universität
wien

MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

„What are states' strategic responses to cyberattacks? Impacts in international relations"

verfasst von / submitted by

Maria José Alvear Larenas

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Advanced International Studies (M.A.I.S.)

Wien 2017 / Vienna 2017

Studienkennzahl lt. Studienblatt Postgraduate programme code as it appears on the student record sheet:	A 992 940
Universitätslehrgang lt. Studienblatt Postgraduate programme as it appears on the student record sheet:	Internationale Studien / International Studies
Betreut von / Supervisor:	Prof. Markus Kornprobst, PhD

diplomatische
akademie wien
Vienna School of International Studies
École des Hautes Études Internationales de Vienne

(Page intentionally left blank)

Table of Contents

ABSTRACT 1

KURZFASSUNG 2

INTRODUCTION 3

CHAPTER ONE: THEORY 7

How a cyberattack differs from cyberwarfare, cybercrime and cyberterrorism 7

A theory for responding to cyberattacks 13

Methodology 18

Case-study 1: 2007 Cyberattacks against the government of Estonia 19

Case-study 2: 2008 Operation Buckshot Yankee in the United States 23

CHAPTER TWO: RESPONSES TO CYBERATTACKS FROM A REALIST PERSPECTIVE 28

Cyberattacks and defensive realism 28

Estonia's National Defence Strategy 30

United States' Cyber Strategy 32

Hypothesis' validation 36

CHAPTER THREE: RESPONSES TO CYBERATTACKS FROM A LIBERAL PERSPECTIVE 39

Cyberattacks and international institutions 39

Estonia's National Security Concept and Cyber Security Strategy 44

United States' National Security Strategy and International Strategy for Cyberspace 46

Hypothesis' validation 50

CHAPTER FOUR: RESPONSES TO CYBERATTACKS FROM A CONSTRUCTIVIST PERSPECTIVE 51

Cyberattacks and international norms 51

Estonia's Cyber Security Strategy 56

United States' Department of Defence Cyber Strategy and International Strategy for Cyberspace 58

Hypothesis' validation 61

CHAPTER FIVE: CONCLUSIONS 63

BIBLIOGRAPHY 72

Pledge of Honesty 79

(Page intentionally left blank)

ABSTRACT

What are states’ strategic responses to cyberattacks? This is the proposed research question for this thesis, which aims at determining the responses of states to cyberattacks and the impact these responses have in international relations. This study is analyzed under two disciplines: political science/international relations and international law.

Cyber issues and cybersecurity lack of a theory of their own. For this reason, mainstream theories of international relations (IR) are analyzed, in order to provide a framework that could explain the responses states develop to address cyberattacks. In general terms, theories such as defensive realism, liberalism and constructivism have elements that can explain what states’ responses to cyberattacks are. Although to this day states have focused mainly on defending themselves from a cyberattack, three hypotheses have been developed, in order to address the specific elements of mainstream IR theories that provide guidance when trying to explain states’ responses to cyberattacks.

This research follows a deductive design and includes a comparative analysis of two case-studies, the 2007 cyberattacks against the government of Estonia and the 2008 cyberattack against the United States’ military system. Based on the responses to these cyberattacks, an analysis of cybersecurity strategies of the two countries under a realist, liberal and constructivist perspective follows. This analysis has provided insights regarding how these states have shaped their policies and legislation related to cybersecurity issues.

Keywords: cyberattacks, cybersecurity, defence, international relations

KURZFASSUNG

Was sind die strategischen Reaktionen von Staaten auf Cyberattacken? Das ist die gestellte Forschungsfrage, die versucht das Reagieren von Staaten auf Cyberangriffe und die Auswirkungen auf die zwischenstaatlichen Beziehungen zu erforschen. Die Frage wird unter dem Gesichtspunkt zweier Disziplinen gesehen, Internationale Beziehungen und Internationales Recht.

Cybersecurity und anderen verwandten Themen fehlt eine eigenständige Theorie. Um eine passende Analysemöglichkeit zu finden werden deswegen bestehende IR Theorien analysiert um ein gutes Grundgerüst zu garantieren und die Antworten der Staaten auf Cyberattacken einzuordnen. Im Generellen, bieten Theorien wie defensiver Realismus, Liberalismus und Konstruktivismus Elemente, die die Reaktionen von Staaten auf solche Angriffe erklären können. Obwohl sich bis heute Nationen darauf konzentriert haben, sich gegen Cyberattacken zu verteidigen, wurden drei Hypothesen für diese Masterarbeit entwickelt, um die Reaktionen der Staaten auf diese Angriffe besser zu begründen.

Diese Forschung folgt einem deduktiven Design und zieht eine vergleichende Analyse zweier Fallstudien in Bezug auf Cyberattacken, eine die im Jahr 2007 gegen Estland erfolgte und eine 2008 gegen das Militärsystem der Vereinigten Staaten. Auf der Grundlage der Antworten im Zusammenhang mit diesen Cyberattacken folgt eine Analyse der Cyber-Security-Strategien der beiden Länder ebenso unter realistischer, liberaler und konstruktivistischer Perspektive. So wird festgestellt wie diese Staaten ihre Politik und Gesetzgebung im Zusammenhang mit Cyber-Security-Themen formuliert haben.

Schlüsselwörter: Cyberattacken, Cybersecurity, Verteidigung, Internationale Beziehungen

INTRODUCTION

Cyberattacks, cyberwarfare, cybercrime or cyberterrorism have become recent areas of study in terms of how states can properly identify their nature and respond accordingly. A cyberattack is different from conventional warfare, since attacks or crimes committed in the cyber domain present challenges that go beyond territorial boundaries and thus, go beyond states' jurisdictions.

A cyberattack can be understood as *"any action taken to undermine the functions of a computer network for a political or national security purpose"*.[1] When facing cyberattacks, the first important aspect that has to be taken into consideration is attribution. This entails answering two essential questions: who is behind the attack and what kind of cyberattack it is. The identification of the individual or entity responsible for the attack is crucial for determining the nature of the attack, as well as its aim and purpose. Determining the type of attack becomes the first step in outlining a reaction[2] and also in designing a legal response to it.[3]

A first challenge arises when trying to determine the place of origin of the attack. Cyberattacks happen online through worldwide Internet servers that enable attackers to use stepping stones i.e. controlling computers that belong to innocent parties to conduct their attacks. Those computers can be located anywhere in the material world. Even when a cyberattack could be traced back to, for example, Germany one cannot conclude that the attack originated in Germany because the attacker might be controlling a computer located in the United States, Argentina, India or in any other country, while making use of the German Internet server.[4]

Depending on its nature, a cyberattack can disrupt and destroy computer systems from remote locations, which can disable national infrastructures and cause dire economic harm. To avoid this, a state must have not only the capacity, but also the legal framework that would allow it to protect itself from, and to respond to cyberattacks. However, to this day neither the domestic nor the international legal framework that should govern

[1] Hathaway, et. al., "The Law of Cyber-Attack", p. 826.
[2] Brenner, "At light speed: Attribution and response to cybercrime/terrorism/warfare", p. 405
[3] Hathaway, et. al., "The Law of Cyber-Attack", p. 821.
[4] Brenner, "At light speed: Attribution and response to cybercrime/terrorism/warfare", p. 409

cyberattacks is clear.[5] Unlike attacks with conventional weapons, cyberattacks present different legal problems mainly because they are not military attacks conducted in one physical place, but they are conducted from remote areas, are difficult to attribute and have unpredictable effects.[6]

Countries that have developed cyber security strategies, which include general provisions for cyberattacks, do not assign the responsibility of handling and responding to cyberattacks to a single entity at the national level, but to several national bodies.[7] At the international level, there is no treaty that would regulate cyberattacks, since cyberspace evolves every day and would quickly render any treaty out of date. International organizations such as the United Nations (UN), the North Atlantic Treaty Organization (NATO), the Organization of American States (OAS) and the Shanghai Cooperation Organization (SCO) provide guidelines related to cybersecurity and cyberattacks. Only the Council of Europe has come up with a legally binding treaty to combat cybercrime.[8]

The previous example of an attacker that could be anywhere in the world, but conducts cyberattacks through a German Internet server, reveals the international nature of this new kind of danger. The challenge states face when attributing responsibility for cyberattacks directed to their networks, coupled with the difficulties of formulating a legal response to them, reveals the need to further research in terms of what are the responses states develop to address this type of attacks. Additionally, the response must be thought of in a way that it secures the state's national interests and at the same time it assures adherence to international regulations and international law. Hence, cybersecurity has become an important research area because cyberattacks entail that security issues are no longer constrained to the material world, since states have to deal with security matters in the cyber domain, too. This research is thus important and valuable considering that determining what states' responses to this kind of attacks are provides additional inputs in terms of strategic responses to cyberattacks and their impact in international relations.

[5] Brecher, "Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations", p. 423, 425.

[6] Brecher, "Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations", p. 430.

[7] Klimburg, ed., *National Cyber Security Framework Manual*, p. 23-25.

[8] Hathaway, et. al., "The Law of Cyber-Attack", p. 859.

This thesis will answer the following research question: what are states' strategic responses to cyberattacks? And it will be analyzed under the framework of two disciplines: political science/international relations and international law. This document seeks to build a classification of types of attacks while at the same time providing appropriate definitions to differentiate between cyberattacks and cybercrime, cyberwarfare and cyberterrorism. The thesis examines two case-studies, one from Estonia and one from the United States to see how these countries responded to the cyberattacks they were subject to. The case-studies are followed by an analysis of the two countries' national cybersecurity strategies from the perspective of three theories of international relations (realism, liberalism and constructivism), in order to identify how each country says it will respond to a cyberattack.

Estonia and the United States have been chosen on the grounds that both states provide extensive analytical reviews in terms of the responses each country developed to a significant cyberattack. The government of Estonia faced several attacks in April 2007, which made the Parliament's email servers unavailable because of floods of junk emails that rendered the digital systems offline for twelve hours. Servers of political parties in Estonia were also subject to attacks and their security was compromised. However, the highly capable emergency response team of the Estonian government was able to mobilize experts to counter the cyberattacks, which presumably originated in Russia.[9] As for the United States, the Department of Defense faced a considerable attack on its military digital networks in 2008. A hidden malicious software attack, suspected to have been conducted by Russian hackers, spread to classified and unclassified systems and threatened to transfer data to foreign servers and to deliver operation strategies to unknown recipients. This marked a turning point in the USA's cyber defense strategy as the Pentagon launched Operation Buckshot Yankee, which led to the creation of the United States Cyber Command.[10]

To answer the research question, chapter one includes the literature review, theoretical framework and three hypotheses that have been identified for the three mainstream IR theories: realism, liberalism and constructivism. An explanation of the methodology that has been applied to this study is described in this chapter, along with the two selected

[9] Shakarian, et. al., *Introduction to Cyberwarfare - A Multidisciplinary Approach*. p. 16-18.
[10] Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy", p. 97.

case-studies, the 2007 cyberattacks against the government in Estonia and the 2008 Operation Buckshot Yankee in the USA. The next three chapters address the possible responses to cyberattacks from a mainstream IR theory, as well as the validation of each proposed hypothesis. Thus, chapter two covers possible responses to cyberattacks from a realist perspective, chapter three explains possible responses from a liberal perspective, and chapter four refers to possible responses from a constructivist perspective. Each of these chapters also make reference to the national legislations, especially national security and/or cybersecurity strategies of Estonia and of the United States to look at the norms these countries have to respond to a cyberattack. Chapter five is dedicated to the conclusions and recommendations drawn from the research.

