Securitization of Cyber Space in the United States of America, the Russian Federation and Estonia

By

Katarina Klingova

Submitted to
Central European University
Department of Political Science

In partial fulfillment for the degree of Master of Arts in Political Science

Supervisor: Paul Roe
Budapest, Hungary
(2013)

Abstract

This research elaborated the difference in securitizing discourse of cyber security. The Copenhagen School's theory of securitization, in particular the three discourses of securitization of cyber space presented by Lene Hansen and Helen Nissenbaum, serve as the theoretical framework for this study. This paper uses the method of content analysis of the latest cyber security strategies of the United States, the Russian Federation, and Estonia as the official securitization speech to analyze the prevailing securitization discourse in these countries. The case selection is not random as the three analyzed countries are the leading nations in the securitization of cyber space. The results of the manual coding of official doctrines as well as of the frequency tables of the open source software Raw Text to Tag Cloud Engine show that securitizing frameworks of cyber securities differ among the three analyzed countries. The securitization of daily life discourse is the most prevailing in the doctrines of the United States and Estonia, while the Russian strategy is a hypersecuritization framework. The analysis showed the difference in terminologies used and in the comprehension of cyber space. While both Estonian and the U.S. strategies distinguish between the expressions "cyber" and "information", the Russian strategy uses the term "information" for both concepts.

Acknowledgements

I would like to thank Professor Paul Roe for his constant support in all the levels of the development of this research. A student is nothing without a good advisor, the one that listens, suggests, encourages and help.

My patient friend Lara for all the help with revision.

Last but not least to my beloved grandmother.

Table of Contents

Introduction

In the beginning of March, 2013 the Czech Republic was attacked by an anonymous group of hackers that temporarily, for a very short time, crashed and disabled access to numerous websites of public institutions, banks or Internet portals (B.C., 2013). The most recently reported attacks, May 2013, in cyber space have been connected with the conflict in Syria when the 'Syrian Electronic Army' was accused by Israel of attacking the water system in Haifa, the third largest city in Israel (The Daily Star Lebanon, 2013) for contemplation of applying cyber strategy against Syrian governmental forces (Finan, 2013). The attacks on information and communication technology systems, portals and databases of various institutions from the governmental or private sector have become increasingly dangerous and more common. The rising debate connected with attacks and disruptions occurring in cyber space questions what measures are pertinent for the international actors to take, in traditional perceptions of security, and what appropriate measures the states should take in order to tackle successfully and withstand the cyber attacks.

Cyber space has become one of the most pressing and prominent national security issues. Due to the high dependency and vulnerability to any kind of disruptions in critical infrastructure networks, any cyber attack or computer malware is highly publicized by media. With the rise of the Internet and technification of societies, many states want to acquire offensive cyber weapons. Mariam Dunn Cavelty and Thomas Rid show that there is an overestimated focus on strategic-military aspects in cyber space that creates an antagonistic zero-sum game in an area where there is no identifiable enemy. Thus, framing of the threats and risk perceptions have not only in

the past decades became a matter of choice, but are deliberate results of political and social effects as well (Dunn Cavelty, 2012b; Rid, 2012).

The term cyber space refers to "the fusion of all communication networks, databases and sources of information into a vast, tangled and diverse blanket of electronic interchange. [It is a 'network ecosystem'], which is virtual and immaterial, a bioelectronics environment that is literally universal" (Dunn Cavelty, 2012a, p.155). However, there is no universally accepted definition or international norms that set the code of conduct in this digital sphere. This lack of uniform standards and security perception are the object of analysis. The focus and main objective of this thesis is to provide an analysis on how different countries securitize cyber space.

For the purpose of this study I use the Copenhagen School's of security studies theory of securitization, which states that security is created by a speech act that 'securitizes' a particular issue as a survival threat towards a referent object, and therefore this object is in grave need of protection against the particular threat. However, pronouncement of the word *security* does not constitute the speech act. It is the acceptance of securitization of particular issue as an existential threat, the acceptance of the emergency issues proclaimed by securitizing actor by the audience, that establishes securitization (Buzan et al. 1998).

In my research, I apply three discourses of securitization introduced by Lene Hansen and Helen Nissenbaum (2009). Hansen and Nissenbaum identified three discourses with different objects of reference and specific forms of securitization grammar, and specific speech acts of securitization. Accordingly, cyber security has three different security modalities: hypersecuritization, everyday security practices, and technifications. The Copenhagen School's theory on securitization provides a suitable

theoretical platform for my analysis of cyber space's 'securitization', because it perceives security as a "discursive modality with a particular rhetorical structure and political effects" (Hansen and Nissenbaum, 2009, p. 1156).

Thus, following the "facilitating conditions" for the speech act, I applied method of content analysis to three official cyber security doctrines, securitizing speech acts, of the selected states, specifically the United States, the Russian Federation and Estonia. The content analysis of particular securitizing strategies enabled me to elaborate how these three states conceptualize and grammatically construct the threats and vulnerabilities in cyber space. In other words, I studied what kind of securitizing discourse is predominant in these securitizing doctrines, and thus provided answers to my hypothesis that the securitizing discourse in cyber doctrines of the analyzed countries is different. Indeed, the selection of the analyzed countries was not based on the random selection. The United States, the Russian Federation as well as Estonia are significant players and actors shaping the framework of cyber space's securitization. Furthermore, political scientists such as Stephen van Evera effectively show that small case-oriented research can serve five main purposes of: "testing theories, creating theories, identifying antecedent conditions, testing the importance of antecedent conditions, and explaining cases of intrinsic importance" (1997).

My research starts with an extensive literature review on cyber space and security in it. I show the reader that the utility of information gathering methods has been part of warfare for centuries. However, the ideas of attacks, spreading of malicious software and espionage have extensively developed with the spread of modern technologies and computers into every aspect of human lives. The second chapter elaborates securitization theory and its three 'securitizing' discourse of cyber space, which were applied in my content analysis of three securitizing speeches – the official cyber

security doctrines of the United States of America, the Russian Federation and Estonia. This thesis provides an insight and elaborates how the analyzed countries securitize cyber space differently, what securitization discourse of cyber space is predominant and whether there is a common understanding of action and measures among the analyzed countries.

Chapter 1: Literature review on security in cyber space

This chapter focuses on a brief overview of the development of cyber space, the importance of information in military, perception of security, understanding of actors, numerous possibilities attacks and elaborations, while highlighting at the same time the aspects of the theory that are of crucial importance for the present study and further analysis.

Intelligence

The warring parties have been for centuries implementing two tactics - either overwhelming their opponent with mass and firepower, or outmaneuvering them with speed and agility. It was successful espionage and decoding that were crucial in shaping historical developments (Berkowitz, 2007). Espionage and intelligence gathering lead to many victories and were incorporated as important elements of battle strategy. Thus, intelligence became one of the central components of military machines (Ferris, 2010).

Interception of the Zimmermann telegram resulted in the declaration of war by the United States on Germany in the First World War. Signal and information intercepting technical devices have been those such as Ultra, which British intelligence used to intercept the Luftwaffe plans, the code breaking device Magic that led to the victory of the United States at Midway against the Japanese or even enigma, among others. The command of the information networks and transmission cables have proved to be an important and crucial asset in wining the World Wars and other battles. It is impossible to deceive and surprise your enemy who knows your every move from decoding secret cables. Indeed, the United States learned it the hard way when a Navy petty officer, Johnny Walker, gave the KGB in 1967 keys to

American ciphers (Berkowitz, 2003). However, this kind of intelligence breach is very unique and requires 'close access', an informer with inside access into the system. Therefore, cyber space, with its intelligence and information gathering is not the only weapon that can take down the whole country, but it is only one element, an important one, of the more comprehensive strategy (Ferris, 2010; Berkowitz, 2007).

The development of modern warfare bought with it the development of new fighting techniques, strategies, new weapons and rising reliance on and use of intelligence in the fighting and decision taking. John Ferris intriguingly describes intelligence as "the collection, collation and analysis of information" in order to effectively evaluate the situation and decide on the tactics, resources and measures that need to be taken against the opponent. Intelligence is not the sole thing that wins the combat, but it is a significant force multiplier that can be decisive element in wining the battles and toppling opponents (Ferris, Ashgate Chapter 7, p. 109). While the technological development and exponential growth of the World Wide Web have just enhanced the possibilities of breaching opponent systems and reaching the data, even a grand cyber attack has to be part of a bigger strategy on how to win a war or beat the opponent in the decision cycle (Berkowitz, 2007). Indeed, software attacks and intelligence gathering in cyber space would be of the greatest benefit in conjunction with conventional warfare practices (Rid and McBurney, 2012).

The launch of the Advanced Research Projects Agency Network (ARPANET) by Massachusetts Institute of Technology, Stanford and Berkley in 1969, as a network connecting universities, started the age of the Internet and the global proliferation of information technologies (Weber, 2012), with rising possibilities of collecting, storing, processing and consequently exploiting information for illegal processes. The idea that digital information can pose a threat dates back to 1976 when Thomas Rona

delivered a report *"Weapons Systems and Information War"* to Boeing in which he coined the term "information war" (Rona, 1976). Thomas Rona in his report captured the increasing dependence of people, the whole international system, on information technology that gradually posed a new set of strategic vulnerabilities. Rona's report ignited the gradual development of the IT-based offensive techniques and retaliation possibilities within the structures of the U.S. military and the U.S. Department of Defense (Dunn Cavelty, 2010b).

Espionage and covert affairs have been part of international relations and international criminal activities for a long time in history. The United States of America has even a legal definition of what a covert action is. According to the United States' Code, Title 50, Chapter 15, Paragraph 413b of Presidential approval and reporting of covert actions, Subchapter 'e' defines covert action as "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly." However, this legal definition precisely states that a covert affair does not include "activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities" (The United States Code 50, § 413b). Consequently, covert activities are not perceived in the legal code of the United States and its administration as deniable activities.

Consequently, in recent years the topic of cyber attack and information warfare has been attracting a rising number of experts and more public attention. Increasing dependence of societies on information technology increased the potential of threats and vulnerabilities posed by cyber space. As Berkowitz points out, the network

warfare in cyber space combines the idea of asymmetric threat introduced by Marshall and Wohlstetter (2007), Rona's idea on the change of the nature of war due to information technology (1976), Boyd's example of beating the opponent's decision cycle, and Arquilla and Ronfeldt's (1993) idea of cyber war using the interconnected digital communication networks.

However, it was the Desert Storm operation that brought the idea and opened the possibilities of network armies using network communication systems as radio waves or satellite. The idea of 'cyberwar' was born (Berkowitz, 2003). The digital communication, transferring the message as an electromagnetic analogue of itself, advantages of package messaging, and the ability to transmit information via any continuous chain within the network, not depending on a pre-specified route, lead to exponential growth of the Internet network. Not only almost every aspect of our lives became dependent on the efficiency of electronic networks, but its dependency had a price. As Berkowitz points out, "decentralized, digital communication systems were a key technology that made network warfare possible" (2003, p. 74). In the present time, it is the communication networks that shape the action of armed conflicts.

Network warfare in cyber space is based on century-old ideas of spyware and combat. These ideas came together and were elevated to the new dimension of cyber network or space, and thus changed the perception of warfare, its organization and the rules of the game. The stealth and control of information or networks became the base ground for modern warfare. Therefore, an ultimate well-planned strike on the network of a particular country can be more important than the pure power and arsenal of the opponent. Thus, the cyber space and the protection of vulnerabilities within it are becoming increasingly important, as every aspect of human life is becoming exponentially dependent on modern technologies (Berkowitz, 2003, p. 74-75). Many

authors and politicians, such as former U.S. Defense Secretary Leon Panetta, have spoken about possibilities of an "electronic Pearl Harbor" and other catastrophic attacks on crucial networks that could lead to large-scale destabilization of particular countries (Panetta, 2012). However, in order to be able to understand what kind of challenges and threats are posed by the cyber threat, its definition and comprehension is first necessary.

