda to be accomplished, "effective institutional and administrative cyber reforms" are to be implemented as well as "increased operational capacities of third countries".[154] As discussed in the previous chapter, major obstacle to adequate securitization pertains to be limitation of Article 5 of the Lisbon Treaty regardless of the legal and

[153] European Defence Agency. (2017) 'Cyber Defence' Available at: https://www.eda.europa.eu/docs/default-source/eda-factsheets/2017-09-06-factsheet_cyber-defence.pdf (Accessed May 18, 2018)

[154] Barmpaliou, Panagiota-Nayia. (2016) "The EU Experience in Global Cyber Capacity and Institution Building." News Item | Global Forum on Cyber Expertise. Accessed May 02, 2018. https://www.thegfce.com/news/news/2016/06/20/eu-experience-in-global-cyber-capacity

administration changes and institution-building process. Member States are the ones who decide on adopting all the proposed policies, technical and organizational measures and taking the concerns seriously. Besides these major actors, all the relevant stakeholders decide on their own approach and necessity for implementation of EU measures. The question of securitization has been differently processed in the United States and extensive set of lessons could be learnt from Washington.

4.2. How Far Ahead is the US?

Barack Obama, former president of the United States singled out cybersecurity as "one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter".[155] One of Obama's very first acts as a president was to commission a two-month review of US cybersecurity policy not only because the significant part of cybersecurity strategies has not developed in quite some time but because the sense of seriousness has become more evident and cyber threats have become tangible to many.[156] Necessity to tackle the threats emerged rapidly after the realization of economic losses caused by cyber espionage. The US military announced that future wars will most certainly include the exploitation of cyberspace whereby it will serve as a front field of incoming battles. Building up on this presumption, US military doctrine classifies cyber superiority as a precondition for the fruitful conduct of nearly any expeditionary operation.[157] From a logical standpoint, it is natural that US perceives cyber dominance through a military lens more prominently than the EU, simply

[155] Fayutkin, D. (2012) 'The American and Russian Approaches to Cyber Challenges' Journal of Defense Management, Vol.2, Issue 4., pp. 1. Accessed May 03 https://www.omicsonline.org/open-access/the-american-and-russian-approaches-to-cyber-challenges-2167-0374.1000110.pdf

[156] Porteus, H. (2010) 'Cybersecurity and Intelligence: The U.S. Approach' Publication No. 2010-02-E Ottawa, Canada, Library of Parliament. pp. 4. Accessed May 03, 2018. https://lop.parl.ca/Content/LOP/ResearchPublications/2010-02-e.pdf

[157] Fayutkin. 2

because EU does not possess military of its own, plus the US tends to perceive cyber capacities as a military might for which it spends annually three times more than the EU[158], and cyber threats are defined in the same category as conventional and non-conventional threats on top of that.[159] Having said that, US has an easier path to securitize cyber if classifying it in the same category as weapons of mass destruction or global terrorism due to having reliable strategy of convincing the audience that cyber space particularly is and continues to be an existential threat.

The focus of American cybersecurity revolves around establishing a front-line defense against threats by advancing US counter intelligence capabilities, expanding cyber education and developing strategies for deterring hostile activities in cyberspace.[160] The US, unlike EU, has already developed a top-down approach while relying on the capabilities of the private sector which has begun its searching for viable solutions to accordingly respond to previously adopted government directives. In narrow terms, American NIST[161] Cybersecurity Framework is a crucial element in delivering security to the citizens of US by "monitoring security on an ongoing basis with the use of automation tools."[162] The NIST Framework is an example of successfully initiated public-private partnership using collaborative and open development process to capitalize on the experience of both cyber and non-cyber stakeholders.[163] It is designed to address different risks and threats of each stakeholder, and is not implemented as one-size-fits-all approach for all critical