CHAPTER ONE: THEORY

How a cyberattack differs from cyberwarfare, cybercrime and cyberterrorism

There are presently many concepts and definitions involving the word “cyber”. Despite the lack of universal agreement, the National Cyber Security Framework Manual by the Cooperative Cyber Defence Centre of Excellence (CCD COE) has come up with a comprehensive understanding of “cyber” as a concept related to computer networks i.e. the Internet. Cyberspace, a concept first identified by William Gibson in 1984[11], would refer to the Internet itself. However, this term goes beyond that, since cyberspace also includes hardware, software and the social interactions within computer systems and networks, which do not exist in the material world. In a political context, sensitive national security issues also take place in cyberspace. Thus, the term cybersecurity emerged during the year 2000 and refers to the necessity to preserve the integrity, availability and confidentiality of information in cyberspace.[12]

Cybersecurity has become a priority for many countries, especially because of several types of offenses that could happen in the cyber domain, such as cyberattacks, cyberwar, cybercrime or cyberterrorism, which could threaten national security. Cyberattacks, cyberwarfare, cybercrime and cyberterrorism are terms often used interchangeably. However, there are specific distinctions among them, which are worthy of consideration when states try to identify a response to a cyberattack.

“The Law of Cyber-Attack” by Oona Hathaway et. al. provides a clear understanding of cyberwarfare and cyberattacks. The authors define a cyberattack as *“any action taken to undermine the functions of a computer network for a political or national security purpose”.*[13] The virtual method is what makes a cyberattack unique.[14] The objective of the cyberattack is to undermine the functions of a computer network and this can happen in two ways. There can be a syntactic cyberattack or a semantic cyberattack. A syntactic attack entails breaking down the operating system in a computer, in order to cause a

[11] Cerf, “Safety in Cyberspace”, p. 59.

[12] Klimburg, ed., “National Cyber Security Framework Manual”, p. 12.

[13] Hathaway, et. al, “The Law of Cyber-Attack”, p. 826.

[14] Kello, “The Meaning of the Cyber Revolution,” p. 22.

malfunction of the network. On the contrary, a semantic attack protects the operating system of the computer, but disrupts the certainty of the information it processes.[15]

Aaron Brecher in “Cyberattacks and the Covert Action Statute” broadens the definition of cyberattacks. In Brecher’s view, a cyberattack is the *“action that alters, disrupts, deceives, degrades, or destroys computer systems, networks, information or programs residing in or transiting such systems or networks.”*[16] However, this definition does not include the political or national security component that Hathaway et. al. takes into account, which is also essential for this thesis’ research question.

The fact that a cyberattack is conducted for a political or national security purpose is what makes it different from cybercrime. Hathaway et. al. conceives internet fraud, intellectual property piracy and identity theft as cybercrimes. These crimes cannot be considered cyberattacks because they do not serve any political or national security purpose, they are simply illegal acts conducted by individuals. There is no single recognized definition of cybercrime. Nevertheless, this term is understood as *“any crime that is facilitated or committed by using a computer, network or hardware device”*.[17] If an individual hacks significant records of a bank, for example, for a political or national security purpose, but does not undermine the banking system in the process, this would also constitute a cybercrime. On the other hand, if a state or a non-state actor hacks the same bank’s records, with a political or national security purpose and undermines the computer network in the process, then the cybercrime becomes a cyberattack. Thus, an attack in cyberspace that is carried out by a state or a non-state actor, which aims at undermining the function of a computer network and has a political or national security purpose, is a cyberattack and not a cybercrime.[18]

Based on this distinction between a cybercrime and a cyberattack, Hathaway et. al. continue on to define cyberwarfare. According to the authors, there are two important considerations in this regard. First, cyberwarfare must also comprise a cyberattack. This means an initial stage, where an individual, a state or a non-state actor carries out attacks

[15] Hathaway, et. al, “The Law of Cyber-Attack”, p. 828.
[16] Brecher, “Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations”, p. 425.
[17] Hathaway, et. al, “The Law of Cyber-Attack”, p. 830, 834.
[18] Hathaway, et. al, “The Law of Cyber-Attack”, p. 835, 836.

in the context of an armed conflict i.e. non-computer-based attacks. This first stage unfolds in combination with a second stage, whereby cyberattacks produce effects equal to those caused by a conventional armed attack. The combination of stage one and stage two gives origin to cyberwarfare. The second consideration is that cyberwarfare can evolve from a cybercrime to a cyberattack and then to cyberwarfare. In this case, the first stage is an attack conducted by a computer system, which pursues a national security or a political purpose and that undermines the functions of another computer network. The second stage happens when the attack's effects are equal to those of a conventional armed attack.[19]

"Introduction to Cyberwarfare" by Paulo Shakarian et. al. gives a broader concept of cyberwarfare. For the authors, cyberwarfare could be regarded as an extension of policy actions taken in cyberspace either by a state or a non-state actor. It constitutes a serious threat to a nation's security or it is conducted in response to a national security threat.[20]

While Hathaway et. al. give a clear understanding of what a cyberattack, cybercrime and cyberwarfare entail, Susan Brenner sheds light on a possible definition of cyberterrorism, which is not discussed by Hathaway et. al. To this day there is no definition of terrorism, only considerations from the United Nations of what this activity entails. In this regard, Brenner frames terrorism as the actions such as mass destruction, kidnapping or assassination used to intimidate and/or coerce a population, a government or the conduct of a government. Its ultimate purpose is to target civilians and demoralize the population.[21]

Cyberterrorism would then comprise the use of computer systems to commit acts intended to demoralize the population. To this day, there have not been known cases of cyberterrorism, but if those were to happen in the future, then computer systems would play a significant role as detonators of a cyber terrorist act. This could happen by hacking security systems and sending out fake information of a possible terrorist attack that would seem credible to authorities. In this case, the cyberterrorist act could lead to property

[19] Hathaway, et. al, "The Law of Cyber-Attack", p. 836, 837.
[20] Shakarian, et. al., *Introduction to Cyberwarfare - A Multidisciplinary Approach,* p. 2.
[21] Brenner, "At light speed: Attribution and response to cybercrime/terrorism/warfare", p. 387.

destruction and death and thus it would be achieving its goal of eroding the people's confidence in the government and would have a demoralizing effect on the population.[22]

Attacks in cyberspace target vulnerabilities found in computer systems, which makes us think that protection against and reactions to cyberattacks depend on technological development. However, it is not only a technological solution that is needed to respond to cyberattacks. Strategic and operational capacities, as well as control of information resources, should be combined in order to effectively respond to cyberattacks. Despite cyberspace being a vulnerable structure, it is at the same time a highly valuable repository of data. Thus, control of information resources could not only give rise to offensive cyberattacks, but it also gives rise to the development of defensive tactics.[23]

Brenner points out that attribution for war is easier than for crime or terrorism. The attacker in war can be identified by military insignias and equipment. If a state uses missiles to attack another state, the location from which they are launched also leads without a doubt to attacker attribution. In the case of crime, perpetrators usually do not identify themselves, but attribution evidence found in the physical world and by identifying witnesses certainly helps in discovering the attacker. Terrorist attacks, on the other hand, can be attributed when terrorists identify themselves or acknowledge that an attack was committed on behalf of a terrorist group.[24]

When facing cyberattacks, the first important aspect that has to be taken into consideration is attribution. This entails answering two essential questions: who is behind the attack and what kind of attack it is. A first challenge arises when trying to determine the origin of the attack. Cyberattacks happen online through worldwide Internet servers that enable attackers to use stepping stones i.e. controlling computers that belong to innocent parties, to conduct their attacks. When we turn to cyberspace, we can no longer rely on the territorial-based assumption of attacks because identifying a "place" or "location" in the cyber sphere is less conclusive and more ambiguous than in the material world.[25] The identification of the person or entity behind the attack is crucial for

[22] Brenner, "At light speed: Attribution and response to cybercrime/terrorism/warfare", p.389, 391, 392.
[23] Harknett and Goldman, "The Search for Cyber Fundamentals", p. 84, 85.
[24] Brenner, "At light speed: Attribution and response to cybercrime/terrorism/warfare", p. 406, 407, 408.
[25] Brenner, "At light speed: Attribution and response to cybercrime/terrorism/warfare", p. 409

determining its nature, aim and purpose. Thus, determining the type of attack becomes the first step in outlining a reaction[26] and also in designing a legal response to an attack.[27]

Today, information technology allows nation states, as well as any Internet user with special skills to launch a virtual attack not to the actual territory of a country, but to its national infrastructure. Moreover, information technologies allow the attacker to reiterate such attacks with a frequency beyond the bound of possibility in the material world, which certainly entails the use of various computers in several countries. Thus, tracing an attack back would require the cooperation of legal authorities in the countries in which the computers were used. If backtracking leads to a degree of certainty of the place of origin of the attack, it means that it would be possible to determine if a state might or might not be involved in an attack. Likewise, the possibility of a state sponsoring a cyberattack is always present.[28]

The next challenge when facing a cyberattack is determining what kind of attack it is. Is it an attack that is stealing information or conducting espionage? Is it disrupting computer systems or using them to conduct other attacks? Most importantly, does it fulfil all characteristics of a cyberattack as mentioned previously? Or is it cybercrime or cyberterrorism? At first glance, there is no precise knowledge on what the attack is trying to accomplish, and without that it is not possible to decide on the type of response to the attack. This scenario could pose other difficulties in the response process. For example, misunderstanding the nature of the attack and assigning the responsibility of coming up with a response to the attack to the wrong national authority, should the military authorities be responsible in the case of cyberwarfare? Or should civil law enforcement authorities be responsible in the case of cybercrime? If responders cannot clarify the nature of the attack, then an appropriate response cannot follow.[29]

Shakarian et. al. mention three elements that make attack attribution much harder. These are origin, structure and purpose. A malware's origin can be tracked down by its Internet Protocol address or IP address. However, one must be aware that the Internet users

[26] Brenner, "At light speed: Attribution and response to cybercrime/terrorism/warfare", p. 405

[27] Hathaway, et. al, "The Law of Cyber-Attack", p. 821.