Definition of cyber space, main actors and their motivations

The prefix 'cyber-' originated from the word cybernetics and its literal meaning is 'through the use of a computer.' The label cyberspace encompasses "the fusion of all communication networks, databases and sources of information into a vast, tangled and diverse blanket of electronic interchange. [It is a 'network ecosystem'], which is virtual and immaterial, a bioelectronics environment that is literally universal" (Dunn Cavelty, 2012a, p.155). Some authors, such as Matt Murphy from the Economist, perceive cyber space as the "fifth domain of warfare, after land, air, sea and space (Murphy, 2010). However, there is no one single definition of cyber space. The most common misperception is to compare it to the World Wide Web, but there is more to it than meets the eye than opening up the Internet Explorer. Cerf points out that broadly defined cyber security refers to protection of data or any devices against any kind of corruption or harm, whether methodical or accidental by using a computer-based network (Cerf, 2011).

The lack of homogenous understanding of what is perceived as the threat in cyber space, the lack of overall control, enforcement of certain cyber codes of conduct or rules, or the high inability to punish perpetrators are obstacles that make the prevention and protection against cyber attack even more difficult. While the

possibilities of any hacker to 'attack' using the world wide net are numerous, the main dangers are identified as cyber crime, cyber terrorism and cyber war (Swiatkowska, 2012).

Bruce Schneier differentiates between cyber-vandalism encompassing actions from non-disruptive use of the Internet for a particular cause, to the defacing of websites and cybercrime, a term comprising theft of intellectual property, identity theft or threat of 'distributed denial of service' attacks. Schneier also recognizes cyber-terrorism as a cyber activity, as for example hacking into a computer system with the purpose of causing various types of malfunctions or catastrophes, such as, collision of planes or a nuclear power plant melt down. Last, Schneier defines the concept of cyber war to refer to "the use of computers to disrupt the activities of an enemy country, especially carrying out deliberate attacks [for example] on communication systems. [Narrative of cyber war] resembles the concept of 'computer network attacks, which is part of the official [national] information operations doctrine and … [implies] the use of the computer networks to disrupt, deny, degrade, or destroy information [stored within the networks and databases of hostile regimes, computer networks or particular computers]" (Schneier, 2007).

However, the definition and perception of cyber warfare differs among the experts. Cyber warfare can be identified by policy makers as "information warfare conducted in the 'fifth domain' - the cyber space" (Skala, 2011). While Richard Clarke, former White House national security and counterterrorism aide, contemplated large scale attacks that would within a few minutes disable the whole operation networks and functioning of countries; or Mike McConnell who anticipates and compares international warfare and attacks within cyber space to attacks of nuclear weapons,

information technology experts such as Bruce Schneier criticizes these kinds of "securocrats of scaremongering" (Murphy, 2010).

Indeed computer security experts Thomas Rid and Peter McBurney define a cyber weapon as "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings" (2012, p.7). In principle any instrument of code-born intended attack is a cyber weapon. It is the presence of external intention of an actor that distinguishes an attack from an accident. However, it is possible to rate cyber weapons according to the spectrum of capabilities. While some malicious softwares are not capable of breaching the system and creating systematic changes or disruptions, and thus represent a low-potential damage weapon, other malwares autonomously are capable of infiltrating physically isolated systems and reprograming the output processes to causing large-scale damages and harm. Those are the intelligent agents capable of autonomous analysis and assessment of the systems they breach, and later reprogram or damage, that represent the most sophisticated cyber weapon and attack on high-profile targets.

Furthermore, another distinction of these damage-seeking malicious software and codes is that they create malfunction within the breached computerized control systems that enables them to influence subtly the targeted system or cause its malfunction to appear as a software bug of the system itself. A sophisticated and stealthy attack is not weaponized, does not explode or causes physical damage itself. It is the infiltrated system's potential of physical damage that is utilized in such a way that it does not trigger investigation and suspicion of external intrusion. So far there have been only three 'known sophisticated weaponized' cyber attacks; the malfunction of Soviet pipeline in 1982 and Stuxnet worm belong in this category.

These kinds of target specific intrusions require extensive preparation, funding and long-term planning, thus they are highly improbable and extremely rare. However, most of cyber malwares have the generic attack function to overload the servers of breached systems or website, as they do not damage or shut down completely the penetrated system.

Indeed, while large-scale cyber attacks on crucial networks can have massive implications on the lives of ordinary people and cyber warfare, such as Stuxnet virus; they can also enhance conventional military power. No casualties as the result of cyber attacks yet have been reported (Bronk, 2013). From the technical point of view, cyber attack is a sequence of zeros and ones, a program or a code breaching the firewalls and other protective measures of secured networks in cyber space. In comparison to the Cold War or Pearl Harbor, no human casualty has been reported yet as the result of cyber attacks. Indeed, as Thomas Rid points out, the only large-scale cyber attack causing physical damage was the U.S. government launched Stuxnet (2013). Therefore, computer security experts, such as Bruce Schneier or Thomas Rid, argue that while it is possible to observe cyber-conflict, cyber-war is ultimately connected with launching real missiles. In addition, from the point of view of computer science, cyber attack is omnipresent, because it is ultimately defined as any "attempt to subvert the function of a system"(Bronk, 2013). As Rid and McBurney remarkably point out, "even a highly sophisticated piece of malware that is developed and used for the sole purpose of covertly extracting data from a network or machine is not a weapon, [neither is a computer bug]" (Rid and McBurney, 2012, p. 11).

According to the general notion, cyber space refers to activities that involve the use of computers and other electronic devices and thus make a distinction between the electronic and physical world. Vinton Cerf points out that the pattern of behavior and

rules of conduct in cyber space are copied from the one implied in the physical world, real-world activities and behavior, and they serve as a model for society's cyberspace counterpart. Generally people try to comprehend new concepts via comparisons to past events or comparisons to real-world counterparts. While on the one hand using this kind of terminology is very convenient, its applicability is limiting and often misleading, because traditional physical principles do not apply for cyber space. Although many cyber intrusions or cyber attacks have analogies in the real world, in cyber space it might not often be apparent whether corruption of the system was a deliberate act, a software malware for example, or a violation of law (Cerf, 2011).

The security experts such as Dunn Cavelty (2012b, 2010), Bruce Berkowitz (2007) or Lunt, Rowe and Ekstrom point out that the incentives of the attackers can be categorized depending on the perpetrators as elaborate cyber crimes of internationally organized groups such as the national espionage agency; loosely-organized groups such as Lulsec or Anonymous; and individuals that are often labeled as lone wolves. As it is possible to observe below in Table 1, a similar typology of cyber actors is offered by Khaliza in 1998.

Table 1: Typology of actors in cyber space

Type	Subtype	Goal
Individuals	Grey hats	Mayhem, joyride, minor vandalism
	Black hats	
Coordinated sub- or pan-national groups or networks	Criminal groups	Money, power
	Terrorists (political)	Gaining support for and deterring opposition to a cause
	Hacktivist (anarchistic/millennial)	Protest, fear, pain, disruption
	Insurgent groups	Overthrow of a government or separation of a province
	Commercial organization	Industrial espionage, sale of information
State	Rogue state	Deterring, defeating or raising the cost of a state's involvement in regional dispute
	Peer competitor	Deterring or deferring a country in a major confrontation, espionage, economic advantage

Source: Adapted from Khalilzad (1998)

Cyber threats

Indeed, the Internet was not designed for security. It is important to remember that originally, from the technical point of view, computers were designed for personal use or work within a very secluded network. A personal computer was not designed to be connected to the Internet, thus it is important to appropriate the rules of engagement and distinguish the lines between personal and 'common' property (Berkowitz, 2003). And with the organized international criminal organization specializing in harvesting of data, malware explosion or installation of 'back doors' to various networks and computers of innocent citizens, the potential of criminal activities and their large-scale implications are vast and had eventually changed the way warfare is conducted. For example, China has been increasingly enhancing its potential of cyber offence and has been repeatedly accused by the Western countries of wholesale espionage. Chinese 'hackers' and cyber attacks have been primary focused on the computers of major Western defense contractors. The classified blueprints of the F-35 fighters, that will

be the backbone of the U.S. Air Force, have been the primary objects of interest of the Chinese (Murphy, 2010).

Indeed, the objectives to conduct intrusions and breaches to computer networks are numerous and depend on the motive and identity of the intruder. The main purposes of 'attacks' in cyber space are primarily the acquisition of information and data. This is connected with military and economic espionage: the acquisition of control of a computer in order to launch denial-of-service attacks against other computers or websites; compromise a number of computers in order to create a 'botnet', robot networks of zombie computers in order to fight other computer hackers or launch large-scale attacks against particular websites; along with extortion and many other goals. The possibilities of cyber space are enormous. The basic principle is to take full advantage of the corrupted computer, without necessarily alarming the owner about the intrusion (Cerf, 2011).

While the truly protected and safe would be those outside of the network, the network itself is not a target. At the same time no special skill-set or big initial cost of hardware technology are necessary to launch a potentially devastating breach into secured networks. A number of hacking programs are easily accessible and ready for download on the Internet. Furthermore, it is important to remember, "that there is no such thing as an uninteresting target" (Lunt et al, 2012, p.23). Information and control of the network are very attractive too for various reasons.

A launch of a massive attack in the virtual world of cyber space might have several motivations such as:

- Intellectual property theft;
- Service disruption;
- Financial gain;
- Equipment damage;
- Critical infrastructure control and sabotage;
- Political reasons (Hacktivism);
- Personal entertainment (Lunt et al, 2012).

One of the most common ways to intrude into a foreign network is by implementing a computer virus. The term was originally coined by Fred Cohen in 1984 who wrote and released a computer virus in his university network. A computer virus uses the analogy from biology and it is a self-replicating program. Microsoft defines computer virus as "a software program that is designed to spread from one computer to another and to interfere with computer operation… such as corrupt or delete data on your computer, use your email program to spread itself to other computers, or even erase everything on your hard disk" (2013). A similar mission has the computer worm, which is a sub-category of a computer virus. The difference is that a computer worm replicates itself and moves from one computer to another without any human action involved. Computer worm's replicating and traveling capabilities across the system network or Internet "result in most cases in a worm consuming too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding" (Beal, 2013).

The attempt to breach a network with the intentions to get hold of sensitive data and other information is the goal of most hackers. However, not all hacking has to have negative connotation and implications. The 'distributed denial of services' (DDOS) viruses that scan the World Wide Web for computers with inadequate firewalls, in other words, they seek computers with weak protection. These computers are vulnerable to viruses and other intrusion thus they could potentially be used as an innocent medium to breach into other systems and could me misused for a criminal activity. Indeed the distributed denial of services viruses take control over the infected computers, then stay put, but once activated they turn breached computers into zombies fully under the control of a hacker (Rid, 2012).

The arduousness is that a virus is hard to detect and furthermore any computer connected to the World Wide Web is a possible target and could be taken advantage of. Another example of misuse of the software program occurred in 1995, when former Marine and soldier in the First Gulf War, Dan Farmer, developed a free software program named System Administrator's Tool for Analyzing Networks (SATAN). This program was designed for the system operations to examine the particular network and detect any weak configurations that could enable intrusions by outer forces. However, at the same time it could be used by outer parties to find out the potential weak point, through which they could breach the network. In addition, in this case of the program, it is possible to observe the impact of the language and name on the success and visibility it received due to its name. The power of its acronym, the imagination and symbol it represented, made it even more famous. Indeed, as Farmer proclaimed: "The technology by itself, if no one knows about it and no one uses it, is pretty useless" (Kerstetter, 2005). Riptech Inc., after a merger in year 2002 with Symatec, has been once of most successful managers of computer security services

and operator of ‘server farms’. The company provides large industrial computers that host hundreds of websites and monitors the computer networks of thousands of computers of its costumers. Riptech Inc. has been specializing in ‘computer forensics’ developing a program that would provide analysis tracing the steps of the violator and identifying the points of entries, the weaknesses of systems and firewalls. Symatec’s data is based on diagnostics of its customers and its computer monitoring system. While for example the U.S. Computer Security Institute gets its data from surveys and questionnaires it sends to various companies, Symatec uses data-mining to detect patterns and trends within the millions of login attempts from firewalls of websites it operates. While this provider of computer security can detect and trace the intruder, the true identity and motive of hacker could be still an undetectable if the hacker is using a zombie computer of innocent bystander as a cutout.