[158] The annual defense budget of the United States is $664 billion, EU spends $227 billion
[159] Fayutkin. 1
[160] Ibid.
[161] The National Institute of Standards and Technology (NIST) Cybersecurity Framework is of voluntary nature and consists of standards, practices and guidelines to manage cybersecurity risks. Its approach helps to protect critical infrastructure and other sectors of high importance to the national security and economy.
[162] Bentley, E. (2014) "Cybersecurity: What the U.S. Can Teach Europe." FCW – The Business of Federal Technology. Accessed May 09, 2018. https://fcw.com/articles/2014/08/07/comment-cybersecurity-us-and-europe.aspx
[163] Nicholas, P. (2017) 'More than just an ocean separates American and European approaches to cybersecurity' Available at: https://cloudblogs.microsoft.com/microsoftsecure/2017/05/17/more-than-just-an-ocean-separates-american-and-european-approaches-to-cybersecurity/ (Accessed May 18, 2018)

infrastructure organizations. The NIS Directive, on the other hand, is a result of trying to manage twenty-eight national cyber agendas which leads to a lack of shared understanding. NIST's voluntary nature and global adoption is more effective at preparing both sectors to improve risk management measures. The Framework was not only eagerly adopted by the federal sector, but it has become a template for companies to assess everyday security practices and consult globally. Continuous diagnostics and mitigation is perceived to be a preferable solution by IT professionals for the following reasons: reducing user disturbance and empowering business innovation with the initiation of automated security.[164] Moreover, continuous monitoring enables a practical solution for moving forward in cybersecurity sense, in addition to the fact that businesses have acknowledged the potential by voluntarily agreeing to adopt such solutions. On the other hand, the EU has some issues with securitizing cyber from the private sector aspect due to skeptic views on adopting the NIS directive. The main objection to full implementation and adoption of the Directive is that it is costly and not entirely effective to the case of their security. European cyber experts argue that the Directive is not as "specific as it needs to be" and that it will not "cause any meaningful change".[165] The higher the number of contrasting views (national dispositions toward cybersecurity), the higher the possibility of lacking preciseness. In experts' opinion, the Directive will not increase cyber-capabilities and will not help businesses to identify the risks. Moreover, transposition of the Directive to the national legislation of each Member State is still in the process wherein work on necessary legislative changes is needed, and in some cases, adoption of new

[164] Bentley.

[165] Perez, R. (2016) 'Industry skeptical of new NIS directive passed today' Available at: https://www.scmagazineuk.com/industry-sceptical-of-new-nis-directive-passed-today/article/531358/ (Accessed May 18, 2018)

cybersecurity laws.[166] Because of these reasons, the EU falls short in achieving valid and efficient cybersecurity strategy, and thus, fails to reach a level of securitization of cyber as the one in the United States. Although having ambitious policies on cyber agenda, human and institution resources, legislation and administration proposals, the Union has a long way to go before fully securitizing cyber and implementing sustainable cyber procedures. Lastly, the Union lacks encouraging ideas for businesses to follow, meaning that the efforts are not as developed and matured as in the US. Europe has inevitably taken a right direction of addressing cyber concerns, questioned and taken advantage of its potentials but it still has the open space to grow, learn and be inspired by the top-down approach that is being practiced in Washington.

[166] Shooter, Simon. (2017) "The NIS Directive: The Implications for UK Technology Businesses." Computer Weekly. Accessed May 07, 2018. https://www.computerweekly.com/opinion/The-NIS-Directive-the-implications-for-UK-technology-businesses

Conclusion

The focus of this research was to detect EU actors who seek to securitize cyberspace as well as their arguments. The extent of this question was to elaborate upon the obstacles that have prevented them to achieve this sufficiently. There is a great scale of credible speech act examples by which actors seek to convince the audience; whether that be a justification for enacting new legislations, proposing the establishment of institutions and policy changes, or cyber capacity building. Obstacles that were present ten or twenty years ago still stand in a way, but they pose a challenge to adequate securitization right now, not because more attention is given to the present challenges but because the Union is still in the process of cyber securitization which was arguably not the case a few decades ago. Cybersecurity policies still fall under the jurisdiction of each Member State, and while terminology comes to be more common among actors on all levels by the legislations that were enacted, the concepts of cybersecurity are in deficiency of shared understanding. The efforts of Member States to develop approaches are recognized but are still fragmented which is quite problematic when it comes to a problem that has global connotations and as such requires global solutions. European Union is primely an alliance of nations with diverse cultures and traditions. Led by 'United in diversity' motto and emphasizing such diversity by conducting concise policies and rules embodied in the Lisbon Treaty, each Member State has limited its sovereignty but not completely lost it. Given the fact that security matters are left to be under jurisdiction of nation states, it is hard to expect that one of the few remaining aspects of control will be aligned with the EU aspirations of having a unique approach to cybersecurity matters. The Union strives to coordinate responses to cyber threats, and it is visible through establishing new institutions and power sharing, but it declines in having a top-down approach, as it is the case in US, and succeeding in intact engagement of relevant stakeholders from areas where