[28] Brenner, "At light speed: Attribution and response to cybercrime/terrorism/warfare", p. 412, 418, 420, 423.

[29] Brenner, "At light speed: Attribution and response to cybercrime/terrorism/warfare", p. 435, 436, 439.

responsible for the attack are resourceful and they can fake and reroute the IP address, thus making the physical location of the attack much more difficult to pinpoint. The structure of the malware itself can be deceiving to analysts and can be designed in a way that hides the malware's primary purpose or its inventor. For example, the source code of a malware may include hints pointing to a specific organization instead of pointing at the inventor him/herself.[30]

Thus far, attribution is crucial for determining a response to a cyberattack. It is important to note that such a response does not lie exclusively in the technological, military or civilian sphere, but in the combination of these fields. To achieve effective attribution Brenner considers important to integrate capabilities. In this regard, the ambiguity of cyberattacks suggests states should forgo the traditional approach of having exclusively a military response to acts of war and exclusively a civil law response to crimes.[31] Harknett supports such approach especially because of the non-geographical aspect of cyberattacks. According to him, there must be an interaction between military defence operations and domestic law enforcement, which then translates into stronger cooperation with foreign law enforcement agencies to fight cyber threats.[32]

Along these lines, Harknett indicates that cyberattacks are a multidimensional conflict and as such they require a holistic strategic response, not a menu with isolated strategies to be chosen depending on the occasion. Thus, Harknett suggests the need of having an integrated security approach to respond to cyberattacks. This approach should include different dimensions that take part in cyberattacks such as the state, state proxies and networks. Every state can make use of networked organizations or anonymity. At the same time, the state can become a target for disruption of information. The state can even become a proxy state, i.e. a third party in the conduct of cyberattacks. Networks are added to this integrated approach in the sense of the potentially unlimited access possibilities they offer, which broaden the scope of security breaches.[33]

[30] Shakarian, et. al., *Introduction to Cyberwarfare - A Multidisciplinary Approach*, p. 4, 5.
[31] Brenner, "At light speed: Attribution and response to cybercrime/terrorism/warfare", p. 455,
[32] Harknett and Stever, "The New Policy World of Cybersecurity", p. 456.
[33] Harknett, "Integrated Security: A Strategic Response to Anonymity and the Problem of the Few", p. 29, 31, 33, 35.

A theory for responding to cyberattacks

When looking at mainstream international relations theories such as realism, liberalism and constructivism, they all have their own approach towards security.

According to realism, the state is the most important unit of analysis in the international system. In this regard, non-states actors cannot possibly exercise any degree of power. The state is considered to be a rational actor, to whom security and power are the most important values. The international system is characterized by anarchy i.e. there is no central government, and this situation makes states pursue national interests for their survival. This context leads to the security dilemma, measured in terms of the military power that can guarantee the safety of the state.[34] However, realists view security threats related to information technology as economic issues, and so they do not consider it necessary to revise the theory to analyse security in the digital sphere. For realists, the notion of offensive and defensive attacks of information and information infrastructures is as old as warfare itself. Thus, information attacks would become relevant if they were defined as one technological component in the traditional interstate conflict.[35]

Liberalism, on the other hand, stresses the plurality of actors in the international system. Unlike realism, liberalism considers non-state actors as part of the international system. However, non-state actors are not considered subjects of international law and so are not subject to international law penalties.[36] Domestic politics determine the behaviour of states in the international sphere, and international institutions establish rules of conduct for states.[37] Due to the fact that liberalism recognizes non-state actors, the theory has the potential to raise awareness of threats coming from groups that interact in the digital realm. The revolution in information technologies, as part of the globalization process, has enabled non-state actors to become more active and powerful. Thus, threats in cyber space are also a result of further integration and globalization. Another characteristic of liberalism is that it leads to interdependence and interconnectedness, which on a first instance can facilitate cohesion and full integration of economic policies. However, such

[34] Dunne, et. al., *International Relations Theories – Discipline and Diversity*, p. 53-69.
[35] Eriksson and Giacomello, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", p. 228, 229.
[36] Kello, "The Meaning of the Cyber Revolution," p. 25.
[37] Dunne, et. al., *International Relations Theories – Discipline and Diversity*, p. 90-106.

strong interdependence also has its costs. Sensitivity, vulnerability and shocks affecting one country can easily influence another because of the interconnectedness of the economy. Nevertheless, inputs from this interdependent approach can easily be translated to the digital sphere considering the next two aspects: (1) the positive integration of information systems at the international level, and (2) the vulnerabilities that come along with this process as a result of a stronger interdependence of computer systems worldwide.[38]

Realism and liberalism were not able to explain the end of the Cold War. Such situation gave room for constructivism to develop, which describes that reality is socially constructed. According to constructivism, there is a material reality (infrastructures) and a social reality (norms, identities and institutions). Unlike the material reality, the social reality is adaptable and is constantly evolving because identities and interests are never static. They are constantly produced and reproduced by the interaction among human beings, their beliefs and backgrounds. Norms shape identities and identities shape interests, which are constantly evolving.[39] When it comes to security issues, constructivism emphasizes that threats could be related to identity and culture.[40] If we take this into account, it can be said that cyberspace has become a tool to adapt and to create new identities. By means of cyberattacks, the identity of nation-states can be threatened. At the same time, the use of rhetoric related to cybersecurity shapes norms that redefine those threatened identities, which then shape the state's interests.

The securitization theory or Copenhagen School also uses a constructivist approach to security. It takes into account the socio-political construction of security, since it regards security as a creation of political speech. This involves a political figure and an audience, the former claiming that a particular situation represents a threat to security, and the latter listening to the speech and eventually agreeing that the situation represents a threat. Important political figures, such as the president, become the main securitizing actors. Their speech will inevitably influence and shape the social context in which decision makers operate. The aim of securitization is to transform a normal-politics issue into a

[38] Eriksson and Giacomello, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", p. 230 – 232.
[39] Dunne, et. al., *International Relations Theories – Discipline and Diversity*, p. 167 – 183.
[40] Eriksson and Giacomello, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", p. 233 – 235.

security-politics issue. Once such concern is part of the security agenda or part of the interests and/or priorities of the securitizing actor, it usually acquires additional characteristics. There is an increase in the sense of urgency, coupled with and increased use of exceptional measures such as power centralization or the use of force, which are considered to be necessary in order to respond to the threats posed to security.[41]

Despite the fact that the securitization theory fails to consider information technologies and how the information revolution has affected security,[42] Lene Hansen and Helen Nissenbaum believe that political discourses and norms can construct cyber threats as security issues and separate them from political, economic or technological issues. The idea that cyberattacks can threaten the security of a state is directly associated with the concept of threat to sovereignty, which leads to issues of authority, order and identity. A cyberattack that renders communications and power grids useless or that disrupts large commercial transportation and financial markets targets the identity of a state directly. Along these lines, the securitizing actor would emphasize not only the threat that a cyberattack represents to network systems, but also to society as a whole.[43]

Cybersecurity can be analysed with a deterrence lens, too. Deterrence theory, also known as rational deterrence theory, suggests that an entity could use a threat, in this case a cyberattack, in an effort to convince or dissuade another entity to keep the status quo and prevent the status quo from being altered. In this regard, a state can deter an attacker by saying: (1) that it can respond with effective military capacities, (2) that it can apply considerable sanctions on the attacker, or (3) that it can conduct the threat if the state is attacked.[44] The understanding of a cyberattack, the threat of taking an action that would undermine the functions of a computer network for a political or national security purpose, would make the potential attacker assess the feasibility of such threat and decide whether to engage in a conflict or to back down.[45]

[41] Hayes, "Securitization, Social Identity, and Democratic Security: Nixon, India, and the Ties That Bind", p. 66.

[42] Eriksson and Giacomello, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", p. 234.

[43] Hansen and Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School", p. 1157, 1160, 1161, 1165.

[44] Quackenbush, "Deterrence theory: where do we stand?", p. 741, 742.

[45] Quackenbush, "Deterrence theory: where do we stand?", p. 747

Deterrence has been particularly important in the nuclear weapons sphere. A country in possession of nuclear weapons can deter another nation’s attack because the latter believes that its adversary could respond to the attack with nuclear weapons. Thus, the colossal costs associated with a nuclear war would render the attack not viable and proves the effectiveness of deterrence in this situation.[46] In this regard, nuclear non-proliferation regimes and the verification of nuclear arsenals and enrichment activities are part of the contributing factors for deterrence. However, applying these measures to deter cyberattacks is just not possible, mainly because of the unlikelihood of constantly monitoring Internet users or programmers to check for the design of malware.[47]

Nevertheless, there is one situation that has shown effective use of deterrence in cyberattacks. North Korea’s cyberattacks on Sony in 2014 are presumed to have stopped after the FBI announced that it was examining the breach. Additionally, the announcement of the FBI was followed by a statement of the President of the United States in which he attributed the attack to North Korea and assured consequences. Here, the warning of the USA to retaliate against or sanction the attacker proved useful to diminish the attacks. In order for deterrence to be much more effective in cyberspace, the attribution challenge must be solved, so that threats to retaliate against cyberattacks can be more credible.[48]

Attribution in cyberspace is a challenge mainly because the cyber domain offers the possibility of creating and retrieving information from multiple locations at the same time. This aspect adds up to the potential for anonymity of activities conducted in cyberspace. Both undermine deterrence’s applicability in cyberspace because they make it difficult to clearly identify the party responsible for a cyberattack. Attribution is possible in nuclear deterrence because it implies that the scope and source of the attack can be quickly identified, which is not the case in cyberspace because of the aforementioned challenges. If the state advocating for deterrence cannot attribute a cyberattack, then retaliation is not possible; who will the state retaliate against? How will

[46] Quackenbush, “Deterrence theory: where do we stand?”, p. 743.
[47] Rid and Arquilla, “THINK AGAIN: CYBERWAR”, p. 83.
[48] Lindsay, “Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack”. p. 57, 58.

it do it and why? For deterrence to work in cyberspace, the attacker/opponent must be identifiable. [49]

Attribution is necessary for deterrence to be credible. The threat of using a cyberattack against a possible aggressor would be effective only if capable to detect the attack, its source, and to retaliate against in response to the attack. Attackers in cyberspace resort to anonymity and have the ability to hide identities and disguise their tracks, which undermines deterrence. In other words, attribution is absolutely necessary for deterrence credibility, since aggressors would be convinced of the possibility of retaliation.[50]

The aforementioned theories reveal there are elements that can be used to explain cyberattacks and how states handle cybersecurity issues. However, to this day there is no theory of cybersecurity and the existence of threats in cyberspace points to the need of developing a theoretical framework that could allow understanding of cyberspace threats and their effects for security.[51] It is suggested that a theory for cybersecurity requires a combination and integration of realism, liberalism, constructivism, as well as other disciplines such as engineering and information technology sciences[52] to be able to explain how information impacts security.[53]

Based on the considerations each theory provides to cybersecurity issues, it has been identified that each mainstream IR theory includes elements that would allow answering what are states' responses to cyberattacks. For this reason, three hypotheses have been elaborated, so to identify such responses to cyberattacks from a realist, liberal and constructivist perspective. These hypotheses are: (1) from a realist perspective, if a state perceives its security is threatened by the possibility of being cyberattacked, then the state resorts to improving its defensive capabilities. (2) From a liberal perspective, if cybersecurity interests of a state depend on global networks, then the state is expected to collaborate closer with international institutions. And (3) from a constructivist

[49] Harknett, "Integrated Security: A Strategic Response to Anonymity and the Problem of the Few", p. 19, 30, 34.
[50] Harknett, "Leaving Deterrence Behind: Warfighting and National Cybersecurity," p. 9, 10.
[51] Kello, "The Meaning of the Cyber Revolution," p. 9.
[52] Kello, "The Meaning of the Cyber Revolution," p. 16.
[53] Eriksson and Giacomello, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", p. 235.

perspective, if a state adopts an appropriate behaviour towards cyberattacks, then the state abides by identity-constructing norms.