Furthermore, in order to find out the intentions of particular attacks, security providers would have to go through the system logs and repeat every command and so re-create the session of one intruder attempting to breach in to one website or network. However, re-creation of millions of logs and attempts to breach into the networks via their-party corrupted personal computers would take not only hundreds of qualified personnel, but also a lot of time, while at the same time new breaches are taking place. Nevertheless, these network security providers are responsible for mending the hole, finding the weakest node in the system and repairing it, but the results of their diagnostics tracing back to intruders belong to their clients. Therefore, if the client does not want to inform the responsible governmental security organization of a cyber attack, no crime is reported (Berkowitz, 2003; Symatec, 2013).

As the potential attacks on the government website or attempts to breach operating systems for governmental agencies and security services could be expected, most of

these networks have the highest security measures. That said, the protection of civilian systems and of all the networks that control them and have an impact on human life is a bit more difficult. The military communications and computers are obvious targets of adversaries, but the majority of military communication, though a secured network, is provided via vulnerable commercial links connecting nodes, or particular households, with each other. The protection of the whole communication or power network is literally impossible. Indeed, the critical infrastructure run by SCADA systems, as computer experts argue and, as is explained few paragraphs below, are very highly vulnerable due to their age and programming patchiness. However, according to Rid, only a sabotage, comprehensive re-programing, not just disruption of SCADA systems would cause failure of critical networks. Therefore, Tomas Rid criticizes administrations of hypersecuritization of the cyber space and spreading of fear among ordinary people, because only an attack that would eventually fall into the category of the disruptions of critical networks was launched by the U.S. administration, the same representatives that fear such attacks (2013).

Computer scientists consistently emphasize the ontological insecurity that is inherent to cyber space (Hansen and Nissenbaum, 2009). However, this constant ontological insecurity of computer networks pronounced by computer specialists derives from the knowledge that critical infrastructure networks, especially their program logic controllers, were not planned and created to withhold the external breach. The supervisory control and data acquisition (SCADA) and other industrial control systems of critical networks were not designed for being connected throughout the World Wide Web, which is inherently connected to the securitization of every day practices. Therefore, the built-in flaws and fragility of these systems need to be fixed as soon as possible, because they present a constant threat. The supervisory control

and data acquisition's accessibility from the Internet and thus creating vulnerabilities in their security systems was proved by the project of the Free University of Berlin. Using the Shodan computer search engine and Google custom search program, the SCADA Systems and Computer Security Group (SCADACS) at Free University of Berlin was able to visualize and create Industrial Risk Assessment Map of SCADA systems all around the world connected to the World Wide Web (SCADACS, 2013; Dieterle, 2013).

One of the first "unclassified" known attacks that used information warfare was conducted via a malfunction in the computer-control system of a Soviet gas pipeline. The explosion that disabled the Soviet pipeline was the result of a CIA software program that, as Thomas Reed, a former U.S. Air Force Secretary recalls, crashed and reset the pipeline's control system creating such conditions which eventually led to the explosion. "This was one of the earliest demonstrations of the power [and possibilities] of a "logic bomb"" (Murphy, 2010).

Cyber Space and International Relations

Therefore, the question whether a cyber attack represents an act of war became very pressing. In the present time there is no common understanding, because within the existing law of armed conflicts and international law every country 'attacked' would decide whether it is going to perceive the attack as an act of war. In the case of the North Atlantic Treaty Organization, its members, when attacked, have the right to choose whether they would like to enforce Article 5 ("any armed attack against one member of the alliance is an attack against them all)" (NATO, 2013) or Article 4 (call for consultations) of the North Atlantic Treaty. However, it is disputable whether the law of armed conflict can be applicable in the case of attacks executed in cyber space

targeting the information and communication technology systems. The United Nations' Charter, the North Atlantic Treaty, the Geneva or Hague Conventions, which set the code of conduct of armed conflicts or set the conditions for the declaration of war, do not recognize the attack in virtual cyber space as an attack. These international conventions and treaties understand armed conflict in the traditional offense-defense setting where armed attack and use of force are being applied "against the territorial integrity of an independent state which is being perceived as the primary actor and subject of attack (Westby, 2013). Thus, 'virtual' cyber warfare comprising a number of codes and encryption is not perceived in the traditional understanding of security as an existential threat. "Security is no longer thought of in the categories of classical attempts at keeping the balance of power [– in cyber-warfare] the perception of the concept of deterrence and the effectiveness of retaliatory actions have changed" (Swiatkowska, 2012, p.17).

Most of the cyber security experts and writers agree that the most important and fundamental element when it comes to penalization or 'securitization' of cyber space is to find the right balance between usability and security (Lunt, Rowe and Ekstrom, 2012). The state representatives or securitizing actors need to be aware of those hundreds of millions of users of cyber space and need to take into account their needs.

Myriam Dunn Cavelty (2012b) successfully points out that cyber threat inherently encompasses both business and national security where only mutual collaboration and shared responsibility would bring successful results. Interestingly, there is a very little research and theoretically based analyses on cyber space by either security studies or international relations scholars. Nevertheless, information and communication technology systems are a fundamental and crucial part of individual states as well as the international community. Information is power and power is information, and

information became one of the most desired assets. Key sectors of the modern society of the 21st century increasingly rely on smooth and undisrupted operation of the software-based control systems. The critical information structure encompasses infrastructure systems, personal, business as well as highly classified governmental data, which are mutually interrelated. Thus, cyber security, which originally dealt with the protection against computer-related economic crimes, espionage and data theft, with evolving computer networks and critical infrastructure protection became one of the key goals and highest priorities of national security (Dunn Cavelty, 2012a).

Indeed, the line between justifiable legal action and unlawful terrorist act can be very thin. The technological innovations and the strategy of dispersed networks with operating agents all round the world are tactics fondly used both by the official representatives of states, governments and their intelligence, as well as terrorist groups. As Berkowitz points out, the only difference between the actions of terrorist groups and official state armies is the compliance of armies with the international rules and norms and consequently the possibility to be held accountable for their actions in court. A country should not use illegal measures and tactics, but should uphold and respect the rule of law. Otherwise, it is no different from the terrorists it is fighting against. Indeed, there is " a key difference between using innovative military tactics to eliminate terrorists, rather than acting like terrorists to eliminate terrorists" (Berkowitz, 2003, p. 132-133). Cyber attacks or cyber war does not distinguish the warring parties from civilians. Furthermore, it is primarily the innocent civilian infrastructure, which is hijacked and used for striking targets. The anonymity and the obstacles to tackle and identify the actors go along with the jurisdictional problems associated with inadequate legal framework for prosecution of cyber offenders.

The lack of unified framework offers a potential for analysis. The aim of this thesis to explore securitization of this area by individual states and compare how their approach differentiates. At the moment, the only 'binding' international instrument and agreement is the Convention on Cybercrime of the Council of Europe, the only binding international instrument on this particular issue. The convention is supposed to serve as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between state parties to this treaty. Furthermore, it is supplemented by a Protocol on Xenophobia and Racism committed through computer systems. The only parties of the Council of Europe that have refused to adopt the Convention on Cybercrime is Russia (Council of Europe, 2001), a superpower and a member of the UN Security Council with a long history of organized crime and questionable enforceability of the rule of law. However, since the Budapest Convention was established within the action against economic crime, it is possible to observe that even within the Council of Europe cyber security is perceived mainly from the point of economic protection.

Therefore, the aim of this thesis is to analyze securitization frameworks of official cyber security strategies in the following three countries: the United States of America, the Russian Federation and Estonia. The area of cyber space has been predominantly an area of U.S. interest, thus, it is not surprising that the first institutional responses towards the potential vulnerability in cyber space, such as the Computer Emergency Response Team or private Computer Security Incident Response Teams were established and initiated in the United States of America. Eventually, national enforcement and security agencies in many countries around the world have expanded their scope of operation so that it would include actions in cyber space (Cerf, 2011). However, the most progressive has been the U.S. Federal Bureau of Investigation

(FBI) with its extensive cyber-crime response system and the U.S. Strategic Command establishing the new Cyber Command. Thus, the new field of military strategy and tactics, cyber warfare, was established and clustered together with traditional espionage discourse (Dunn Cavelty, 2010a).

Another country whose securitization of cyber space I would like to thoroughly analyze and compare is Estonia. Though not being of a particular great size or geopolitical importance, Estonia was the target of a massive cyber attack in April 2007. Estonia has a high dependence of public administration on information technologies. Therefore, the massive cyber-attacks of 2007 were perceived by the Estonian officials as a serious threat to national security. Estonia as a new member of the European Union had even pushed this perception of the new threat, cyber attacks, to the level of common EU policy, when in 2008 the European Union redefined and upgraded its European Security Strategy, originally adopted in 2003, with cyber security defined as one of the five global challenges and key threats (European External Action Service, 2008).

While the 2007 cyber attacks on Estonia that caused denial-of service of websites belonging to the Estonian government, media and bank Internet servers and providers were perceived as retaliation for a decision to remove a Soviet-era memorial from the center of Tallinn, the declaration at that time, by the Estonian minister of foreign affairs, Urmas Paet, that “the European Union is under attack, because Russia is attacking Estonia," questioned the implications and adequate response to such attacks (Davis, 2007). The only retaliation by Estonia during the “Web War 1”, as many authors address the 2007 cyber attacks on Estonia, has been the commitment of this small Baltic country to develop cyber-defense capabilities and tactical units. Estonia became the center of NATO Cooperative Cyber Defense Centre of Excellence

(NATO CCD COE) that was formally established on the 14th of May 2008, in order to enhance NATO's cyber defense capability (NATO, 2013).

Indeed, the traditional realist or neo-realist threat perception is not applicable to cyber space, where traditional offense defense strategies or balance of power are not applicable. In cyber space the vastness of conventional military equipment, the number of missiles or tanks do not matter. Cyber space is an area where super powers become small and individuals from their basements can cause serious disruptions and security breaches to powerful international players. Cyber space does not make a difference between a nuclear super power and a small country; you just have to master its language of zeros and ones. Consequently, Maryam Dunn Cavelty (2012) as well as Thomas Rid (2013) point out that militarizing or securitizing cyber space base on states' cyber capabilities is pointless, because individuals are referent objects of majority of issues connected with cyber space. Thus, taking into account the primary owners of the network, the decreased power of military and state as well media attention of cyber space, theory of securitization of Copenhagen School's of security studies was an appropriate theory for analysis of cyber space.

Chapter 2: Securitization of Cyber Space

The world and the notion of security changed during the 1980s. The end of the Cold War, the dissolution of the Soviet Union and the end of the bipolar world based upon nuclear deterrence led to the demise of the understanding of international relations and security under purely Realist and Neo-realist terms. Information gathering and information technology incorporated with weapons precision have increasingly become a crucial part of modern warfare and forces. It is possible to observe that information technology based weapons have especially after the Cold War transformed the "knowledge available to armed forces, their nature and that of war" (Ferris, 2010, p.118). Indeed, the past years it was possible to observe increasing rise of usage of unmanned aerial vehicles being at the center of counter-terrorism. John Ferris envisages that "armed forced will act without friction on near-perfect knowledge, through the fusion of command, control, communications, intelligence, surveillance and reconnaissance (C4ISR). They will jettison traditional hierarchies; adopt interconnected and flat structures based on the Internet, and conduct net-centric warfare" (Ferris, 2010, p.118). Thus, the military sector would use public as well private communications technologies, the overlap of military and private sector would be inevitable. Cyber space and its security have become the most pressing concern not only national but individual security.

Therefore, traditional concept of security, focusing solely on the military projection of power and state's ability to face the threat, needs to be widened. The Realist and Neo-Realist ability to explain the changes within the global security and international relations became too narrow and state-centric. The rapid expansion of globalization and technification of human society encouraged debate and increased the notion of

non-military conceptions of security not exclusively applied to the state. Indeed, the actors within the international security arena were no longer states, but also various international criminal organizations, terrorist groups that were operating within and beyond state borders as well as hackers who were breaching the national security domains in cyber space. The specifications of who the subjects of security are, whose security the experts should be dealing with, have increasingly become the center of the debate of security in cyber space. These changes in the international arena led to securitization theory, because it provides a comprehensive alternative that is the most appropriate for cyber space, its characteristics, threats or actors. Drawing on useful insights from constructivist as well as classical realist traditions, theory of securitization provides the bridge between the old and the new perceptions of security.