an overlap of interest tends to prevail. Besides the fact that cybersecurity has become a profound expression of national interest and aspirations of EU as a supranational entity, securitizing connotations and frameworks were not disregarded. The advancement of information technologies has led to dissemination of security aspects needed to be addressed correspondingly. The securitization theory of the Copenhagen School enabled this research to suitably analyze cybersecurity strategy because the perception of security is signified as a "discursive modality with a particular rhetorical structure and political effects."[167] Moreover, securitization theory is a convenient approach for the cyber discourse, for it enables a fluent transition between the securitizing actors and referent objects from both private and public sectors. The success of carrying out an efficient cybersecurity strategy relies on the cooperation between these two, which is why a dissimilar understanding of cyber space and one-sided approach or concept-development of each relevant actor pose a challenge for satisfactory cyber policy on the EU level. Securitization of cyber has taken place in the EU and has not ended still. It has become all-inclusive, using all the tools on its disposal along the way and having far-reaching influence. To be successful, securitization should fulfill two conditions; securitizing actors with ample authority need to make a securitizing move and the audience requires to be convinced of a threat constructed by the actors. Firstly, several parts of this thesis provided patterns of actors' conviction to immediately address and act upon cyber issues. Discourse analysis used earlier presented several cases in which speech acts were existent, legislations were enacted, and policy proposals were issued, along with the existing support of the academic literature that go in favor of conclusion how cyberspace on the EU level has been securitized. Although Balzacq noted that "securitization sometimes occurs and

[167] Hansen and Nissenbaum. 1156

produces social and political consequences without the explicit assent of an audience"[168] this thesis asserts a notion that actors strive to convince as broader audience as possible. In this case, EU actors' efforts are directed to put on an agenda acceptable for all the Member States, meaning all EU citizens, whether that be academics who will elaborate and discuss on this issue on conferences or teach their fellow students, technocrats who will skillfully approach the rising problem and contribute to the development of cybersecurity strategy, the elites who will assist in the implementation of proposed policies and solutions, or citizens who will willingly support the ideas and back-up the securitization actors' threat construction. More so, the referent object shifted from the financial and individual security to the collective and national one; a threat construction matched with the expectations and ideas of the actors' speech acts. Bearing in mind that theory of securitization stays indifferent in answering questions 'how fast' and 'how conviction of the audience exactly occurs', it is uncertain to state anything on these matters. However, the observations made in this thesis will give a contribution to the existing literature by testing and successfully applying theoretical concepts and thus making it more relevant in the field of international relations. Although securitization of cyberspace does not belong to a firmly embedded notion of traditional security understanding of the Copenhagen School, this thesis detected securitizing actors and moves which place it up within the existing literature on the cyber securitization, a concept of security that has been reconceptualized. By absorbing a wide understanding and the connotations of what security encompasses, it is more likely to gain a profound comprehension of the security and what it presents to a targeted audience with different interpretations and understandings of it. As much as the securitization of cyberspace may not be a

[168] Balzacq, Thierry. 2008. "The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies." Journal of Common Market Studies 46 (1): 76

new phenomenon, it could possibly present a new experience to the targeted audience that has never been in the situation of facing with the securitization moves, approval of the proposed measures and experiencing its consequences directly. The concept of security is not something to be taken for granted, and knowing that, there will always be a case of an audience willingly accepting employment of the security as a political tool.

Bibliography

Alker, Hayward. (2005) 'Emancipation in the Critical Security Studies Project' In Critical Security Studies and World Politics, ed. Ken Booth., 181-187.

Andress, A. (2003). 'Surviving Security: how to integrate people, process, and technology' 2nd. Boca Raton: Auerbach Publications

Aradau, C. (2004) 'Security and the democratic scene' in: Journal of International Relations and Development (Vol. 7, No. 4) pp. 388–413

Argomaniz, J. (2009) 'When the EU Is the "Norm-taker": The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms'. Journal of European Integration, Vol. 31, No. 1, pp. 119–37.