Methodology

Existing literature on cybersecurity has been found mainly in academic journals and academic reviews, such as, the Journal of Criminal Law and Criminology, the California Law review and SAGE Publications, among others. Specific literature on how states respond to cyberattacks and the strategies they resort to is limited, for most academic journals refer to the attribution problem of cyberattacks.

This research follows a deductive design and explains what makes a cyberattack different from cyberwarfare, cybercrime and cyberterrorism. As explained previously, existing understandings of cyberattacks have been contrasted, in order to identify a proper definition of this term to be used throughout the entire research. Moreover, the thesis analyses comparatively two case-studies, the 2007 cyberattacks against the government of Estonia and the 2008 cyberattacks against the military system of the United States. Each case-study is examined to see how these states responded to the cyberattacks they were subject to. With this information we then look at the countries' national security and cybersecurity strategies to see how they officially say they will respond to cyberattacks. The National Cyber Security Framework Manual by the Cooperative Cyber Defence Centre of Excellence (CCD COE) refers to security and/or cybersecurity Strategies of the United States and Estonia, as well.

The analysis of the case-studies follows a most dissimilar system design (MDSD). In a MDSD the dependent phenomenon does not change across observations.[54] In other words, the essence of the case-studies varies from one another; however, the outcome in each one of them is similar.[55] In the case of the proposed research question for this thesis, the case-studies have shown that the dependent variable "strategic responses to cyberattacks" has remained invariant in both cases, i.e. each case-study is different from one another and the outcome in both cases in terms of the response to the cyberattack is

[54] López, "Theory Choice in Comparative Social Inquiry", p. 273.
[55] Collier, "The Comparative Method", p. 7.

similar. Both case-studies provide significant analytical reviews in terms of each country's response to cyberattacks, which is the reason why they are relevant for the comparative analysis.

Case-study 1: 2007 Cyberattacks against the government of Estonia

The 2007 cyberattacks against Estonia became a cornerstone case in the study of cybersecurity, especially because they were the first to be considered a politically motivated cyberattack. It started in April 2007 when the government of Estonia began plans to relocate a national monument. The monument honoured Soviet soldiers who died in World War II and it was placed in Tallinn by the former USSR in 1944. The relocation plans faced opposition from the ethnic Russian population living in Estonia because this group regarded the monument as a symbol of Russian sacrifice and its victory over Nazi Germany. The group protested in Tallinn and several other locations until mid-May. There were violent encounters between rioters and security forces for days.[56] On April 27, protests began after authorities in Estonia removed the statue, exhumed the bodies of soldiers of the Red Army that were buried beneath the monument and transferred them to a military cemetery. President Putin criticized this act angrily.[57] Later that day, a post on an Internet forum appeared and gave indications on how to participate in a distributed denial of service (DDoS) attack against governmental systems.[58]

A DDoS attack is a well-know and common aggression conducted on the Internet. A denial of service (DoS) attack floods the target computer or system with disproportionately large amounts of legitimate data, in order to overburden the system with these large amounts of information to be processed. Thus, the system cannot process all this data, so it crashes and the attack renders the system inaccessible to practically any users. When numerous networks are subject to a denial of service attack, it becomes a distributed denial of service (DDoS) attack. A DDoS attack is successful when it exceeds

[56] Shakarian, et. al., *Introduction to Cyberwarfare - A Multidisciplinary Approach,* p. 12, 14.
[57] Schmidt, "The Estonian Cyberattacks", p. 4, 5.
[58] Shakarian, et. al., *Introduction to Cyberwarfare - A Multidisciplinary Approach,* p. 16

the number of data a router or server is normally designed to process. The attack can gain momentum when in a network more computers flood others at the same time.[59]

On the evening of April 27, Internet servers of Estonian organizations were attacked and stalled with exceptionally high data traffic and web defacements. Email servers of the Estonian parliament had to be shut down and the Estonian news outlet ‘Postimees Online’ had to close foreign access to its networks. Average-day peak loads in Internet traffic exceeded by a factor of 10, which resulted in malfunctioning and unavailability of Internet services. Operational teams started handling such excessive traffic, but what started as an IT security issue quickly turned into a national security issue, when the Ministry of Defence announced they were being cyberattacked.[60]

By April 29, a sophisticated attack of disruption and denial was taking place against the electronic infrastructure in Estonia. Thousands of Internet users in Russia were inspired by the Internet posts and also took part in DDoS attacks against Estonian computers. Four forms of attacks were identified: network flood, rented network flood, web site defacement and junk email. Email servers are used to receiving junk email at a moderate pace on a regular basis. When they receive an abnormal amount of emails, the servers are not prepared to deal with it. On April 29, email servers of the Estonian Parliament were rendered unavailable because of junk email floods. The system stayed offline for twelve hours. It is not known how this situation affected the government’s response. However, the unavailability of email definitely affected direct communication among government authorities and direct action to restore the servers’ availability. Some attackers compromised the security of web servers of political parties in Estonia. Once they gained access, they were able to deface governmental web pages i.e. replace legitimate content of the web page with content that mocked the government. One such defacement, for example, showed a false letter of apology from the prime minister.[61] Web pages from other government agencies, media outlets and from the two largest banks were also subject to DDoS.[62]

[59] Shakarian, et. al., *Introduction to Cyberwarfare - A Multidisciplinary Approach*, p. 12, 14.
[60] Schmidt, “The Estonian Cyberattacks”, p. 5, 6, 9.
[61] Shakarian, et. al., *Introduction to Cyberwarfare - A Multidisciplinary Approach*, p. 16 – 18.
[62] Hansen and Nissenbaum, “Digital Disaster, Cyber Security, and the Copenhagen School”, p. 1168.

From the beginning, the attack was highly disruptive; this forced the government to take quick and extensive measures that were available to it. Such measures included: improving firewalls, installing security patches and making encryption tools stronger. This information technology (IT) approach was necessary because Estonia is a wired country almost in its entirety. To put an example, 97% of the population does online banking.[63] The networks' breakdown affected both the state and society at large. The people did not receive any information from the government because the web sites were down. Private financial transactions were blocked because the two main banks were attacked as well. Accurate and legitimate information was unavailable because news media were also targeted, and could not trust information posted on authoritative web pages because of web defacements.[64] The attacks rendered the country's government and financial systems unavailable for approximately three weeks.[65]

It is worth noting that NATO did not intervene in the Estonian cyberattack. The organization claimed that it lacked a coherent doctrine and a comprehensive strategy in the cyber sphere.[66] Additionally, authorities in Estonia had difficulties in proving that the cyberattack constituted an attack on Estonian political sovereignty. Consequently, there was not enough evidence to invoke NATO's Article 5 (collective self-defence[67]).[68]

Thus, the response of the government of Estonia to the attacks involved IT capabilities. Due to the fact that a DDoS attack leads to confusion and panic among IT personnel, a quick and significant IT response is crucial to react to the attack. The government of Estonia counted with a very skilful computer emergency response team (CERT), which was able to identify that an attack was targeting its infrastructure, and mobilize experts to counter it. The Estonian CERT could contact other CERTs in Germany, Finland and Slovenia, and together they identified the nature of the attack against Estonian networks, as well as the general location of the systems generating the attack's floods. Likewise, they could identify the networks that originated the attacks targeting Estonia and could guide network operators to block such networks from reaching the country. The attacks originated outside the country and this facilitated Estonian businesses and network

[63] Rid and Arquilla, "THINK AGAIN: CYBERWAR". p. 85.
[64] Hansen and Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School", p. 1169.
[65] Kello, "The Meaning of the Cyber Revolution," p. 24.
[66] Hathaway, et. al, "The Law of Cyber-Attack", p. 861.
[67] NATO, "The North Atlantic Treaty (1949)", p. 1.
[68] Hansen and Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School", p. 1169.

operators to block the flood coming from outside and maintain the service for the population inside the country.[69]

Based on this information, it was concluded there were two rounds of attacks. The first one constituted the DDoS, whose IP (Internet Protocol) addresses the Estonian authorities claimed to have traced back to Putin's administration. Nevertheless, Russia not only denied such accusations on the grounds of lack of evidence, but also refused to provide forensic assistance to Estonian investigations.[70] The inability of the Estonian government to attribute the cyberattack facilitated the second round of attacks. It was conducted with botnets i.e. a group of compromised computers that are controlled by the same entity.[71] These botnets provoked a cascading effect and eventually attacks were said to have originated from 50 different countries including China, Egypt, Peru, the USA and Vietnam, which infected approximately a quarter of the world's computers.[72] During this second round, the most significant attacks were those against Estonian banks. One of them, the Hansabank, owned 50% of the national retail banking. Because of the attacks, Internet services of the Estonian banks were offline for about 45 to 90 minutes, which represented losses of around USD 1 million.[73]

The DDoS attacks diminished in the weeks following the response of the Estonian government and over time they stopped. The attacks were carried out by individuals, who did not gain any financial reward. This showed that personal interest was the only incentive behind the attacks. However, nearly two years after the attacks, Konstantin Goloskokov, a leader from a pro-Kremlin youth group called "Nashi" claimed the group's responsibility for the cyberattacks against Estonia. Presumably, the attack claims are accurate. Still, involvement of the Russian government in the cyberattacks remains unanswered.[74] Russia denies any engagement in the cyberattacks, even though Russia's information warfare strategy conceives the use of political and military actions in conjunction with attacks conducted through the Internet.[75]

[69] Shakarian, et. al., *Introduction to Cyberwarfare - A Multidisciplinary Approach*, p. 18, 19.
[70] Kello, "The Meaning of the Cyber Revolution," p. 24.
[71] Shakarian, et. al., *Introduction to Cyberwarfare - A Multidisciplinary Approach*, p. 15.
[72] Hansen and Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School", p. 1170.
[73] Schmidt, "The Estonian Cyberattacks", p. 11.
[74] Shakarian, et. al., *Introduction to Cyberwarfare - A Multidisciplinary Approach*, p. 19.
[75] Galeotti, "The cyber menace", p. 34.