However, identification of threats and security is more difficult when moved out of the military sector (Buzan et al., 1998,) and cyber space defined by social interactions, technical implementation as well as network science's principles with main referent object being critical infrastructures is unsuitable for the traditional concepts of security and traditional security bodies. Furthermore, cyber space is not a domain completely controlled by state actors. Majority of network providers and owners are private companies, thus state actors do not have direct access. Indeed, military protection of cyber space is impossible. Firstly, because it is not possible to deploy troops and tanks into cyber space and. Secondly, because the logic of national boundaries does not apply in the digital domain comprised of zeros and ones (Dunn Cavelty, 2012; Rid, 2013).

The Theory of Securitization

Barry Buzan in his book *People, States and Fear* enhanced the understanding of security. While claiming that the political-military sphere is still the very basis and dominating aspect of state's security, Buzan widened the range of potential national security areas to economic, societal and ecological problems. He presents the idea that insecurity of state reflects a combination of threats and vulnerabilities in these five dimensions of national security (1991). Consequently, "the question of when a threat becomes a national security issue depends on what type of threat it is, how the recipient perceives it" (Buzan, 1991, p.134). Buzan was interested in the constant dramatic change in the priority among the five dimensions of national security that are the main driving force behind the shift of one state's security.

Following the notion that security is always subjective, the Copenhagen School of security studies widened the understanding that 'society' was just one of the dimensions through which the state might be threatened. Barry Buzan enhanced comprehension of societal security. Along with his fellow scholars and co-authors of the book *Identity, Migration and the New Security Agenda in Europe* Buzan proclaimed societal security to be increasingly important and proposed a reconceptualization of the security field. Waever followed the idea and presented the societal security as not just a "human" approach to security, "negating state security, rather than the Copenhagen School's reconceptualization in the sense of duality of state and societal security within Buzan's five original dimensions" (Weaver, 1993) Thus, societal security deepened the scope of security by the level of society, since it became a distinct referent object of security alongside the state. Thus, the Copenhagen School of security studies interestingly argues that state security can be perceived as a

sole nation-state security, as well as a set of societal securities within the state, which perceive threat in identity terms (Weaver et al, 1993).

The Copenhagen School is prominent for its securitization concept when threats and vulnerabilities are pronounced as "existential threats to a referent object, [to us, the community] by a securitizing actor who thereby generates endorsement of emergency measures" (Barry Buzan, Ole Waever, and Jaap de Wilde, 1998, p. 5). Consequently, "the security of a society could be threatened by whatever puts its 'we' identity in jeopardy" (Buzan, 1993, p. 42).

Barry Buzan and his colleagues interestingly show that security deals with survival threat, when a particular issue posses an existential threat a designated referent object. The invocation of threat via speech act thus legitimizes the use of force and application of security measures by securitizing actors. A threat is perceived to be of existential and requiring immediate application of measures only when a particular referent object is endangered. While the meaning of existential is unlimited because it is the referent object that ultimately defines its existential threat, the Copenhagen School of security recognized five sectors of security and identified the referent object as a collective of identities.

The crucial part of the theory of securitization is the securitizing process. Lene Hansen remarkably elaborates the significant difference between the concept of politicizing and securitization. To politicize an issue means that an issue is of particular importance and implications to society and thus the topic needs to be up for open discussion and contestation in political arena. Politicization refers to public decision-making process based on deliberations, negotiations and bargaining about a particular topic. However, securitization of an issue implies taking the concept

beyond (above) the political sphere into the emergency mode with military actors handling the issue (Hansen, 2012). A securitized issue has priority over everything else, because the whole existence, national security, of the referent subject depends on the prompt and successful resolution of the situation (Buzan et al., 1998, p. 23).

According to Buzan and his co-authors every issue can be located on the spectrum ranging from nonpoliticized- politicized- securitized and the position of particular issue differs from state to state. Therefore as authors themselves suggest, a textual analysis would provide answers to concerns where on the securitization spectrum is the particular issue (Buzan et al., 1998). As the authors point out, "a successful securitization [needs to have essential] components (or steps): existential threats, emergency action, and [the scale of chain] effects on interunit relations by breaking free of rules [when implementing securitizing measures]" (Buzan et al., 1998, p. 26).

Furthermore, the perception of security is created by a speech act that 'securitizes' a particular issue as a survival threat towards a referent object or objects, primarily a state or nation, and thus these objects are in grave need of protection against the particular threat. However, pronouncement of the word *security* does not constitute the speech act. It is the acceptation of securitization of particular issue as existential threat, the acceptance of the emergency issues by the audience, by significantly big referent object, that establishes securitization (Buzan et al. 1998). "It is predicated on the inter-subjective establishment of existential threat" to which the audience, the referent object, must respond in order to provide legitimation for the application of emergency measures (Roe, 2004, p. 281). Consequently, security would no longer have to be acknowledged as a concept referring to something real, existing independently of society's notion, because securitization is intersubjective and socially constructed.

Indeed, in general numerous securitizing actors as political leaders, bureaucracies, governments, lobbyists or pressure groups have an option and choose whether to securitize or not to securitize particular issue. And this decision and specific conceptualization of how an issue is framed as an existential threat is, as Buzan and his colleagues effectively argue a matter political choice, but each speech act has to fulfill "facilitating conditions" for an issue to be successfully securitized.

These facilitating conditions are distinguished into two categories: "[firstly], the internal, linguistic-grammatical – to follow the rules or act (or, as Austin argues, accepted conventional procedures must exist, and the act has to be executed according to these procedures), and [secondly,] the external, contextual and societal – to hold a position from which the act can be made" (Austin 1975 [1962] in Buzan et al., 1998, p.32), meaning that securitizing actors need to have particular authority to gain the attention of audience.

Following the second condition of speech act, authors point out that competing actors constantly attempt to securitize issue. Furthermore, a certain bias towards state is acknowledge, because of its traditional historical role of being responsible for the security of its citizens and thus it is assumed that state actors have the most suitable resources at their disposition to take care of existential threats (Buzan et al., 1998).

The Copenhagen School of Security Studies and Cyber Space

Interestingly, in the 1990s the renowned scholars of the Copenhagen School did not perceive cyber security as an existential threat to states because it did not have "cascading effects on other security issues" (Buzan et al. 1998, p. 25). However, technical development and the dependency of human society on the critical networks have risen in the past decades exponentially. Therefore, securitization, based on the

"discursive modality on particular rhetorical structure [of speech act with implications in the political and military sphere], is particularly suited for a study of cyber security discourse" (Hansen and Nissenbaum, 2009, p. 1156).

Just like economic or environmental issues, threats of cyber space have global implications and tore down the concepts of nations boarders. Indeed, securitization theory of Copenhagen School of security studies balanced out rigidity of realist security concepts with the fluidity of international relations of the 21st century, between the state and the individual as well as between consistency and flexibility. Therefore, it has great applicability and provides an excellent framework for cyber space's security.

Indeed, cyber attacks and especially cyber war are extensively modifying the traditional concept of conflicts and the process of providing security. Myriam Dunn Cavelty points out "cyber-security and national security differ most decisively in scope, in terms of the actors involved and in their 'referent object', [which protection they seek]"(2012a). Furthermore, it is possible to observe that nations round the world have securitized or penalized particular actions in cyber space. However, it is questionable whether militarization of this 'commonly shared' network is efficient.

Therefore, the Copenhagen School's theory or securitization is exceptionally suitable for 'securitization' of cyber space because of "its understanding of security as a discursive modality with a particular rhetorical structure and political effects" (Hansen and Nissenbaum, 2009, p. 1156). In addition, the securitization theory is appropriate of cyber space because it points out that security discourse comprises of other referent objects than just the state or nation. And consequently, it understands that if the existential threat is sufficiently explicit and gained the attention of the

relevant audience, then armed forces would be just one of the sectors of society that would be involved in handling the situation (Hansen and Nissenbaum, 2009). Undeniably, for proper securitization of cyber space a comprehensive action plan with all societal and global actors involved is necessary. Therefore, the theory of securitization is an appropriate approach for cyber security discourse, because it enables fluent transition between the referent objects as well as securitizing actors, both from private to political-military sphere.

Indeed, the cyber domain does not exist as a totally insulated plane. It is occupied by states, individuals, private companies and many other organizations. The multitude of security discourses that relate to these groups and individuals in the physical world are often mirrored in discourses of cyber security. Lene Hansen and Helen Nissenbaum therefore view the discourse of cyber security as "arising from competing articulations of constellations of referent objects rather than separate referent objects", exemplified by the "linkage between 'networks' and 'individuals' and human collective referent objects" present in this discourse (2009, p. 1163). Therefore, within securitization theory, Hansen and Nissenbaum identified three discourses with different objects of reference and specific forms of securitization grammar, specific speech act of securitization. Accordingly, cyber security has three different security modalities: hypersecuritization, everyday security practices and technifications (Hansen and Nissenbaum, 2009).

The discourse of hypersecuritization is a concept of securitization amplifying the vastness of upcoming threats, predicting their immense cascading effects, and thus calls for extreme and most of the time unnecessary countermeasures. While the authors point out that securitization in general is connected with hypothetical scenarios of existential threat, it is the instantaneity of its impact, the urge for

immediate action, and interconnectedness resulting into cascading effects throughout the whole range of reference objects of security. The hypersecuritization discourse of cyber space "hinges on multi-dimensional cyber disaster scenarios" that are going to severely damage the computer network system. The unprecedented disaster is going to have implications for the whole of human society. Hyper-securitized cyber discourse compares the attack in cyber space to the dangers of the Cold War and utilizes the analogies to the logic and language of nuclear war. This discourse utilizes the language of fear based on the power of the ripple effect in the whole network. The absence of prior large-scale attack of a nuclear explosion's magnitude leads to vagueness in the cyber-security discourse, since no one knows what measures would be appropriate. "The extreme reliance on the future and the enormity of the threats… make the discourse susceptible to charges of 'exaggeration,'" while the rising probability of such attack in the world highly dependent on the technology increases the vulnerabilities and dangers if all warnings are ignored and no safety precautious measures are applied (Hansen and Nissenbaum, 2009, p. 1164). The retaliation would be enormous. The object of referent in hyper-securitization is mainly the state or nation whose security is being threatened by a massive electronic attack.

The second discourse of securitization of cyber space is of every day security practices implying the effect on the daily lives of ordinary people. The referent point of securitization is an individual. Threats are more plausible to be experienced, because this discourse links elements of disaster scenarios with ordinary actions and every day needs (Hansen and Nissenbaum, 2009). With accessible and easily downloadable hacking tools, any breach into critical networks could escalate into severe national threat and implication of the highest security measures (Dunn Cavelty 2010). The referent subject is familiarized with the threat, not only because

individuals will experience the disruptive effects first hand, but also because they themselves can be responsible for an attack in cyber space. The individual is the necessary element in the fight against insecurity as well as the liability to the system as a whole, whether through deliberative actions or not (Hansen and Nissenbaum, 2009).

Following the referent subject of everyday securitization of cyber space, a responsible action of each individual connected to the network via World Wide Web is necessary. Proper educative measures of "computer hygiene" need to be applied, otherwise the innocent might be misused as zombie computers providing perfect cover for the intruders and criminal networks. Indeed, the development of personal computers and other smart devices have led to exponential growth of the Internet, which made cyber networks denser and much more vulnerable. The daily lives of ordinary people are vulnerable to the computerization and programming of the administration system. The vulnerabilities of the critical infrastructure is high, but establishment of individual responsibility and ownership of data as well as proper education, as applied in Estonia, should reduce direct correlation of individuals with adjectives such as careless and helpless. Nobody, neither government officials, private sector nor individuals want the total collapse of the Internet or the critical infrastructure networks.

The last securitization discourse applicable to cyber space is of technification deriving from computer experts' know-how. In order to properly understand and implement efficient measures an extensive knowledge of the computer network is necessary, not just the large-scale disruptive consequences of the cyber attack (Hansen and Nissenbaum, 2009). Therefore, computer experts have to closely cooperate with security experts and other representatives of administrations. Techno-utopian solutions of the privileged experts have to be subject of open discussion of wider

expertise. One of the critiques of technical securitization of cyber space is the privileged role of computer experts who might defy the blind uneducated masses (Hansen and Nissenbaum, 2009). However, despite the fact that certain differences in opinion between computer experts exist, most of them argue against hypersecuritization and exaggeration of threats and fear (Cavelty 2010b, Rid 2013).