Balzacq, Thierry. (2011) 'A theory of securitization: origins, core assumptions, and variants.' Securitization Theory: How security problems emerge and dissolve. New York: Routledge., 5-11

Balzacq, Thierry. (2008) "The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies." Journal of Common Market Studies 46 (1): 76

Barmpaliou, Panagiota-Nayia. (2016) "The EU Experience in Global Cyber Capacity and Institution Building." News Item | Global Forum on Cyber Expertise. Accessed May 02, 2018. https://www.thegfce.com/news/news/2016/06/20/eu-experience-in-global-cyber-capacity

Barnard-Wills, David and Ashenden, Debi. (2012) 'Securing Virtual Space: Cyber War, Cyber Terror, and Risk' in: Space and Culture (Vol. 15, No. 2), 110-123

Bendrath, R. (2001), 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection' in: Information & Security. Vol.7., 80-103

Bentley, Edwin. (2014) "Cybersecurity: What the U.S. Can Teach Europe." FCW – The Business of Federal Technology. Accessed May 09, 2018. https://fcw.com/articles/2014/08/07/comment-cybersecurity-us-and-europe.aspx

Besch, Sophia. (2016) "An EU Army? Four Reasons It Will Not Happen." Centre for European Reform. Accessed May 09, 2018. https://www.cer.eu/insights/eu-army-four-reasons-it-will-not-happen

Bigo, D. (2002) 'Security and Immigration: Towards a Critique of the Governmentality of Unease', Alternatives 27 (Special Issue): 63-92

Boros, Crina. (2016) "How the EU Cosied up to the Defence Lobby." EUobserver. Accessed March 23, 2018. https://euobserver.com/investigations/136310

Brattberg, E. and Rhinard, M. (2012) 'The EU as a Global Counter-Terrorism Actor In The Making'. European Security, Vol. 21, No. 4, pp. 557–577

Burkeman, O. (2009) 'Forty years of the internet: how the world changed for ever' The Guardian. Available at: https://www.theguardian.com/technology/2009/oct/23/internet-40-history-arpanet Accessed, May 15, 2018

Buzan, Barry. (1991) 'People, States, and Fear', London: Harvester Wheatsheaf

Buzan, Barry, Waever, Ole and de Wilde Jaap. (1998) 'Security: A New Framework for Analysis', Boulder. Lynne Rienner Publishers.

Bygrave, Lee A., and Jon Bing. (2017) 'Building cyberspace: a brief history of Internet', Oxford University Press, 32-37

Carr, M. (2016) 'Public-private partnerships in national cyber-security strategies'. International Affairs, Volume 92, Issue 1.

C.a.s.e Collective (2006) 'Critical Approaches to Security in Europe: A Networked Manifesto', Security Dialogue 37(4): 443-87

Carrapico, H., & Barrinha, A. (2017). 'The EU as coherent (cyber) security actor?' *Journal of Common Market Studies, 55*(6), 1254–1272.

Christou, G. (2016) 'Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy', London: Palgrave

Darmois, E. and Schmeder, G. (2016) 'Cybersecurity: a case for a European approach' Human Security Study Group, SiT/WP London. 5-23 Accessed May 1, 2018. http://www.securityintransition.org/wp-content/uploads/2016/02/WP11_Cybersecurity_FinalEditedVersion.pdf

Dekker, Marnix. (2018) "2018: The Year of the NIS Directive." Help Net Security. Accessed March 25, 2018. https://www.helpnetsecurity.com/2018/01/03/nis-directive/

Di Matteo, B. (2017) 'New EU cyber strategy leaves key security gaps' Available at: https://globalriskinsights.com/2017/10/new-eu-cyber-strategy-leaves-key-security-gaps/ (Accessed May 17, 2018)

Diez-Nicolas, J. (2015) 'The perception of security in an international comparative perspective', Royal Institute, Working Paper 16., 2-12

Duić, I. (2017). 'International cyber security challenges.' [online] Bib.irb.hr. Available at: https://bib.irb.hr/datoteka/878827.Duic_Cvrtila_Ivanjko_International_cyber_security_challenges_.pdf [Accessed 19 Mar. 2018].