As a result of this cyberattack, NATO, the EU and the USA made information systems and networks part of their security agenda. Over the course of 2008, NATO adopted a Cyber Defence Concept, a Policy of Cyber Defence and created a Cyber Defence Management Authority.[76] The 2007 cyberattacks against Estonia also led to the creation of the Tallinn Cooperative Cyber Defence Centre of Excellence in collaboration with NATO, as well as the creation of EU Agency for large-scale IT systems.[77]

Case-study 2: 2008 Operation Buckshot Yankee in the United States

"Buckshot Yankee" was the operation set in place to counter a cyberattack that represented the greatest breach of military networks in the history of the United States. In 2008, a foreign intelligent agent infected military computers at a base in the Middle East.[78] Those computers were used to oversee combat zones in Afghanistan and Iraq. This breach was first reported by the "Danger Room" blog of Wired Magazine in November 2008 and later by "The Los Angeles Times", who mentioned it was suspected that Russia was behind the attack. An official confirmation of the incident, although not from the perpetrator, only came in 2010 with an article written by William J. Lynn III, who was US Deputy Secretary of Defence at the time.[79]

A flash drive with a malicious computer code was used to infect the computers. This code uploaded itself to the network ran by the USA Central Command and from there it spread without being detected to classified and unclassified systems.[80] The code, dubbed "agent.btz", was a self-replicating computer worm with dozens of variants. It was created to scan computers for data and vulnerabilities that could be exploited. Even though most of its variants had been detected by 2011, the worm has not been eradicated and continues to this day to copy itself from one flash drive to another when these flash drives are connected to infected computers. New variants of the malware have not been created in several years and new versions of Windows have closed the "autorun.inf" tool, which was the vulnerability found by agent.btz and used to self-activate and run automatically from

[76] Hansen and Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School", p. 1170.
[77] Schmidt, "The Estonian Cyberattacks", p. 18.
[78] Nakashima, "Defence official discloses cyberattack".
[79] Knowlton, "Military Computer Attack Confirmed".
[80] Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy", p. 97.

the flash drives. However, as said before, this computer worm still exists and in 2013 alone it was detected 13,832 times in 107 countries, most of them in Russia.[81]

Agent.btz was first detected when a mysterious signal that originated within the USA military's classified network was trying to send coded messages back to its maker. A special team of the National Security Agency (NSA) quickly determined that the classified network had been infected. This classified network is kept separate from the public Internet and it collected the most important military secrets and battle plans used in Iraq and Afghanistan. Government cyber experts could not decipher who created the program and for how long it had been in the USA's network, although they came to be suspicious of Russian intelligence. NSA experts found that agent.btz had infected two networks: the Secret Internet Protocol Router Network, used to transmit classified material, but not the most sensitive information; and the Joint Worldwide Intelligence Communication System, used to transmit top-secret information to country officials across the globe. What the experts also discovered was the self-replicating characteristic of the malware and that it was a computer worm looking for documents to steal.[82]

One possible explanation of how the malware reached the military computers is that an American soldier in Afghanistan went to an Internet café, attached a flash drive to an infected computer and used that same flash drive in a computer connected to the classified network. Once in the network, the malware self-replicated to steal information and to establish a communication with its maker, so as to receive further instructions on the files to look at and to transmit. These signals were noticed by the Advanced Networks Operations (ANO) section of the NSA, which designed a potential response to counter the malware.[83]

The reasoning behind this potential response was based on the signals emitted by agent.btz to its creator. Since the malware was waiting for instructions, ANO thought of finding a way to make the malware receive the instruction of shutting itself down. To achieve this objective, ANO designed a program overnight, which was tested the next day. The program recognized the communication signals of agent.btz and the program

[81] Infosecurity Magazine, "Worm that Wreaked Havoc for US Military Likely a Progenitor of Red October".
[82] Nakashima, "Cyber-intruder sparks massive federal response – and debate over dealing with threats".
[83] Nakashima, "Cyber-intruder sparks massive federal response – and debate over dealing with threats".

responded back. Soon afterwards, the malware on the test server dozed off permanently. With this test, a technical solution was found, but the challenge remained on how to neutralize agent.btz in every computer it had infected. To achieve this, Tailored Access Operations within NSA took part in operation Buckshot Yankee as well. TAO is specialized in intelligence operations abroad and focuses on collecting sensitive technical information. Thus, it ventured into electronic spying outside USA's military networks looking for the agent.btz malware and that is how TAO identified other variants of the computer worm.[84]

The use of offensive measures to neutralize agent.btz was also contemplated by the military's offensive cyber unit, the Joint Functional Component Command – Network Warfare. However, senior officials refused to approve this alternative based on the fact that the malware seemed to be an act of espionage rather than a conventional attack. Thus, an aggressive response was not justified.[85]

The NSA concentrated its work on neutralizing the worm in government computers. Considering that the situation might have started with an infected flash drive, part of this work included prohibiting the use of USB drives. The rate of new infected computers finally declined in early 2009. Still, no evidence could be found that agent.btz succeeded in transferring secret documents to unknown adversaries or in communicating with its creator. With that precedent, other security measures were put in place and the ban on the use of flash drives was modified.[86] Agent.btz is a variant of the computer worm called "SillyFDC", also a self-replicating malware and it was classified as "Risk Level 1: Very low" by the security firm Symantec in 2007. Because of its low risk level, it could be said that agent.btz was also a level 1 risk malware, whose ability to compromise classified information is to some extent limited.[87]

Operation Buckshot Yankee led to the creation of the USA Cyber Command (USCYBERCOM), a unit devised to protect military computers and communication systems. It began full operations on 31 October 2010 and has brought together into two other units: the Joint Task Force-Global Network Operations, in charge of the disinfection

[84] Nakashima, "Cyber-intruder sparks massive federal response – and debate over dealing with threats".
[85] Nakashima, "Cyber-intruder sparks massive federal response – and debate over dealing with threats".
[86] Nakashima, "Cyber-intruder sparks massive federal response – and debate over dealing with threats".
[87] Shachtman, "Insiders doubt 2008 Pentagon hack was foreign spy attack (updated)".

of computer systems that took 14 months[88]; and the Network Warfare Unit, the offensive cyber arm of the military.

However, USCYBERCOM did not resolve the issue of how to respond to cyberattacks. Still, officials from the Pentagon began to work in a set of rules of engagement for cyber defence during the summer of 2009. It proposed that the strategic and cyber commands could direct operations and defend military networks anywhere in the world. Nevertheless, several requirements had to be met first. In order to engage in cyber defence, the provocation had to be aggressive and directed either to the USA territory, its infrastructure or its population. Additionally, the provocation had to represent an imminent likelihood of damage that could threaten national or economic security, serious injury or death. The response then would be coordinated with combatant commanders and the government agencies that were affected by the aggression. Yet, the attempts to establish such rules of engagement failed due to concerns of other departments. For example, the Department of State worried the military could unintentionally disrupt a network in an allied country and undermine future collaboration with that nation. At the national level there were concerns as well, since the military has the mandate to act in cyberspace when an attack is launched from domestic networks, unless the attack comes from the military's own systems. The current set of rules of engagement was signed in February 2011 and it limits the military to the defence of its own networks and it needs a special permission from the president to engage in the defence of other networks.[89]

Despite claims of former US Officials that there was evidence of Russia taking part in the development of agent.btz, some doubted the malware was used to spy on US military computers and steal data. Others considered that Russia might have been involved at some stage of the computer worm's development and then that it was modified by others. Some, however, are convinced that agent.btz was created to target the Department of Defence. Since there was no conclusive attribution, Russia denounced such allegations as "irresponsible" and "groundless" in late 2008.[90]

[88] Zetter, "The return of the worm that ate the Pentagon".
[89] Nakashima, "Cyber-intruder sparks massive federal response – and debate over dealing with threats".
[90] Nakashima, "Cyber-intruder sparks massive federal response – and debate over dealing with threats".

As a final consideration, William J. Lynn in his article on Operation Buckshot Yankee, points out the amount of cyber research that the government of the USA conducts on a regular basis. This entails routine simulation exercises that are necessary for understanding the behaviour of malicious malware. The purpose of these exercises is to improve the government's capabilities to effectively attribute cyberattacks. Additionally, cybersecurity professionals receive further training, for example, Pentagon personnel is now trained in "ethical hacking", an exercise that comprises the use of techniques to hack the USA's own networks, in order to identify one's own vulnerabilities and address them before they are exploited by an intruder or cyber attacker.[91]

[91] Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy", p. 105, 106.

CHAPTER TWO: RESPONSES TO CYBERATTACKS FROM A REALIST PERSPECTIVE

Cyberattacks and defensive realism

Currently, cyberattacks have not resulted in casualties, but still they have the potential to do so. For this reason, the traditional understanding of interstate conflicts is needed, in order to articulate the eventuality of a cyberattack causing physical destruction and death.[92]

In addition to traditional interstate conflicts, the offensive and defensive aspect of the cyber domain must also be taken into consideration. Security planners in cyberspace regard the offense to have an advantage over the defence. The attacked system or network is unaware of the vulnerabilities that could be targeted by malicious attackers and/or malware. Thus, the difficulty in predicting a cyberattack hinders setting up measures to respond to, and counteract it. A malware that self-replicates to steal information, disrupt a system, or overburden it with excessive data has two main potential functions: (1) to infiltrate itself in the network and (2) to render the network inaccessible to its legitimate users. While the attacker needs to exploit the vulnerability that would allow him/her to conduct the attack, the defender must constantly reinforce and defend the network's protection against all possible forms of attacks. Thus, offense outweighs defence.[93]

This advantage of the offense over the defence is the structure that can be said is used by states to pursue power in the cyber domain. Due to the unpredictability of a cyberattack and the ever more present possibility of having a state cyber attacking another one, one could think each state would seek to be powerful enough in the cyber sphere to protect itself in the event of being cyber attacked.[94] This would be structural realism applied to cyberspace.