Interestingly, Misha Glenny points out that computer experts, whether government employees or hackers, are the new mafia (Glenny, 2011) utilizing precious know how of modern technologies. However, technical discourse distinguishes between good and bad knowledge, distinguishes between the computer scientist and a hacker (Hansen and Nissenbaum, 2009). Overall, the call for "mobilization of technification within the logic of cyber security […constitutes] epistemic authority and political legitimacy" (Huysmans, 2006, p.6-9). The general public and politicians lack the technical expertise of computer specialists who have become the securitizing actors in the case of cyber security. Thus it is possible to distinguish the political domain of general discussions from the technical domain of computer experts. Technical and securitizing discourses are complimentary to each other, because they take the issue of cyber space out of the open political debate; they both depoliticize it. Thus, as Hansen and Nissenbaum interestingly explain, "technifications play a crucial role in legitimizing cyber securitizations, on their own as well as in supporting hypersecuritizations, [as well as] in speaking with [representatives of administration] to the public about the significance of its everyday practices [and vulnerabilities in cyber space]" (2009, p. 1168).

Therefore, following the "facilitating conditions" for the speech act, in the following chapter I applied to analyze three official cyber security doctrines of the selected states. The method of content analysis enabled me to study internal linguistic-

grammatical conditions for a successful speech act; in particular the grammar of security, the referent objects, the construction of the existential plot as well as particular securitizing dialogues of cyber space Buzan et al., 1996, p.32-33). Furthermore, according to the Copenhagen school: "A successful speech act [cyber security doctrine] is a combination of language and society, of both intrinsic features of speech and the group that authorizes and recognizes that speech" (Bourdieu 1991; Butler 1996a,b as cited in Buzan et al., 1996, p.32). Following these principles, a content analysis of particular securitizing acts, official cyber security documents, enabled me to elaborate how the three analyzed states conceptualize and grammatically construct the threats and vulnerabilities in cyber space. In other words study what kind of securitizing discourse is predominant in these securitizing doctrines.

Chapter 3: Content Analysis of Particular Cyber Security Strategies

This thesis focuses on a content analysis of 'securitization of cyber space' in cyber space strategies followed by a comparison of a small case selection of countries. In the previous chapter I established and explained three securitization narratives of cyber space. This chapter provides a content analysis of the utility and prevalence of particular securitizing narratives in the cyber security strategies of three countries that play significant and leading roles in securitization of cyber space. For the purpose of this content analysis I use the securitization narratives introduced and established by Hansen and Niessenbaum in their article "Digital Disaster, Cyber Security, and the Copenhagen School" (2009).

Using a specific codebook based on the three narratives of securitization I coded the cyber security doctrines of the United States of America, the Russian Federation and Estonia, namely the "*International Strategy for Cyber Space: Prosperity, Security and Openness in a Networked World"* of the United States published in May 2011, the unofficial translation of NATO's Cooperative Cyber Defense Centre of Excellence of the latest Russian strategy on cyber space entitled "*Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space"* from January 2012; and "*Cyber Security Strategy"* of Estonia for 2008-2013 published by the Estonian Ministry of Defense in 2008.

The selection of case studies is not based on random independent sampling. While the United States of America and the Russian Federation are permanent members of the Security Council of the United Nations and superpowers in warfare, Estonia is a small but highly technologically sophisticated country, internationally recognized as a

pioneer in e-government and e-election practices (The Estonian Information System's Authority, 2012).

One might say that these countries are outliers in the random distribution of cyber security capabilities. However, these 'outliers', as authors such as Geddes claim, provide a much more interesting examination of the securitization phenomena of cyber space in its most pure way (2003). The data from these particular countries possess very unique characteristics. This kind of case study of content analysis provides an insight into how particular countries securitize cyber space differently, what securitization discourse is predominant, and on the common understanding on action and measures, if any. Indeed, in-depth case studies yielded important data that can be overlooked and are otherwise inaccessible when using a large number analysis. This small case content analysis and comparison addresses how cyber space is securitized in these particular countries.

Content analysis and its methodology

The content analysis of the chosen security strategies was based on a codebook that enabled the coding and abstraction of particular elements of the three securitizing discourses from each document. This analysis is just an exploratory content analysis of three particular official documents. The statistical representation of the content analysis is their partial account for research purposes. In order to comprehensively understand the development of cyber security or cyber space as a new area of human activities and securitization - a comprehensive discourse analysis of cyber doctrines and governmental policies on cyber space should be elaborated in the future. Nevertheless, comparative content analysis provided an understanding of the securitizing ideas, issues and policies that the documents contain.

The premise is that the national cyber strategies which were analyzed represent the speech act of state representatives proclaiming cyber security to be an important issue of national security with regard to a referent object in mind. Within the documents themselves, as Hansen and Niessenbaum effectively point out, it is possible to observe numerous objects of reference depending on the securitizing discourse used. Therefore, my method of content analysis is centered around exploration and coding of paragraphs depending on most commonly used words in relation to the securitizing referent object of interest.

Furthermore, content analysis is an especially suitable methodology applicable to the securitization theory because it enables to set the coding parameters and categories according to the securitizing actors and objects of reference. The frequency with which certain words connected to particular securitizing discourse, which occurs in the official documents, is an indicator of securitizing discourse.

My code book is based on the identification of primary words that describe the referent object mentioned by a securitizing actor and by identifying particular secondary words indicating the need of securitization that are used in conjunction with the primary words of referent object indication. This method is not solely based on a simple count word frequency of particular words, but also provides a contextual approach by including words that are semantically linked to the referent object.

The development of the codebook based on three securitizing discourses not only provides content analysis based on the indicators of the referent object, but also inclusive words characteristic for the particular discourse. The method of content analysis, in particular coding of paragraphs of strategic documents on cyber space,

captures the complexity of securitization of cyber space and provides an insight into how different countries approach this issue.

Table 3 displays the used codebook that contains the selection of securitizing terms divided into three securitizing narratives presented by Hasen and Niessenbaum. In the case of hypersecurtiziation, the referent object is the state, so the terms have to depict and be connected with the threat on a state as whole. Consequently, hypersecuritizing securitization terminology contains terminology of "traditional" securitizing actors and measures employed as for example military attack, employment of armed forces, offense-defense narrative, or retaliation. Furthermore, bearing in mind that hypersecuritized discourse is induced with fear, with the visualizations and images of the unprecedented attacks bringing down the whole countries, I coded catastrophic scenarios or terms of unparalleled size as belonging to hypersecuritized discourse.

Secondly, since the daily life securitization has as object of its reference people and the society as a whole, I searched for the terms that posed the threat to daily lives and functioning of the society as a whole, and had a direct impact upon an individual. The vulnerability of critical infrastructures and perception of society as an interconnected network were the primary words of interest. Furthermore, this securitizing narrative stresses the interconnectedness of all levels of society, thus I depicted words that included private as well as public collaboration; that represented the basic needs and services; that stressed the need for better education and awareness spreading among all actors involved in order to reduce the vulnerability towards the malware or intrusions. In the technical securitization narrative, it is the experts and computer specialists who elaborate the threat potential of cyber space. This discourse is technical; it looks on the potential treats from the perspective of network science. In this coding category I included terms connected with the operability of the Internet.

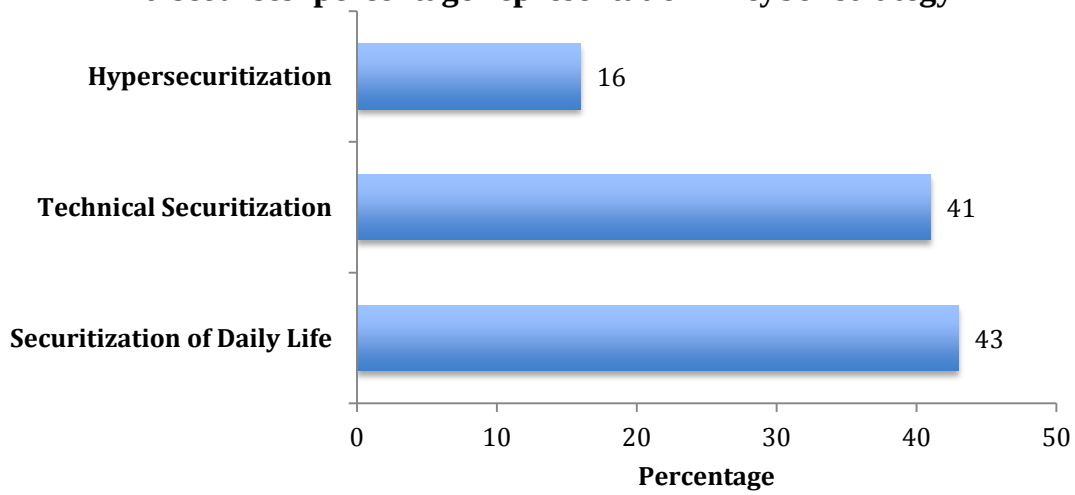
Table 3: Securitization Codebook

Securitization of Daily Life	Hypersecuritization	Technical Securitization
Society Population Community Individual	Nation State Government State authority	Specialists Computer experts
Vital activities	War	Network
Critical infrastructure	Hostile aggression/attack	Disruptions
Goods	Armed conflict	Software/Hardware/Malware
Privacy of data	Defense	Standards of information /norms
Society as network	Destruction	Vulnerability reduction
Dialogue/consensus	Command	Incident response
Collaboration	Deter/ defend	Interoperability
Training/education	Global issue	System management/provider/operator
Awareness	Terrorists	Prevention
Public/private sector	Organized crimes	Capacity building
Freedoms	Cascading effect	Intrusions/disruptions
Rule of law	Military/ armed forces	Access/ connectivity
Interdependence	Catastrophe	User-end
Connectivity (social dependence)	Cold War analogies	Stakeholders
Competence (individual as well as global)	Escalation	Intellectual property/ data

Results

The content analysis of cyber security doctrines demonstrated interesting similarity between the manner of particular securitizing discourses used by the United States of America and Estonia. Figure 1 to Figure 3 show the percentage representation of three securitizing narratives in paragraphs of the three analyzed cyber doctrines. Figure 1 and Figure 2 show a slight difference between the first and the second most used narrative in both the U.S. and Estonian cases. The prevailing language of securitization in the United States and Estonia is of daily lives with the object of reference being the society as a whole, as well as other levels of society.

Figure 1: The U.S. visualization of securitization discourses' percentage representation in cyber strategy



However, the technical securitization narrative, where experts are the securitizing actors calling for a comprehensive approach towards the cyber space without the utility of language of fear and scaring the general population, is only one percent behind both in the content analysis of the U.S. and Estonian cyber doctrines. On the other hand, the securitizing conceptual difference is possible to observe in the case of the Russian Federation. The content analysis of the latest Russian cyber security doctrine revealed that the document is written in a hypersecuritizing framework, as can be observed from Figure 3. Following the doctrine's narrative, the Russian armed forces are the securitizing actors protecting the sovereign Russian nation state from any kind of attack in cyber space, regardless of the international or domestic nature of the threat.