Dunn Cavelty, Miriam. (2010) 'Cyberthreats, in M.Dunn Cavelty and V. Mauer (Ed), The Routledge Handbook of Security Studies', London: Routledge, 180-189

ETSI. (2018) 'Position Paper on Draft Regulation 2017/0225 "Cybersecurity Act"' Available at: http://www.etsi.org/images/files/ETSI_position_paper-CyberAct_20180206.pdf (Accessed May 17, 2018)

EU2017EE. (2017) 'EU cyber security conference 2017 – 14 September' Filmed [September 2017]. YouTube video, 5:34:11, Posted [September 2017]. Accessed March 21, 2018. https://www.youtube.com/watch?v=uY9d1hpoOvc

Eurasian Group. (2014). 'Cybercrime and Money Laundering.' [online] Available at: http://www.eurasiangroup.org/files/Typologii%20EAG/Tipologiya_kiber_EAG_2014_English.pdf [Accessed 14 Mar. 2018].

European Commission (2006) 'Communication from the Commission to the European Council of June 2006: Europe in the World- Some Practical Proposals for Greater Coherence, Effectiveness and Visibility', COM (2006) 278 final, 8 June.

European Commission. (2015) 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions' Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf (Accessed May 18, 2018)

European Commission. (2018) 'European Agenda on Security' Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en (Accessed May 18, 2018)

European Commission. (2017). 'Joint Communication to the European Parliament and the Council', Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. High Representative of the Union for Foreign Affairs and Security Policy, JOIN(2017) 450 final. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450

European Commission. (2017) 'President Juncker Delivers State of the Union Address 2017.' Accessed March 20, 2018. https://ec.europa.eu/commission/news/president-juncker-delivers-state-union-address-2017-2017-sep-13_en

European Commission. (2017) 'State of the Union 2017 - Cybersecurity: Commission Scales up EU's Response to Cyber-attacks.' European Commission - PRESS RELEASES - Press Release - State of the Union 2017 - Cybersecurity: Commission Scales up EU's Response to Cyber-attacks. Accessed March 20, 2018. http://europa.eu/rapid/press-release_IP-17-3193_en.htm

European Defence Agency. (2017) 'Cyber Defence' Available at: https://www.eda.europa.eu/docs/default-source/eda-factsheets/2017-09-06-factsheet_cyber-defence.pdf (Accessed May 18, 2018)

European Parliament. (2018) "Legislative Train Schedule." Accessed March 26, 2018. http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-eu-cybersecurity-agency-and-cybersecurity-act

European Parliament. (2017) 'The fight against cybercrime plenary sitting', Recorded on October 2, 2017, 28:44. Posted in October 2017. http://www.europarl.europa.eu/plenary/EN/vod.html?mode=chapter&vodLanguage=EN&startTime=20171002-19:35:39-573#

European Union Institute for Security Studies. (2018) 'The Eurasian Customs Union: The Economics and the Politics | European Union Institute for Security Studies' Accessed May 01, 2018. https://www.iss.europa.eu/content/cyber-capacity-building-task-force-0

European Union Institute for Security Studies. (2017) 'The EU's approach to cybersecurity capacity building abroad' Consultation with civil society, Accessed May 01, 2018. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCBII%20Programme.pdf

Europol. (2018) "About Europol." March 01, 2018. Accessed March 26, 2018. https://www.europol.europa.eu/about-europol

Fayutkin, D. (2012) 'The American and Russian Approaches to Cyber Challenges' Journal of Defense Management, Vol.2, Issue 4., 1-4. Accessed May 03 https://www.omicsonline.org/open-access/the-american-and-russian-approaches-to-cyber-challenges-2167-0374.1000110.pdf

Federal Register. (2013) 'Executive Order 13636: Improving Critical Infrastructure Cybersecurity' Available at: https://www.federalregister.gov/executive-order/13636.pdf (Accessed May 16, 2018)

Fischer, E. (2016). 'Cybersecurity Issues and Challenges: In Brief.' [online] Fas.org. Available at: https://fas.org/sgp/crs/misc/R43831.pdf [Accessed 19 Mar. 2018].