However, it is important not to forget that structural realism disregards different regime types among states, cultural differences and those responsible for the state's foreign

[92] Kello, "The Meaning of the Cyber Revolution," p. 23, 26.

[93] Kello, "The Meaning of the Cyber Revolution," p. 27, 28.

[94] Dunne, et. al., *International Relations Theories – Discipline and Diversity,* p. 72.

policy. Structural realists assume that states are alike, except for the fact that some are more or less powerful than others. Moreover, structural realism is divided in offensive realism and defensive realism. Considering the fact that offense has an advantage over defence in the cyber domain, defensive realism would provide the framework for strengthening the defence for responding to cyberattacks. Defensive realists identify that the international system creates incentives to gain additional power. Traditionally, power has been based on material capabilities, such as military assets, arms and nuclear weapons. Socio-economic aspects also go into strengthening the military power, as well as money, personnel and technology. Traditionally, war and increasing the share of global wealth were the only ways for states to gain power. Now, cyberspace and the possibility of conducting online attacks that could have effects equivalent to those of a conventional armed attack could represent a possible new way for acquiring an advantage over other states. Cyberspace could then be seen as an incentive for states to gain advantage and power over others. Still, defensive realism supports the argument that pursuing hegemony is foolish because states should not maximize power, but compete for a proper amount of power.[95]

Defensive realists also argue that an offence-defence balance exists. Such balance would usually be in favour of the defender and so any state trying to acquire more power is likely to finish up fighting wars it will lose.[96] Information technology and information flows in cyberspace, like military assets, have effects on the use of force that benefit both the less and the more powerful countries, even though dominant states will still have larger resources. Thus, a less powerful state, who is trying to gain power in the cyber domain by cyber attacking a more powerful state, will soon realize the ineffectiveness of engaging in such an attack and would concentrate more on keeping its share of power and its position in the international system.[97]

Under this understanding, cyberattacks could represent the offense-defence balance that defensive realists claim there is because probable aggressions in cyberspace are making states reinforce their networks' defences. A state that is constantly increasing its defences would be much better prepared in the case of an attack because it is ready to repeal and

[95] Dunne, et. al., *International Relations Theories – Discipline and Diversity,* p. 72, 73, 75.
[96] Dunne, et. al., *International Relations Theories – Discipline and Diversity,* p. 76.
[97] Nye Jr. *The Future of Power,* p. 117, 118.

defend its networks. In this scenario, smaller states trying to cyberattack a powerful state would realize the ineffectiveness of conducting such attack. Thus, cyberspace and the possibility of states resorting to cyberattacks would not represent a means to achieve hegemony because the offence-defence balance would be in favour of the country with reinforced defences. In this regard, when such balance is in the defender's favour, it is also allowing the country to defend its share of power in the international system.

Estonia's National Defence Strategy

If we look at the 2011 National Defence Strategy of the Republic of Estonia, it defines the Ministry of Defence as the responsible entity in charge of coordinating defence in the cyber domain as part of the national defence. The country also counts with a militarily-organized league called Estonian Defence League, which is a voluntary national defence organization within the Ministry of Defence in charge of developing cyber-defence capabilities. This League engages in military exercises and possesses arms as part of its training to aid in the defending of the country's territorial integrity, independence and constitutional order. As a nationwide organization, its administrative subdivisions support the implementation of other national defence efforts. One of the main purposes of the Estonian Defence League is to respond to any kind of threats that arise from developments in information technology.[98] Another of its purposes is to maintain technical cyber skills available at all times so to provide support to military cyber forces in case of an emergency.[99]

The Ministry of Interior of Estonia is another entity taking part in cyber issues. This Ministry is in charge of establishing the procedures for classifying the types of information and procedures for receiving and transmitting such information. Moreover, the Police and Border Guard Board is responsible for anticipating, identifying and preventing risks (including cyberspace risks) that are a menace to law and order. Furthermore, the functioning of communication networks is considered a service essential

[98] Ministry of Defense of the Republic of Estonia, "National Defense Strategy, Estonia", p. 12 – 14.
[99] Klimburg, ed., "National Cyber Security Framework Manual", p. 122.

to national defence, which falls under the scope of governance of the Ministry of Economic Affairs and Communications of Estonia.[100]

The 2007 cyberattacks against the government of Estonia marked a turning point in security considerations everywhere. Matters of cyber security became part of the political agenda and this was reflected in several national cyber security strategies released between 2009 and 2011. Ever since, policy-makers and decision-makers recognize the increasing relevance of cyber security. A study conducted by McAfee and the Security and Defence Agenda in 2012 revealed that 45% of the surveyed policy-makers considered cyber security as important as border security. Furthermore, the Estonian attacks in 2007 have drawn the attention to the protection of information infrastructures, prompting countries to have security strategies and cyber security strategies addressing cyber considerations.[101]

After the 2007 cyberattacks, it can be said that the Estonian government has been focusing in strengthening its defensive capabilities. The defensive tasks that have been assigned mainly to governmental institutions demonstrate the importance the government places to defence rather than offence. Moreover, cyber defence capabilities are tightly tied with the military capacity of the country. Cyber issues are part of Estonia’s national defence. For this reason, the Ministry of Defence is the entity responsible for coordinating the cyber defence capacity along with the military league within this Ministry. In Estonia, the traditional concept of military readiness to face threats from outside has been translated to the cyber domain, thus expanding military considerations to cyberspace.

Even though the militarily-organized Estonian Defence League is in charge of responding to information technology threats, the National Defence Strategy does not explain what kind of response it is referring to. Yet again, it can be understood that this response is focusing mainly on defending the country because of the tasks assigned to other governmental bodies. The Police and Border Control is in charge of the prevention of risks arising from cyberspace, while the Ministry of Economic Affairs is entitled to watching over the functioning of the information and communication networks, which the government of Estonia has identified as essential for national defence.

[100] Ministry of Defense of the Republic of Estonia, “National Defense Strategy, Estonia”, p. 19, 21, 22.
[101] Klimburg, ed., “National Cyber Security Framework Manual”, p. 50. 53.

For Estonia, the country's security is not just seen as strengthening its military defence with the direct involvement of key state entities such as the Ministry of the Defence and the Ministry of Interior. The country's security in the cyber domain is also thought of as one that counts with the development of cyber defence capabilities and risk management of menaces that could threaten national defence infrastructures, such as communication networks. The current legislation in Estonia is not showing that the country is pursuing hegemony, but that it is trying to preserve its share of power by strengthening its defensive capabilities.

United States' Cyber Strategy

Improving and strengthening defence capabilities is also envisaged in current legislation of the United States. The Cyber Strategy of the USA is a document designed by the Department of Defence (DoD) to reduce and counter threats from cyberspace. According to the strategy, the DoD is the entity responsible for defending the USA's territory and interests from any attack, including cyberattacks. The DoD seeks to deter such attacks and to this end it has developed capabilities for operations in cyberspace.[102]

The strategy encompasses three missions for cyber operations. The first one is that the DoD must defend its own networks and information systems. Due to the fact that the US military is highly dependent on cyberspace for its operations, the DoD must secure its networks from any attack and recover quickly when security measures fail. For this reason, the DoD conducts network defence operations on a regular basis to identify its own vulnerabilities in the cyber sphere. The second mission is that the DoD must be prepared to defend the USA and its interests against cyberattacks. Cyberattacks against the USA are assessed on a case-by-case basis by the President and the National Security Team. For this reason, the military may conduct cyber operations to counter such attacks if directed by the President or the Secretary of Defence of the USA. The final mission establishes that when directed by the President or Secretary of Defence, the DoD must be able to provide cyber capabilities to support military operations. This entails that the

[102] Department of Defense of the United States of America, "The DOD Cyber Strategy", p. 2, 3.

military could conduct cyber operations to disrupt an adversary's infrastructures or networks if the President or the Secretary of Defence considers it appropriate, in order to protect USA's interests. In addition to the military, the United States Cyber Command (USCYBERCOM) could also be asked to conduct cyber operations to defend, deter and counter cyber threats.[103] For the USCYBERCOM a defensive cyber operation involves synchronizing actions that would allow for the detection, analysis, counteraction and mitigation of cyber threats, as well as for the protection of important missions that would facilitate the USA's freedom of action in cyberspace.[104]

The cyber strategy gives deterrence a crucial role, and so it is the DoD who must work on developing and implementing such a cyber deterrence strategy. To achieve this, the DoD realizes that deterring cyberattacks does not only involve articulating policies, but also developing warning capabilities, effective response procedures, and resilient networks. The cyber strategy stresses that the USA must be able to demonstrate effective response capabilities to deter an adversary from initiating an attack, as well as effective defensive capabilities to counter a potential attack.[105]

The cyber strategy clearly mentions that the USA will use its defence capabilities to respond to cyberattacks that target USA's interests and it will continue to use its capabilities *"at a time, in a manner, and in the place of our choosing"*[106] according to applicable laws. Still, the response to an attack depends on attribution and it must be addressed in order to have effective deterrence. Attribution is essential for cyber deterrence because anonymity allows harmful activities to take place in cyberspace. Attribution entitles the DoD and other related agencies of the state to conduct proper responses against cyberattacks, which may include, but are not limited to: diplomatic actions, law enforcement actions or economic sanctions.[107]

According to the CCD COE Manual, retaliation measures goes hand in hand with deterrence. When the USA says it will respond to a cyberattack as if it were any other threat to the country, the fact of mentioning possible retaliations such as economic or

[103] Department of Defense of the United States of America, "The DOD Cyber Strategy", p. 4, 5.
[104] Klimburg, ed., "National Cyber Security Framework Manual", p. 13.
[105] Department of Defense of the United States of America, "The DOD Cyber Strategy", p. 10, 11.
[106] Department of Defense of the United States of America, "The DOD Cyber Strategy", p. 11.
[107] Department of Defense of the United States of America, "The DOD Cyber Strategy", p. 12.

diplomatic means already serve as a deterrent. In order for these retaliations to be feasible, not only attribution must be addressed, but also offensive capabilities because they would make the probability of retaliating credible. As a result, countries interested in conducting a cyberattack would be aware of the consequences of engaging in such an attack.[108]

Using deterrence as a means to enhance defensive capabilities could probably work in the case of the most severe attacks like, for example, those that would have effects equivalent to conventional military attacks. In this regard, the United States is the clear enforcer of such practice, since the country spends a considerable amount of its cyber budget on developing and strengthening its defensive capabilities. The active engagement in improving the USA's defence has to some extent supported its deterrence policy. Nevertheless, this strategy still relies on attribution. Even though advancements in technology could eventually facilitate attribution in cyberspace, it still remains improbable that attribution in cyberspace would reach the attribution level given, for example, to the firing of a ballistic missile. Despite the United States advocates for defence by deterrence, it requires both attribution and offensive cyber capabilities to ensure retaliation possibilities are credible.[109]

Public-private partnership remains the cornerstone of the United States' cyberspace security strategy.[110] This aim goes hand in hand with the DoD's goals of developing cutting-edge technologies and innovations to enhance defence capabilities in cyberspace, achieve security objectives, reduce destruction of properties and prevent loss of life. There are several processes the DoD has devised to implement its goals. Of relevant importance are building a cyber workforce and technical capabilities for cyber operations, developing mechanisms and capacities to mitigate vulnerabilities that pose a risk to data from the DoD and its networks. Additional processes include developing a plan for network resilience and network defence, mitigate insider threats, develop and collect intelligence that would allow anticipation of cyberattacks and assess deterrence strategies.[111]

[108] Klimburg, ed., "National Cyber Security Framework Manual", p. 83.
[109] Klimburg, ed., "National Cyber Security Framework Manual", p. 84.
[110] Harknett and Stever, "The New Policy World of Cybersecurity", p. 456.
[111] Department of Defense of the United States of America, "The DOD Cyber Strategy", p. 13 – 28.