Figure 2: Estonian visualization of securitization discourses' precentage representation in cyber strategy

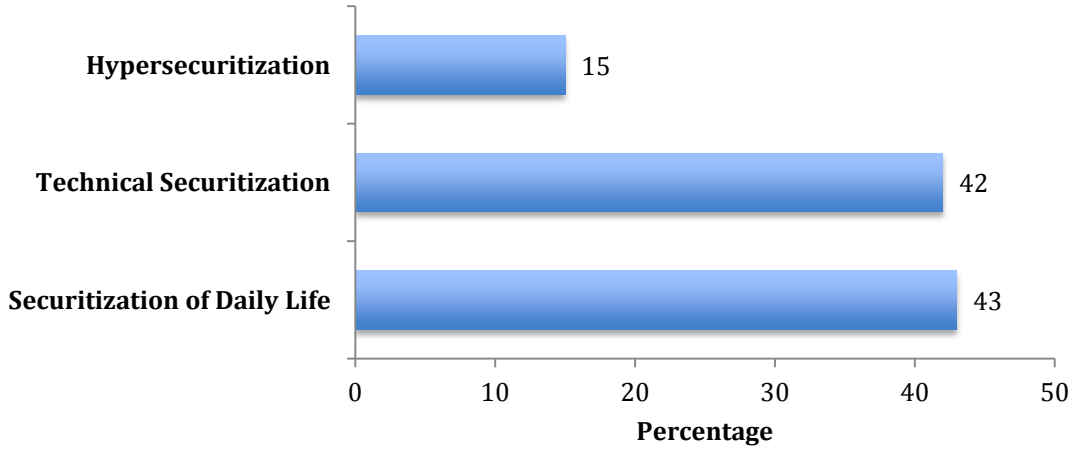
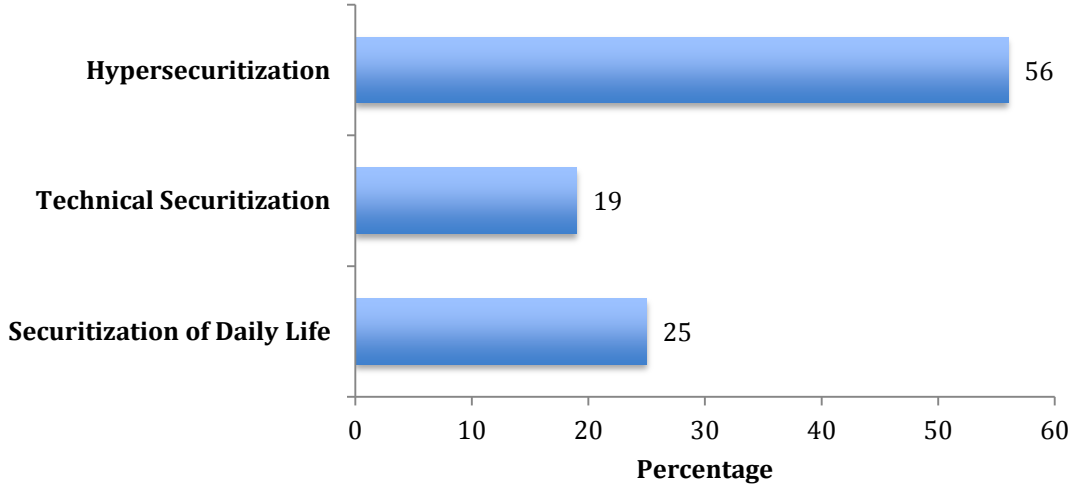


Figure 3: Russian visualization of securitization discourses' precentage representation in cyber strategy



Furthermore, to enhance the validity and reliability of my coding and content analysis I used open source software *Raw Text to Tag Cloud Engine* of the Digital Methods Initiative to generate a tag cloud that calculated the frequencies of particular words within each doctrine. With this software I generated the following tables containing only the forty most used securitizing words in the analyzed cyber security strategies.

For the purpose of my analysis I disregarded conjunctions or pronouns in the following tables because they do not constitute part of the theory.[1] Additionally, the parameters of the Tag Cloud Engine software were set to disregard words with less than a minimum number of four characters and with lesser frequency occurrence in the text than six times.

The tables below provide the frequencies and consequent percentage representation of the forty most frequently used words in the cyber security strategies of the analyzed countries. The examination of the most prominent and recurring terms used in the latest Russian strategy entitled "*Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space"* from January 2012, effectively reaffirmed the results graphically presented in Figure 3. The language and framing of the Russian doctrine is written in a hypersecuritization discourse of "military", "forces" or "conflict', (see Table 5), where the Russian armed forces have a duty to protect the state and its integrity by any means possible. The results of manual coding indicating a prevailing hypersecuritizing discourse were supported by the tag cloud method of counting the rate of occurrence of words within a document. Similarly, when it comes to the United States and Estonia, Tables 5 and 6 indicate that the results of manual coding are significantly trustworthy as well. The narrative of the forty most securitizing words is a mixture between the securitization of daily life and technical securitization.

In addition, the graphical visualization of text data can be observed in word cloud Figures 4-6 generated by open source software *Wordle.* The pictures are the visual representation of weighted lists of terms in the analyzed cyber doctrines. The tag or

[1] The unabbreviated results of the Tag Cloud Engine can be found in the Annexes.

word cloud format is a useful tool providing a quick graphical exemplification of the most prominent terms, where the size of the font determines relative prominence and frequency occurrence of a particular word in cyber strategy.

Table 4: The most frequently used securitizing words in cyber security strategy of the United States of America

#	Word	Frequency	%	#	Word	Frequency	%
1	states	120	8.73%	21	capacity	23	1.67%
2	**cyberspace**	**93**	6.77%	22	norms	23	1.67%
3	international	84	6.11%	23	effective	23	1.67%
4	network(s)	81	5.90%	24	private	23	1.67%
5	united	80	5.82%	25	reliable	21	1.53%
6	internet	64	4.66%	26	enforcement	21	1.53%
7	**information**	**49**	3.57%	27	ensure	21	1.53%
8	**security**	**43**	3.13%	28	networked	21	1.53%
9	national	40	2.91%	29	development	21	1.53%
10	**cybersecurity**	**37**	2.69%	30	collaboration	20	1.46%
11	global	33	2.40%	31	sector	20	1.46%
12	technical	32	2.33%	32	defense	19	1.38%
13	build	31	2.26%	33	privacy	19	1.38%
14	systems	29	2.11%	34	nations	18	1.31%
15	secure	29	2.11%	35	infrastructure	18	1.31%
16	innovation	27	1.97%	36	benefits	18	1.31%
17	building	27	1.97%	37	behavior	18	1.31%
18	world	26	1.89%	38	community	18	1.31%
19	future	25	1.82%	39	organizations	18	1.31%
20	technology	24	1.75%	40	principles	17	1.24%

Table 5: The most frequently used securitizing words in Russian cyber strategy

#	Word	Frequency	%	#	Word	Frequency	%
1	**information**	**101**	14.25%	21	defense	11	1.55%
2	federation	53	7.48%	22	cooperation	11	1.55%
3	Russian	52	7.33%	23	tasks	10	1.41%
4	space	45	6.35%	24	command	9	1.27%
5	forces	32	4.51%	25	regulations	9	1.27%
6	**security**	**31**	4.37%	26	weapons	8	1.13%
7	armed	30	4.23%	27	priority	8	1.13%
8	military	27	3.81%	28	solving	8	1.13%
9	international	23	3.24%	29	containment	8	1.13%
10	system(s)	20	2.82%	30	pursuant	8	1.13%
11	state(s)	18	2.54%	31	prevention	8	1.13%
12	principle(s)	17	2.40%	32	collective	7	0.99%
13	conflict	16	2.26%	33	troops	7	0.99%
14	activity	15	2.12%	34	doctrine	7	0.99%
15	resolution	13	1.83%	35	implementation	6	0.85%
16	measures	13	1.83%	36	adherence	6	0.85%
17	means	13	1.83%	37	demands	6	0.85%
18	global	12	1.69%	38	activities	6	0.85%
19	development	12	1.69%	39	control	6	0.85%
20	ensuring	11	1.55%	40	escalation	6	0.85%

Table 6: The most frequently used securitizing words in Estonian cyber strategy

#	Word	Frequency	%	#	Word	Frequency	%
1	**security**	**272**	12.48%	21	society	34	1.56%
2	**cyber**	**234**	10.74%	22	crime	32	1.47%
3	**information**	**204**	9.36%	23	internet	32	1.47%
4	Estonia(n)	95	4.36%	24	cyberspace	31	1.42%
5	system(s)	90	4.13%	25	protection	31	1.42%
6	infrastructure	72	3.30%	26	research	30	1.38%
7	international	69	3.17%	27	framework	29	1.33%
8	operation	67	3.07%	28	state	28	1.28%
9	critical	62	2.85%	29	strategy	28	1.28%
10	attacks	59	2.71%	30	convention	28	1.28%
11	national	49	2.25%	31	communication	27	1.24%
12	public	47	2.16%	32	threats	27	1.24%
13	countries	45	2.07%	33	training	26	1.19%
14	development	45	2.07%	34	implementation	25	1.15%
15	measures	41	1.88%	35	networks	24	1.10%
16	services	39	1.79%	36	computer	23	1.06%
17	necessary	38	1.74%	37	Europe	23	1.06%
18	legal	36	1.65%	38	level	23	1.06%
19	private	35	1.61%	39	related	22	1.01%
20	defense	35	1.61%	40	activities	22	1.01%

Country specifications

All countries analyzed are highly cyber dependent nations that consider cyber security a matter of national security and societal welfare. However, as shown, there is no unified understanding on the definition of cyber space and its securitization even among the three analyzed countries. For example, as it is possible to observe either from Table 5 or from Figure 5, the Russian Federation does not use the term cyber. The narrative of the latest Russian strategy "*Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space"* derives from the term information. While both Estonian and the U.S. strategy distinguishes between the expressions cyber and information, the Russian talks about information weapons, information space, information resources. This distinction might be a source of many misconceptions, since term information has broader application, while the 'cyber'- prefix automatically implies the digital network among computers (please see chapter one). However, the Russian Federation defines information (cyber) space as an "area of activity related to the formation, creation, transformation, transmission, use and storage of the information affecting inter alia the individual and social consciousness, information infrastructure and the information per se" (The Ministry of Defense of the Russian Federation, 2012, p. 5). On contrary, the Estonian cyber doctrine points out that various terms, "such as cyber war, cyber attack, cyber terrorism or critical information infrastructure, have not been defined clearly" (The Estonian Information System's Authority, 2012, p. 17), meaning that they lack one internationally accepted definition.

One of the explanations is the difference in how the framework and narrative the national cyber security strategies have been written. The difference in threat perception of cyber

space is observable in Table 7, which provides the overview of the priority level of cyber space and of the leading responding authority in the analyzed countries.

Table 7: Overview of priority level and threat perception of cyber space

Country	Level of prioritization	Characterization of threat	Lead responding authority
Estonia	High (4 on 5x5 matrix of impact and likelihood)	Focus on effects of cyber space perpetrators	Estonian Authority for Information Systems
Russian Federation	Most prominent	Internal (crime and corruption) External (state, terrorists, foreign competition)	Security Council of the Federation/ Ministry of Defense National system of information protection and intelligence community
The United States of America	One of four priorities	Criminal hackers Organized criminal groups Terrorist networks Advanced nation states	Responsibility is distributed across a number of organizations with inter-agency policy committee

Source: RAND Corporation, 2013

Other explanations could be based on the countries' military culture and tradition in society or on the level of development including society's reliance on cyber space. One of the obvious distinctions is their length and the date when they were adopted. Estonian Cyber Security Strategy was adopted in 2008, and for the 2008-2013 time period it is the most comprehensive the document, as well as the longest strategy. On contrary, the latest Russian cyber doctrine is quite short, as it has only thirteen pages. This is very prominent when looking at Table 5, where the frequency of particular terms are very small in comparison to frequencies in the other two doctrines, or from the Russian word cloud displaying the forty-five most prominent words in Russian information strategy, (please see Figure 4).

However, in all three countries the major securitizing actor is the government or particular governmental organizations. The ultimate speech acts of securitization, the cyber doctrines themselves, were pronounced in all three countries by the head of the state. In addition, the securitizing object of reference is primarily the whole nation, later distinguished and specified as interconnected layers of society and individual users. The state is the regulator establishing the rules of conduct; it regulates societal expectations and defines the major actor responsible for crisis management in cyber space.

Even though the results of the content analysis showed that that Estonia and the United States use a similar securitizing discourse, as shown in Figure 1 and Figure 2, the difference between these two countries persists. The obvious explanation behind the similar utility of securitizing discourse could come from the fact that both the United States of America and Estonia are members of the North Atlantic Treaty Organization (NATO) as well as sponsoring nations of NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE). Therefore, numbers in Figures 1 and Figure 2 show equivalence. However, Estonia is not only a home to NATO CCD COE, but also a leading e-governance member of the European Union. Therefore, Estonian cyber strategy puts an emphasis on the need for international cooperation and coordination of various international organizations such as the Council of Europe, the United Nations, NATO, the European Union or the Organization for Security and Co-operation in Europe, in order to adopt universal standards and norms of conduct. The United States also emphasizes the need for cooperation and for the establishment of universal rules of conduct in cyber space. Therefore, the cyber doctrine is a well-balanced document mentioning all the aspects of cyber space. This is noticeable in the U.S. table for the forty

most frequently used securitizing terms that encompass all three securitizing discourses (Table 4) or please see the visual representation of the U.S. cyber doctrine in Figure 4. The distinction between Estonia and the United States is that while Estonia might be a highly digital society and e-services are utilized by majority of its population, the United States has always been and aims to keep its leading position in cyber space. Indeed, the U.S. has been shaping the international securitizing framework and setting the standards for cyber space for the past decades.