Goutam, R. (2015) 'Importance of Cyber Security' International Journal of Computer Applications, Volume 111, No. 7 Available at: https://pdfs.semanticscholar.org/5cfb/7a5bd2e6c181e8a69ebd49b1dadb795f493b.pdf (Accessed May 10, 2018)

Guzzini, S. (2011), 'Securitization as a causal mechanism' in: Security Dialogue, Vol. 42, No. 4-5., 329-341

Hansen, Lene and Nissenbaum, Helen. (2009) 'Digital Disaster, Cyber Security, and the Copenhagen School', International Studies Quarterly. Vol 53, no. 4, 1155-1175

IMF. (2017). 'Working Together to Fight Money Laundering & Terrorist Financing.' [online] Available at: https://www.imf.org/en/News/Articles/2017/06/21/sp062217-working-together-to-fight-money-laundering-terrorist-financing [Accessed 19 Mar. 2018].

Jain, N. and Shrivastava, V. (2014) 'Cyber crime changing everything – An empirical study", International Journal of Computer Application, Issue 4, Vol. 1, 76-80

Janes, P. (2012). Information Assurance and Security Integrative Project: People, Process, and Technologies Impact on Information Data Loss. SANS Institute, Available at: https://www.sans.org/reading-room/whitepapers/dlp/people-process-technologies-impact-information-data-loss-34032 [Accessed May 16, 2018]

Jonnalagedda, Sreelata. (2011) 'Revenue generation in the information era: Opportunities and challenges', IIMB Management Review, 51-56

Kasper, Agnes. (2014) 'The Fragmented Securitization of Cyber Threats', Springer International Publishing Switzerland, 157-162

Krimsky, S. (2007) 'Risk communication in the internet age: The rise of disorganized skepticism', Tufts University, Medford, Environmental Hazards 7., 157-164

Lean, T. (2016) 'Electronic Dreams: How 1980s Britain Learned to Love the Computer', Bloomsbury. Available at: https://www.historyextra.com/period/20th-century/a-brave-new-world-the-1980s-home-computer-boom/ Accessed May 15, 2018

Lewis, J.A. (2002) 'Assessing the risks of cyber terrorism, cyber war and other cyber threats', Washington DC: CSIS.

Mazzini, F. (2014) 'Cyber-Cultural History: Some Initial Steps toward a Cultural History of Digital Networking',Universita di Padova, Humanities 2014, 3, 185-209

McCusker, R. (2006) 'Transnational organised cyber crime: distinguishing threat from reality', Crime, Law and Social Change, 46 (4-5), 257-273

Meyer, C. (2017) 'Measuring the Impact of Cyberattacks: Lost Revenue, Reputation & Customers) Available at: https://www.securitymagazine.com/articles/87778-measuring-the-impact-of-cyberattacks-lost-revenue-reputation-customers (Accessed May 10, 2018)

Moravcsik, A. (2002) 'In Defence of the Democratic Deficit: Reassessing Legitimacy in the European Union', Center for European Studies, Working Paper No. 92, Journal of Common Market Studies, Vol. 40, Issue 04., 603-624

Nicholas, P. (2017) 'More than just an ocean separates American and European approaches to cybersecurity' Available at: https://cloudblogs.microsoft.com/microsoftsecure/2017/05/17/more-than-just-an-ocean-separates-american-and-european-approaches-to-cybersecurity/ (Accessed May 18, 2018)

OECD. (2012) 'Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the Internet economy', Accessed March 29, 2018. https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Oliner, S. and Sichel, D. (2000) 'The Resurgence of Growth in the Late 1990s: Is Information Technology the Story?', Journal of Economic Perspectives 14, no. 4, 1-3

Perez, R. (2016) 'Industry skeptical of new NIS directive passed today' Available at: https://www.scmagazineuk.com/industry-sceptical-of-new-nis-directive-passed-today/article/531358/ (Accessed May 18, 2018)

PGi. (2016) 'What is the difference between cyber crime and traditional crime' Available at: http://www.pgitl.com/explore/article/what-is-the-difference-between-cyber-crime-and-traditional-crime (Accessed May 17, 2018)

Podhorec, M. (2012) 'Cyber security within the globalization process', Journal of defense Resources Management, Vol. 3, Issue 1., 1-8

Porteus, H. (2010) 'Cybersecurity and Intelligence: The U.S. Approach' Publication No. 2010-02-E Ottawa, Canada, Library of Parliament. 1-6. Accessed May 03, 2018. https://lop.parl.ca/Content/LOP/ResearchPublications/2010-02-e.pdf

Raile, D. (2014). 'A look back at the first issues of Wired prompts the question: How far have we come?.' [online] Pando. Available at: https://pando.com/2014/07/15/a-look-back-at-the-first-issues-of-wired-prompts-the-question-how-far-have-we-come/ [Accessed 8 Mar. 2018].