The document of the cyber security strategy finishes with managing considerations of the strategy. To achieve its objectives, cyber forces and personnel is required. Thus, the Office of the Principal Cyber Advisor to the Secretary of Defence has been established. At the same time, the DoD works towards improving efficiency and transparency regarding budget management of cyber operations, as well as developing a framework for cyber operations and cybersecurity policy.[112]

The Cyber Security Strategy of the DoD can be said is very much aligned with defensive realism postulates, especially because the three missions for cyber operations envisaged in the strategy seek to reinforce defensive capabilities and information networks of the United States. The Department of Defence is the entity responsible for safeguarding the country's territorial sovereignty, as well as its political independence and interests from any type of attacks including cyberattacks. In this regard and like in the case of Estonia, there is also a strong combination of defensive and military considerations.

This entails that the USA regards military readiness as a crucial aspect for developing effective responses to cyberattacks and this notion is supported by the three missions envisaged in the Cyber Strategy. The three missions for cyber operations already point out the existent dependence of military's defence operations on information networks. In this regard, the defence of networks is tied to the performance of the military in safeguarding USA's interests and territory. In other words, the military can fulfil its duties as a defender of the USA's territory and interests against cyberattacks because information networks are protected and defended for optimal performance. This is the reason why the network defence operations conducted by the DoD to identify its own vulnerabilities allows the country not only to defend its national interests and networks, but also to reinforce the military. Additionally, the fact that the DoD could develop cyber capabilities to support military operations further strengthens the active role of the defence against cyberattacks. The military defence capabilities are crucial not only because they allow the USA to defend itself from cyberattacks, but also because they open the possibility for the USA to conduct cyber operations to disrupt and adversary's infrastructures or networks that are seen as threat to the security of the country. For this

[112] Department of Defense of the United States of America, "The DOD Cyber Strategy", p. 29, 30.

reason, it can also be said that the DoD Cyber Strategy might also represent a cornerstone for eventual offensive counteracts to cyberattacks in the future.

Improving defensive capabilities are crucial for the security of the USA. However, the cyber strategy suggests that the USA is looking for a more active role than just defending itself from cyberattacks. After the 2008 cyberattack to the country's military, the USA has been engaging more actively not just in developing its defensive capabilities, but also in developing effective responses to cyberattacks. Even though the strategy mentions that cyberattacks are assessed on a case-by-case basis, the USA is also interested in establishing effective response capabilities because that would allow it to further develop technical capacities, and mechanisms to mitigate vulnerabilities in information networks. The mitigation of such kind of threats along with strong defence capabilities is what could allow the USA to turn deterrence into a more dominant aspect in cyberspace, something which is also in the interest of the USA, to lead in the quest of defining responses to cyberattacks.

Hypothesis' validation

Taking these considerations into account, it can be said that states do improve their defensive capabilities when they perceive their security is threatened by a cyberattack. This confirms the validity of the first hypothesis and the two analysed case-studies corroborate this fact.

On the one hand, during the 2007 cyberattacks against Estonia, the country improved its defences because the DDoS and the botnets threatened its security. The attack did not include a military intervention, so in this regard no territorial sovereignty was violated. However, the country's political independence was damaged because the DDoS and the botnets rendered the government unable to provide information to authorities and to its citizens because authoritative web sites and media sites were inoperative. Likewise, financial transactions were inoperative and the disruption of bank services online brought financial consequences. When orders cannot be communicated and financial transactions are frozen, the country has no control over the institutions and mechanisms it is supposed to control and this is what happened during the 2007 cyberattacks. For this reason, improving firewalls and making encryption mechanisms stronger were part of the defence capabilities that were improved during and after the cyberattack.

In the aftermath, Estonia has perceived that is security is threatened by the possibility of being cyberattacked again. This is the reason why the country has established governmental bodies like the Ministry of Defence, Ministry of Interior and Ministry of Economic Affairs, among others, to develop cyber defence capabilities. The country has also focused in assuring the well-functioning and well-protection of information networks. Estonia's defensive capabilities have not been just focused on strengthening the military because the military has become one element within the defensive capacity of the country against cyberattacks.

On the other hand, the 2008 cyberattack against the USA's military network was not a military intervention either. Still, the political independence of the country was partially affected because the malicious self-replicating worm infiltrated a key branch of the state: the military, the main arm in charge of defending the country. Due to the fact that the malware was trying to communicate with its creator to retransmit the information it was trying to steal, although in the end it was not successful, such attempt nevertheless could be seen as in interference with sensitive information of the USA. The United States resorted to improving its defences during the attack and that led to the development of the software that was able to doze off the malware. As a consequence, improving defensive capabilities has become of vital importance. This can be seen in the simulation exercises conducted on a regular basis by the DoD to improve the government's capabilities to effectively defend itself from cyberattacks.

The current legislation in the USA also shows that the country perceives its security is threatened by cyberattacks. This is the reason why it has also focused on improving defensive capabilities. Such defensive capabilities are not the ones from the military only, but also the ones from information networks and infrastructures because an attack on information systems can threaten USA's national security. Even though the country is focusing on improving its defences, coming up with offensive capabilities and responses to cyberattacks is also envisaged in its cyber strategy because the USA sees defensive capabilities no just as a means to protect the country from a cyberattack, but also as a means to respond to the attack. This is also the reason why the cyber security strategy mentions that diplomatic actions, economic sanctions or law enforcement could be considered as possible responses to cyberattacks. Despite the fact that the attribution challenge is still present, it can be said that for the USA developing a stronger defensive capacity to respond to cyberattacks could be part of solving the attribution challenge itself. This goes hand in hand with the strategy of defence by deterrence that the United States has adopted. The country is aware that solving the attribution challenge and developing offensive capabilities would make retaliation measures credible and would strengthen its defence by deterrence strategy. This means that once reached the point of having strong defensive capabilities and well-defended infrastructures and networks, the USA will eventually seek to improve its offensive capabilities in cyberspace.

For the time being and in a general perspective, cyberattacks are making states focus on improving their defence capabilities not to pursue hegemony, but to protect its territory and its political independence. At the same time, states are also focusing on keeping their share of power in the international system. As of today, most states are concentrating efforts on discovering their system's vulnerabilities and in reinforcing their networks and systems in the case of being cyberattacked. Considering the financial, technical and human resources needed to improve defences, this could be another reason why big and small states are focusing at the moment just on defending themselves from cyberattacks. The United States and Estonia, as the examples of this thesis, already show how strengthening defensive capabilities are important for powerful and less powerful states. It also shows that the possibility of developing offensive strategies has not been excluded.

CHAPTER THREE: RESPONSES TO CYBERATTACKS FROM A LIBERAL PERSPECTIVE

Cyberattacks and international institutions

An important consideration when analysing responses to cyberattacks is that power does not refer to information-based power, but it refers to cyber power and it can relate to two important aspects: (1) the resources involved in the creation, control and communication of computer-based and electronic information, and (2) that information resources in cyberspace are used to obtain specific expected outcomes. Even though states remain the most important actors in the international system, it must be taken into account that the interconnectedness of information networks, the vulnerabilities that come along with such interconnectedness and the dissemination of information have widely distributed power. Thanks to technology, individuals and non-state actors can now access destructive powers that were once exclusively reserved to governments. Thus, cyberspace is not replacing geographical boundaries or the state's sovereignty, but it hinders what it takes to be a sovereign state or a dominant country.[113]

Because of this diffusion of power, Joseph Nye argues that one cannot talk about dominance in cyberspace like in airpower or sea power. In this regard, the challenges of effectively attributing a cyberattack contribute to the growing diffusion of power among countries. The broad number of actors and a relative reduction of power-share among them is another consideration why it is not possible to gain dominance in the cyber sphere. Even when cyber dominance would not be possible, alliances seem to be proliferating in this context, since criminal groups or teenage hacking skills are advantageous for states, who are seeking opportunities to increase capabilities in cyberspace whilst denying involvement in cyberattacks.[114]

Taking this into account, several international organizations have been working closely with their member states on stablishing guidelines for addressing cybersecurity issues. The North Atlantic Treaty Organization (NATO) possesses extensive knowledge on cyber security. NATO's first policy on cyber defence was approved in January 2008 following

[113] Nye Jr. *The Future of Power,* p. 114, 116, 121-123.
[114] Nye Jr. *The Future of Power,* p. 125, 132. 137.

the cyberattacks against Estonia in 2007. By 2011, NATO approved a second policy on cyber defence, which envisaged coordinated efforts and an action plan in cyber defence.[115]

Although Hathaway et.al identified that NATO does not regard a cyberattack as an armed attack and that member states would not be obliged to assist each other under Article 5 of the NATO treaty;[116] in September 2014 at the Wales Summit, NATO member states agreed upon an improved policy and action plan on cyber defence. This policy makes cyber defence part of NATO's core exercise of collective defence. It assures that international law is applicable to cyberspace activities and it emphasizes NATO's collaboration with the industrial sector. The main purpose is to protect NATO's information and communication systems.[117] In this regard, Article 5 of the treaty on collective self-defence could be invoked if the effects of a cyberattack are comparable to those provoked by a conventional armed attack. Nevertheless, the policy does not specify the criteria necessary for triggering Article 5 and it would need to be decided by the member states on a case-by-case basis. Additionally, the policy points out that NATO is responsible for defending its own networks while states are expected to defend theirs. [118]