Figure 4: Word cloud of the U.S cyber security strategy

Another interesting comparison is that in the Russian Federation and the United States, numerous security departments or particular units of the armed forces, especially in Russia, coordinate the cyber security policy. However, in Estonia this competence and cyber coordination was transferred to one single agency, the Estonian Information System's Authority within the Ministry of Economic Affairs and Communications (The Estonian Information System's Authority, 2012). This decision to move the agency away

from the state's security units automatically decreases the level of fear and utility of armed forces in cyber space. These kinds of intentions and moves towards the de-securitization of actors in the competence of cyber space do not occur in Russia, where the armed forces are delimited to be in control of protection and stability even in cyber space (The Ministry of Defense of the Russian Federation, 2013).

Another interesting feature specific for Estonia is its legislation. "By law [in Estonia], public sector institutions and providers of vital services are required to report major information security incidents" (The Estonian Information System's Authority, 2012). This lack of legislative force to report intrusions and cyber attacks is not present even in the U.S. legislation. Here, security network providers gather the data, but they report to their individual customers who then have the opportunity to initiate legal investigation (Symatec, 2012). Estonian cyber strategy is based on the Personal Data Protection Act, establishing a clear legal basis for processing any kind of personal data. In Estonia it is believed that the essential precondition for the securitization of cyberpace is that "every operator of a computer, computer network or information system realizes the personal responsibility of suing the data and instruments of communication at his or her disposal in a purposeful and appropriate manner" (Ministry of Defense of Estonia, 2008, p.3). Furthermore, the Public Information Act set in the Estonian Constitution "enables the state to exercise authority over the dissemination of high-quality public information, [… and also] defines the role of the Intent in the communication between state and [its] citizen[s]" (Ministry of Defense of Estonia, 2008, p.20).

Furthermore, the element, where the difference in strategic and military culture is very obvious, is the emphasis (or its lack) on the respect of fundamental freedoms, privacy and

the free flow of information. While the United States and Estonia attempt to securitize cyber space with regard to the right to information and privacy of individuals, the cyber doctrine of the Russian Federation stresses "the maximum use of opportunities of the information space for strengthening the defensive potential [and security] of the state" (The Ministry of Defense of the Russian Federation, 2013, p.13). Furthermore, the Russian cyber doctrine has a very clear and encompassing definition of information war. It is the only doctrine out of the three analyzed that has a definition of information war. According the Ministry of Defense of the Russian Federation, information war is:

> "Confrontation between two or more states in the information space for damaging the information systems, processes and resources, which are of critical importance, and other structures, to undermining the political, economic and social system, and massive brainwashing of the population for destabilizing the society and the state, and also forcing the state to make decisions in the interests of the confronting party" (The Ministry of Defense of the Russian Federation, 2013, p.5).

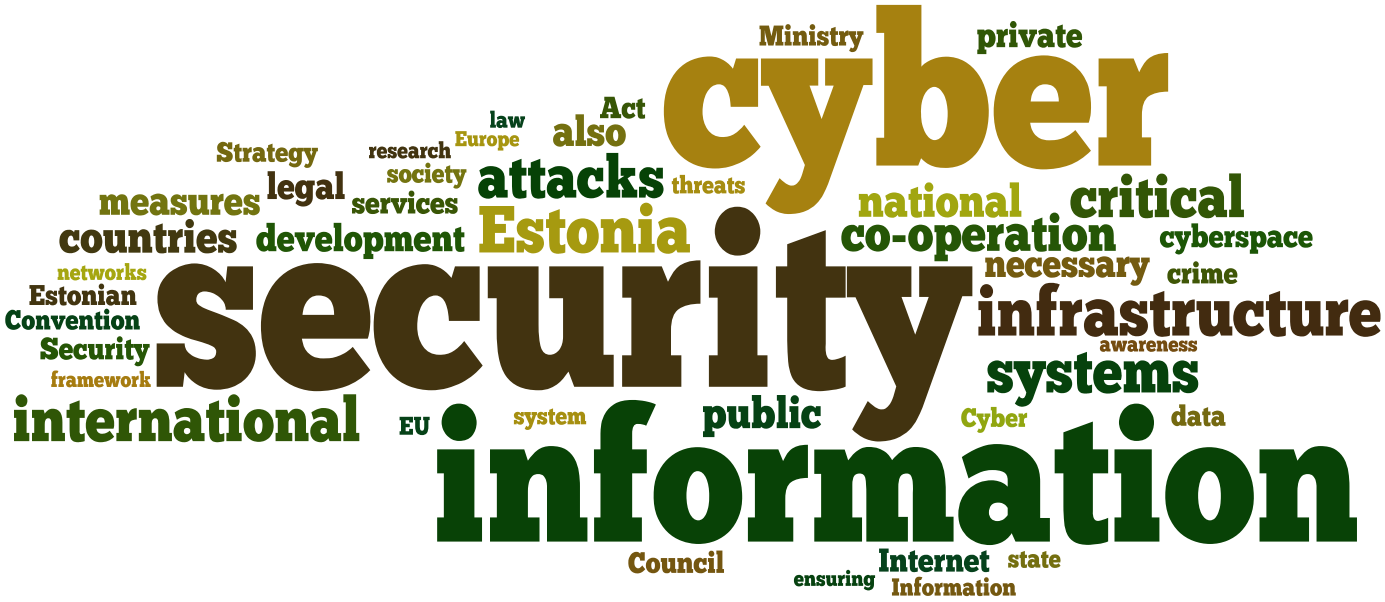
The above tables, deriving from an exploratory content analysis of three particular official documents, offer an interesting insight into the utility of three securitization discourses presented by Lene Hansen and Helen Niessenbaum. From the Russian table of the most frequently used securitizing terms, Table 5 or Figure 5, it is possible to observe that since Russian narrative focuses on information space rather than cyberspace, the top words are "information" and "space". Furthermore, it is possible to observe that four out of top ten words are of hypersecuritizing discourse as categorized in the codebook. This means that, while disregarding the most common English words, 16.92 percent of the

words of the Russian information strategy are of hypersecuritizing character invoking images of fear and the need to apply hostile measures.

Figure 4: Word cloud of Russian cyber security strategy

The Estonian frequency table of terms, not only proves that Estonia though the smallest country has the longest cyber security strategy, but also that Estonians are very much concerned about the data. The top three most frequent terms (security, cyber and information) show that Estonia is truly a digital society as e-Estonia, the e-governance website points out (e-Estonia, 2013). The overwhelming majority of Estonians utilize e-services as electronic voting in elections, signing a legally binding contract or filing out tax returns. As it is possible to see from the frequency Table 6 or Figure 6, the security of personal information and data in Estonia is a highly securitized issue. The security of personal information and responsibility of each citizen for his or her data in cyber space are established in the Personal Data Protection Act.

Figure 6: Word cloud of Estonian cyber security strategy



In this chapter I presented the content analysis of cyber security strategies of the United States of America, the Russian Federation and Estonia, and I drew attention to the most obvious differences and parallels between the official national documents on cyber space. The analysis was based on a codebook developed on the basis of three securitizing discourses presented by Lene Hansen and Helen Niessenbaum. The research shows significant similarities between the securitized framework of daily securitization and technical securitization used by Estonia and the United States. The results of manual coding presented in Figures 1-3 were supported and proven viable by the frequency tables of the forty most used securitizing terms generated by open source software *Raw Text to Tag Cloud Engine* as well as tag clouds. However, this study bears limitations of the depth of discourse analysis and thus a comprehensive discourse analysis of cyber doctrines and governmental policies on cyber space should be elaborated in the future.

Conclusion and Further Assumptions

The research focused on cyber security, which has become a prominent national and well as international security issue, and on its securitizing frameworks. Despite the fact that the utility of intelligence and espionage has been part of warfare for centuries, the technical development and the spread of communication technologies have significantly enhanced the security aspect as well as threat potential of the Internet and other critical infrastructures. This study was based upon the theory of securitization of the Copenhagen School's of security studies and its three securitizing narratives of cyber space developed by Lene Hansen and Helen Nissenbaum. The theory of securitization has provided a suitable theoretical base for my analysis of cyber space's 'securitization', because it perceives security as a "discursive modality with a particular rhetorical structure and political effects" (Hansen and Nissenbaum, 2009, p. 1156). Furthermore, the theory of securitization was an appropriate approach for cyber security discourse, because it enables fluent transition between the referent objects as well as securitizing actors, both from the private to the political-military sphere. The successful and efficient cyber security strategy needs to inherently demand the cooperation of private and public sectors.

Following three securitizing discourses of cyber security I have developed a codebook and used the method of content analysis to provide elaborate the framework of the latest official cyber security strategies of the United States of America, the Russian Federation, and Estonia. In order to enhance the validity of my analysis I used open source software to generate the forty most frequent securitizing terms for each of the analyzed doctrines. The analyzed documents represent the securitizing speech act and securitization of cyber

space in particular countries. Therefore, the content the research methods implied showed that these particular countries use different securitizing frameworks of cyber space. While the narrative of securitization of daily life is predominant in the U.S. and Estonian cyber strategies, the Russian Federation used the language of fear and hypersecuritization. Additionally, the analysis showed that countries do not have a common understanding of cyber space and that they apply even different concepts among them. In particular, the Russian Federation uses the term information space rather than cyber space and 16.92 percent of the terms of the forty most frequent words are on hypersecuritizing discourse.

In addition, this study bears limitations of the depth of discourse analysis and thus a comprehensive discourse analysis of cyber doctrines and governmental policies on cyber space should be elaborated in the future.

APPENDIX 1

The tag cloud of the U.S. cyber security strategy generated by the open source software *Raw Text to Tag Cloud Engine* when set to disregard words with less than a minimum number of four characters and with lesser frequency occurrence in text. than six times.

states (120) cyberspace (93) international (84) united (80) internet (64) networks (55) their (52) these (49) information (49) security (43) national (40) cybersecurity (37) global (33) those (32) technical (32) build (31) continue (30) systems (29) secure (29) innovation (27) building (27) network (26) through (26) world (26) future (25) technology (24) capacity (23) norms (23) effective (23) private (23) other (23) enhance (22) reliable (21) enforcement (21) ensure (21) networked (21) development (21) collaboration (20) sector (20) defense (19) privacy (19) should (19) nations (18) infrastructure (18) benefits (18) behavior (18) community (18) organizations (18) support (17) principles (17) policy (17) issues (17) recognize (16) government (16) governments (16) cooperation (16) which (16) develop (16) environment (15) governance (15) efforts (15) economic (15) digital (15) countries (15) standards (15) access (15) among (15) cybercrime (15) promote (15) freedoms (14) fundamental (14) challenges (14) would (14) partners (14) stakeholder (13) developing (13) nation (13) internationally (13) ability (13) consensus (13) protect (13) across (13) while (13) action (13) important (13) strategy (13) essential (13) multi (13) users (12) capabilities (12) society (12) state (12) individuals (12) partnerships (12) shared (12) trade (12) interoperability (11) stability (11) growth (11) critical (11) needs (11) technologies (11) interoperable (11) military (11) actors (11) committed (11) social (11) range (11) civil (10) activities (10) response (10) expand (10) relationships (10) strengthen (10) prosperity (10) preserving (10) people (9) appropriate (9) political (9) initiatives (9) abroad (9) share (9) together (9) responsible (9) policies (9) incident (9) public (9) collective (9) association (9) peace (9) require (9) lives (8) industry (8) stakeholders (8) partnership (8) expression (8) ideas (8) disrupt (8) property (8) borders (8) training (8) potential (8) international (8) citizens (8) threats (8) realize (8) tools (8) others (8) interests (8) fully (8) confidence (8) existing (7) including (7) respect (7) because (7) practices (7) computer (7) allies (7) interconnected (7) openness (7) globally (7) economy (7) disruption (7) organization (7) increasingly (7) societies (7) dialogue (7) convention (7) necessary (7) enhancing (7) freedom (7) protecting (7) multilateral (7) awareness (7) commitment (7) online (7) assistance (6) criminal (6) encourage (6) basis (6) broad (6) particularly (6) defend (6) personal (6) theft (6) markets (6) threaten (6) intellectual (6) engage (6) criminals (6) often (6) risks (6) services (6) economies (6) become (6) rights (6) businesses (6) trust (6) providing (6) responsibilities (6) agencies (6) responsibility (6) bilaterally (6) understanding (6) actions (6) sustain (6) measures (6) companies (6) around (6) another (6) promoting (6) provide (6) software (6) advance (6)