Ramunno, G. (2014) 'EU Cyberdefence Strategy'. European Union Military Committee, Vol. 6, May 2014.

RAND Corporation. (2016) 'A framework for exploring cybersecurity policy options', Published Research, Available at: https://www.rand.org/pubs/research_reports/RR1700.html (Accessed May 16, 2018)

Renard, T. (2014) 'Partners in Crime? The EU, its Strategic Partners and International Organised Crime', ESPO Working Paper No. 5, European Strategic Partnership Observatory.
Schmidt, H.A. (2011) 'The Administration Unveils its Cybersecurity Legislative Proposal' Available at: http://www.whitehouse.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal (Accessed May 16, 2018)

Shooter, Simon. (2017) "The NIS Directive: The Implications for UK Technology Businesses." Computer Weekly. Accessed May 07, 2018. https://www.computerweekly.com/opinion/The-NIS-Directive-the-implications-for-UK-technology-businesses

Singer, P.W. and Friedman, A. (2014) 'Cybersecurity and Cyberwar – What everyone needs to know', Oxford University Press, New York. 12-26

Sliwinski, K. (2014) 'Moving beyond the European Union's weakness as a cyber-security agent' Contemporary Security Policy 35.3., 468-486

Smith, S. (2005) 'The Contested Concept of Security'. In Critical Security Studies and World Politics, ed. Ken Booth, 27-62

Stupp, C. (2018) 'Commission should 'walk the walk' on cybersecurity, German chief says' Available at: https://www.euractiv.com/section/cybersecurity/interview/commission-should-walk-the-walk-on-cybersecurity-german-chief-says/ (Accessed May 17, 2018)

Teffer, Peter. (2018) "EU Cyber Chief Says Expectations Exceed Resources." EUobserver. Accessed March 25, 2018. https://euobserver.com/digital/140481

Teffer, P. (2018) 'New EU privacy rules to benefit Facebook users globally' Available at: https://euobserver.com/science/141520 (Accessed May 17, 2018)

The Lisbon Treaty. "The Lisbon Treaty." Accessed March 27, 2018. http://www.lisbon-treaty.org/wcm/the-lisbon-treaty.html

Valeriano, B. and Maness, R. (2018). 'International Political Theory and Cyber Security.' In the *Handbook of International Political Theory*. Oxford University Press., 259-269

Van der Meer, S. (2016) 'Defence, deterrence, and diplomacy: Foreign policy instruments to increase future cyber security' Available at:

https://www.clingendael.org/sites/default/files/pdfs/book_securing-cyberspace-chapter_July2016.pdf (Accessed May 16, 2018)

Wæver, Ole. (1995) 'Securitization and Desecuritization' In On Security, ed. Ronnie Lipschutz. NY: Columbia University Press., 50-58

Walt, Stephen. (1991) 'The Renaissance of Security Studies.' International Studies Quarterly. Vol. 35, No. 2, pg. 213

Wang, R (2007) 'The Fate of the European Union. Global Politics.' Available at http://www.global-politics.co.uk/issue2/archive.htm (Accessed May 17, 2018)

Wiener, A. (2018). 'On Reading Issues of Wired from 1993 to 1995.' [online] The New Yorker. Available at: https://www.newyorker.com/culture/cultural-comment/on-reading-issues-of-wired-from-1993-to-1995 [Accessed 2 Mar. 2018].

Williams, Michael C. (2003) 'Words, Images, Enemies: Securitization and International Politics' International Studies Quarterly 47: 511-31

Wong, A. (2016). 'Cybersecurity: Threats, Challenges, Opportunities.' [online] Acs.org.au. Available at: https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf [Accessed 12 Mar. 2018].

Woodward A., Williams P.A.H. (2015) 'An Uncomfortable Change: Shifting Perceptions to Establish Pragmatic Cyber Security'. In: Unger H., Meesad P., Boonkrong S. (eds) Recent Advances in Information and Communication Technology 2015. Advances in Intelligent Systems and Computing, vol 361. Springer, Cham., 1-8

Zbiral, R. (2009) 'Agencies of the EU: The Emerging Network of Supranational Administrative Bodies' Contemporary Administrative Law Studies, Vol. 4, No. 1., 171-192