APPENDIX 2

The tag cloud of the Russian information strategy generated by the open source software *Raw Text to Tag Cloud Engine* when set to disregard words with less than a minimum number of four characters and with lesser frequency occurrence in text.

information (101)
federation (53) Russian (52) space (45) forces (32) security (31) armed (30) military (27) international (23) conflict (16) activity (15) resolution (13) conflicts (13) measures (13) other (13) means (13) which (13) global (12) development (12) principles (11) cooperation (11) system (11) defense (11) ensuring (11) tasks (10) from (10) states (10) systems (9) command (9) regulations (9) pursuant (8) containment (8) prevention (8) state (8) weapons (8) towards (8) priority (8) solving (8) also (7) troops (7) collective (7) doctrine (7) this (7) adherence (6) principle (6) resources (6) their (6) with (6) shall (6) implementation (6) demands (6) interests (6) activities (6) countries (6) rules (6) control (6) following (6) well (6) escalation (6) creation (6) settlement (6) president (6)

APPENDIX 3

The tag cloud of the Estonian cyber strategy generated by the open source software *Raw Text to Tag Cloud Engine* when set to disregard words with less than a minimum number of four characters and with lesser frequency occurrence in text.

security (272)
cyber (234)
information (204) infrastructure (72) international (69) operation (67) Estonia (67) systems (64) critical (62) attacks (59) national (49) public (47) should (45) countries (45) development (45) which (43) against (42) measures (41) services (39) necessary (38) legal (36) private (35) defense (35) society (34) crime (32) internet (32) cyberspace (31) protection (31) research (30) framework (29) other (29) state (28) strategy (28) council (28) ministry (28) Estonian (28) convention (28) communications (27) threats (27) system (26) training (26) between (25) implementation (25) networks (24) ensuring (23) computer (23) Europe (23) level (23) related (22) activities (22) order (22) awareness (22) their (21) government (19) economic (19) ensure (18) member (18) users (18) sectors (18) basis (18) global (18) service (17) sector (17) states (16) affairs (16) agencies (16) network (16) companies (16) functioning (16) attack (16) important (16) through (16) develop (16) these (16) common (15) there (15) field (15) organizations (15) policy (15) exchange (14) following (14) include (14) organization (13) different (13) competence (13) technology (13) general (13) personal (12) legislation (12) would (12) country (12) might (12) vulnerability (12) issues (12) requirements (12) further (12) European (11) because (11) plans (11) including (11) committee (11) control (11) fields (11) principles (10) efforts (10) financial (10) attention (10) solutions (10) levels (10) members (10) provide (10) electronic (10) combating (10)

List of References

Arquilla, J. & Ronfeldt, D.F. (1992). Cyberwar is coming!. Santa Monica, California: RAND Corporation. Retrieved from http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch2.pdf

B.C. (2013, March13). Cyber-attack in the Czech Republic: Thieves in the night [Web log post]. Retrieved from http://www.economist.com/blogs/easternapproaches/2013/03/cyber-attack-czech-republic

Berkowitz, B. (2003). *The New Face of War: How War Will Be Fought in the 21st Century*. New Your, NY: The Free Press.

Bronk, C. (2013, February 28). Hacking Isn't Cyberwar, for Now. *New York Times*. Retrieved from http://www.nytimes.com/roomfordebate/2013/02/28/what-is-an-act-of-cyberwar/hacking-is-hardly-cyberwar-for-now

Buzan, B. (1991) *People, States and Fear*, London: Harvester Wheatsheaf.

Buzan, B. (1993). Societal Security, State Security and Internationalisation. In Ole Waever et al. (Ed), *Identity, Migration and the New Security Agenda in Europe* (p.42). London: Pinter.

Buzan, B., Waever, O. and de Wilde, J. (1998). *Security: A New Framework for Analysis. Boulder*: Lynne Rienner Publishers

Cerf, V.C. (2011). Safety in Cyperspace. *The American Academy of Arts & Sciences.* Retrieved from http://www.mitpressjournals.org/doi/pdf/10.1162/DAED_a_00115

Council of Europe (2001). Convention of Cybercrime No. 185. *Action Against Economic Crime*. Retrieved from http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

Davis, J. (2007).Hackers Take Down the Most Wired Country in Europe. *Wired Magazine.* Issue 15.09, http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all

Dunn Cavelty, M. (2010a). Cyberthreats, In M. Dunn Cavelty and V. Mauer (Ed), *The Routledge Handbook of Security Studies* (180-189*).* London: Routledge 2009.

Dunn Cavelty, M. (2010b).Cyberwar,.In G. Kassimeris and J. Buckley (Ed), *The Ashgate Research Companion to Modern Warfare* (p. 123-144). Aldershot: Ashgate.

Dunn Cavelty, M. (2012a). Cyber-Security In A. Collins (Ed.), *Contemporary Security Studies* (p. 155). New York: Oxford University Press.

Dunn Cavelty, M. (2012b). The Militarization of Cyberspace: Why Less May Be Better

(p.141-153). 4th International Conference on Cyber Conflict. Retrieved from http://www.css.ethz.ch/publications/DetailansichtPubDB_EN?rec_id=2128

European External Action Service (2008). *Report on the Implementation of the European Security Strategy – Providing Security in a Changing World*. The European Union. Brussels http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf

Ferris, J. (2010). After the RMA: Contemporary Intelligence, Power and War. In G. Kassimeris and J. Buckley (Ed), *The Ashgate Research Companion to Modern Warfare* (p. 109-122). Aldershot: Ashgate.

Finan, C. (2013, May 23). A Cyberattack Campaign for Syria. *New York Times*. Retrieved from http://www.nytimes.com/2013/05/24/opinion/a-cyberattack-campaign-for-syria.html?_r=0

Geddes, B. (2003). *Paradigms and Sand Castles: Theory Building and Research Designing Comparative Politics* (p.89-132). University of Michigan Press.

Glenny, M. (2011). *DarkMarket: How Hackers Became the New Mafia.* Knopf Doubleday Publishing Group.

Hansen, L. (2012). Reconstructing Desecuritisation: The Normative-Political in the Copenhagen School and Directions for How to Apply It. *Review of International Studies*, Volume: 38, Issue 03, (p.528). Retrieved from http://journals.cambridge.org/abstract_S0260210511000581

Hansen, L. and Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*. Vol 53, no. 4, (p. 1155-1175) Retrieved from http://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf

Huysmans, J. (1998). Revising Copenhagen: Or, On the Creative Development of the Security Studies Agenda in Europe. *European Journal of International Relations*, Vol. 12, Issue 3. (p. 341-370). Retrieved from http://ejt.sagepub.com/content/4/4/479

Kerstetter, J. (2004, April 4). Has Dan Farmer Sold His Soul? *Bloomberg BusinessWeek*. Retrieved from http://www.businessweek.com/stories/2005-04-04/has-dan-farmer-sold-his-soul

Lewis, J. A. (2013). Conflict and Negotiation in Cyberspace. *Center for Strategic and International Studies*, Feb. 2013. http://csis.org/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf

Lunt, B., Rowe, D & Ekstrom, J. (2012). Cyber Security, Security Enhanced Applications for Information Systems, Dr. Christos Kalloniatis (Ed.), *InTech*, Retrieved from:

http://www.intechopen.com/books/security-enhanced-applications-for-information-systems/cybersecurity-in-the-real-world-implications-and-applications

Microsoft. (2013). What is a computer virus? Retrieved from http://www.microsoft.com/security/pc-security/virus-whatis.aspx

Ministry of Defence of Estonia (2008). *Cyber Security Strategy 2008-2013.* Tallinn. Estonia. Retrieved from http://www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

Ministry of Defense of the Russian Federation (2012). *Conceptual Views on the Activity of the Armed Forces of the Russian Federation in Information Space.* Unofficial translation of NATO's Cooperative Cyber Defense Centre of Excellence retrieved from http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf

Murphy, M. (2010, July 1). War in the Firth Domain. *The Economist*. Retrieved from http://www.economist.com/node/16478792

NATO. (2013). What is Article 5? Retrieved from http://www.nato.int/terrorism/five.htm

NATO Cooperative Cyber Defence Centre of Excellence (2013). Retrieved from https://www.ccdcoe.org/2.html

Panetta, L. (2012, Ocober 13). Leon Panetta Warns of 'Cyber Pearl Harbor'. *Washington Post*. Retrieved from http://www.washingtonpost.com/leon-panetta-warns-of-cyber-pearl-harbor/2012/10/13/6cdcbd6e-14c9-11e2-9a39-1f5a7f6fe945_video.html

Rid, T. (2012). Think Again: Cyberwar. *The Foreign Policy*. March/April 2012. Retrieved from http://www.foreignpolicy.com/articles/2012/02/27/cyberwar

Rid, T. (2013). The Great Cyberscare. The Foreign Policy. March 13.2013. Retrieved from: http://www.foreignpolicy.com/articles/2013/03/13/the_great_cyberscare?page=0,1

Rona, T. (1976). Weapons Systems and Information War. *Boeing Aerospace Company*. Retrieved from http://www.dod.mil/pubs/foi/homeland_defense/missile_defense_agency/09-F-0070WeaponSystems_and_Information_War.pdf

Schneir, B. (2007). *Schneier on Security: A Blog Covering Security and Security Technology.* http://www.schneier.com/essays-2007.html

Skala, M. (2011). Cyberwarfare: Identifying the Opportunities and Limits of Fightin. In Majer, M., Ondrejcsak R., Tarasovic, V and Valasek T. (Ed), *Panorama of Global Security Environment 2011*. (p.552). Center for European and North Atlantic Affairs: Bratislava.

Symatec Corporation. (2013) *Internet Security Threat Report (ISTR).* Vol. 18. http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=istr-18.

Swiatkowska, J. (2012). Cyberthreats as Challenge to the Security of the Contemporary World. In J. Swiatkowska (Ed.), *V4 Cooperation in Ensuring Cyber Security: Analysis and Recommendations* (pp. 13-20). The Kosciuszko Institute.

The Daily Star Lebanon. (2013, May 25). Israel Targeted in Syria Cyber Attack: Expert. *Daily Star Lebanon*. Retrieved from http://www.dailystar.com.lb/News/Middle-East/2013/May-25/218347-israel-targeted-in-syria-cyber-attack-expert.ashx#axzz2UVfkQKUt

The Estonian Information System's Authority (2012). Summary of the Estonian Information System's Authority on Ensuring Cyber Security in 2012. Retrieved from https://www.ria.ee/public/publikatsioonid/EISA_on_Cyber_Security_2012.pdf

The U.S Government. (2013). 50 USC § 413b - Presidential approval and reporting of covert actions. *The United States' Legal Code* Retrieved from http://www.law.cornell.edu/uscode/text/50/413b

The White House (2011*). International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*. Retrieved from http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Weaver, O. (1993). Societal Security: The Concept. In Ole Waever et al.(Ed). *Identity, Migration and the New Security Agenda in Europe*. (p.24-24). London: Pinter.

Weber, M. (2012, September 12). Who Invented Which Internet? *Computer History Museum*. Retrieved from http://www.computerhistory.org/atchm/who-invented-which-internet/

Westby, J. (2013, February 28). We Need New Rules For Cyberwar. *The New York Times*. Retrieved from http://www.nytimes.com/roomfordebate/2013/02/28/what-is-an-act-of-cyberwar/we-need-new-rules-of-engagment-for-cyberwar