NATO's Policy on Cyber Defence is implemented by political, military and technical authorities of the Organization, as well as by individual member states. The most important bodies involved in this process are the following: The North Atlantic Council (NAC) is the high-level entity for overseeing the implementation of the policy. The Cyber Defence Committee, subordinated to the NAC, leads the general political governance and defence policy regarding cyber issues. The NATO Cyber Defence Management Board (CDMB) coordinates cyber defence with NATO's civilian and military bodies. NATO's Consultation, Control and Command Board (NC3) is the main consultation body regarding technical and implementation aspects of cyber defence.[119]

NATO praises efforts on setting confidence-building measures and advocates sharing best practices to promote a more transparent behaviour in cyberspace. NATO has also

[115] NATO, "Cyber defence".
[116] Hathaway, et. al, "The Law of Cyber-Attack", p. 846.
[117] NATO, "NATO Cyber Defence Fact Sheet", p. 1.
[118] NATO, "NATO Summit Updates Cyber Defence Policy".
[119] NATO, "Cyber defence".

developed targets for member states to implement national cyber defence capabilities and conducts regular exercises to better integrate and enhance elements for cyber defence, cyber education and training. The organization has further increased its collaboration with the UN, the EU, the Council of Europe and the OSCE.[120] For instance, in February 2016, NATO and the EU signed a Technical Arrangement on Cyber Defence. It aims at better preventing and responding to cyberattacks by means of information-sharing on specific cyber threats, sharing best practices on network configuration and other technical procedures, as well as practices on partnerships with the industrial sector.[121]

At the Warsaw Summit of 14 June 2016, defence ministers agreed to incorporate cyberspace as an additional operational domain to NATO's domains of air, sea and land. Such recognition does not alter NATO's defensive mandate. Later, in July 2016, Heads of State and Government of member states reiterated NATO' defensive mandate and the identification of cyberspace as an operational domain for the organization. Along the same lines, it was emphasized that NATO should defend itself in cyberspace as effectively as it does in the air, on land and at sea domains. On the other hand, member states agreed to improve their resilience and capacity to effectively respond to a cyberattack.[122]

In addition to NATO, the Organization for Security and Cooperation in Europe (OSCE) is broadly engaged in addressing cybersecurity issues. The organization adopted Decision No. 1106 on 3 December 2013 and it defined an initial set of confidence-building measures (CBMs) on the use of information and communication technologies (ICTs).[123] The CBMs have been regarded as ground-breaking risk-reduction measures since they are expected to improve transparency and curb escalation among countries. CBMs are based on information-sharing and communication, the exchange of lessons learned and best practices at the government and expert level, in order to increase stability and cooperation between states.[124]

[120] NATO, "NATO Cyber Defence Fact Sheet", p. 1, 2.
[121] NATO, "NATO and the European Union enhance cyber defence cooperation".
[122] NATO, "Cyber defence".
[123] OSCE, "Decision No. 1106 - Initial set of OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies".
[124] OSCE, "Confidence building measures to enhance cybersecurity in focus at OSCE meeting in Vienna".

Decision No. 1106 establishes eleven CBMs based on a voluntary cooperation among participating states. Thus, they are encouraged to voluntarily provide their national insights in terms of national and international threats that could stem from compromised security of, and/or the use of ICTs. On a voluntary basis, states can also hold consultations to reduce possible tensions coming from the use of ICTs, as well as to protect critical ICT infrastructure at a national and international level. Furthermore, participating states should advocate for information-sharing, awareness-raising and capacity-building on measures that can bring about a more reliable Internet, the safe use of ICTs and responses to related threats. Likewise, states are encouraged to share national policies, programs and public-private partnerships relative to the safe use of ICTs. In the absence of agreed upon terminology on cyber terms, Decision 1106 provides a very interesting and quite useful CBM to have states voluntarily share a list of national terminology related to security of, and in the use of ICTs. Each participating state is free to choose the terms it considers most necessary to share. This is enhanced with the measure of states having a contact point, in order to facilitate dialogue among countries. A long-term objective is to come up with an agreed upon glossary of terms related to security of, and in the use of ICTs.[125]

To ensure an effective implementation of the CBMs, it is not only necessary that national policy-makers be involved, but also stakeholders from the private and non-governmental sectors. The protection of ICTs and critical infrastructures from cyber threats is a priority for both the infrastructure operator and national security authorities.[126] The CBMs have had positive impacts in OSCE participating states, for there has been an increase in the share (from 61% in 2015 to 90% in 2016) of states that have implemented one or more CBMs. Thus, in 2016 the OSCE adopted new CBMs on cyber and ICT security measures, which promote greater collaboration at the regional level, protection of critical infrastructure, channels for crisis communication, and stronger public-private partnerships.[127]

Other organizations such as the Organization for American States (OAS) and the Shanghai Cooperation Organization (SCO) have recently taken actions that address

[125] OSCE, “Decision No. 1106 - Initial set of OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies”, p. 1, 2.
[126] OSCE, “Confidence building measures to enhance cybersecurity in focus at OSCE meeting in Vienna”.
[127] OSCE, “OSCE milestones in cyber/ICT”, p. 2.

cyberattacks. A 2004 resolution of the OAS advises member states to evaluate implementing the provisions established in the Council of Europe's Convention on Cybercrime, as well as considering acceding to the Convention. The OAS has developed a "Comprehensive Inter-American Cybersecurity Strategy", which aims at adopting legislation to protect from, and prevent cybercrime. These guidelines, however, do not mention how states can combat cybercrime or cyberattacks. On the other hand, the SCO has taken significant steps in terms of cooperation in cybersecurity. Their Yekaterinburg Declaration of 2009 establishes that international information security is crucial for a common system of international security. Thus, the organization has adopted an ample understanding of cyberattacks and that the use of cyber technologies could undermine political stability. To some extent, such framework opposes western views in the sense that western countries try to avoid cyber-regulations that might undermine the expression of political dissent.[128]

Likewise, the European Union (EU) is taking steps to address cybersecurity issues. The European Parliament's directive of 6 July 2016 on Security of Network and Information Systems (NIS) is an example. This directive comprises the EU's first rules on cybersecurity and sets the foundations for achieving a common level of information and network security within the EU. This would be achieved by improved capabilities on cybersecurity at a national level, increased cooperation at the EU level and defined risk management and incident reporting responsibilities for operators and service providers. In order for member states to increase their cybersecurity capabilities, each country will adopt national strategies on network and information security, which should include, inter alia, public-private partnerships, awareness raising and other actors involved in the implementation of the strategy. Furthermore, states should designate Computer Security Incident Response Teams (CSIRTs), which should be in charge of monitoring incidents at country level, provide early warning and respond to incidents. At the EU level, a Cooperation Group and network of national CSIRTs will be set up, to coordinate information-sharing and develop further trust and confidence among member states. Regarding the final aspect covering operators and service providers, the NIS Directive requires them to take appropriate security measures for their information and network systems and report serious anomalies to relevant national authorities. Operators in the

[128] Hathaway, et. al, "The Law of Cyber-Attack", p. 864, 865.

energy, transport, banking, financial markets, health, water and digital infrastructures must adopt such security measures under the NIS Directive. In case of serious incidents, the Directive establishes three main parameters that operators must look at: number of affected users, duration of the incident and geographic spread. In the case of digital service providers, they should take into account two additional parameters: the extent of the disruption of the service and the impact on economic and social activities.[129]

Thus far, the mentioned international organizations are aware of the challenges that cybersecurity incidents pose to the international community. Information dissemination is possible thanks to interconnected networks on a global scale. However, at the same time such networks represent a vulnerability to states because cyberattacks can be disseminated through these networks and affect not just one but many countries. For this reason, states are also aiming at improving their defensive capabilities by cooperating with international organizations because they provide states with a collaborative forum for sharing information and building partnerships. It is worth noting that such partnerships are built not only among states, but also with other actors such as the industrial and the private sector to mutually benefit and enhance national defensive capabilities in cyberspace and the organization's collective cyber defence.

Estonia's National Security Concept and Cyber Security Strategy

When we look at Estonia, its National Security Concept points out at how globalization has increased interdependence and interconnectedness among countries and the security threats that this process brings along. In terms of information and communication technologies, the security concept notes that distorted information may impact international relations negatively. Furthermore, this document mentions the existent and growing dependence on the use of cyberspace, the difficulty of attributing cyberattacks, as well as the growing abuse of cyberspace by terrorist groups. Cyberspace is an important security consideration for Estonia. Thus, the protection of information and communication systems is necessary, since inadequate capabilities to respond to

[129] European Commission Press Release Database, "European Commission - Fact Sheet: Directive on Security of Network and Information Systems".

cyberattacks targeting critical services may render other critical services unavailable for society.[130]

Estonia's security concept emphasizes the importance of combating crimes conducted by means of information technologies. For this reason, prevention of cybercrime is crucial for ensuring proper functioning of communications and information systems, and financial security. Within the cyber sphere, ensuring cybersecurity is vital for the country, in order to reduce vulnerabilities found in communication networks and information systems. According to the security concept, cybersecurity needs an effective legal framework, so as to raise awareness about the importance of information security.[131]

Estonia's 2014-2017 Cyber Security Strategy refers to the increasing possibilities the Internet offers for potential attacks, along with the growing threat posed by cyber criminals and cybercrimes. The strategy clearly highlights the increasing dependence on information technologies as the main risk for cybersecurity. Estonia stresses the necessity of timely detection and response to cyberattacks that threaten the state and society. In order to achieve this, the strategy integrates civilian and military resources not only to prevent and deter cyber threats, but also to enhance cybersecurity-related technology and know-how.[132]

The strategy indicates that cybersecurity is an integral part of Estonia's national security, which is ensured in cooperation between the public and private sectors. Due to the interdependence and interconnectedness of existing infrastructures and networks in cyberspace, anticipation and prevention of potential threats is a top priority for ensuring cybersecurity. Additional goals of the cybersecurity strategy include delineating methods to ensure uninterrupted operation of vital services, as well as the protection of critical information infrastructures against cyberattacks. Communication and information technology infrastructures are constantly updated and protected from cyber threats. Although the strategy explains that a national monitoring system for cyber security is

[130] Ministry of Defense of the Republic of Estonia, "National Security Concept of Estonia", p. 5, 6, 8.
[131] Ministry of Defense of the Republic of Estonia, "National Security Concept of Estonia", p. 17, 18.
[132] Ministry of Economic Affairs and Communication of the Republic of Estonia, "2014–2017 Cyber Security Strategy", p. 5, 6.

adopted, the document itself does not provide further details on the functioning of this system.[133]

The current legislation in Estonia reflects awareness in terms of the effects that interconnected networks and the information transmitted through them can have in international relations. This is important because Estonia is not disregarding that the dissemination of distorted information through such networks can affect the country. Such was the case during the 2007 cyberattacks, when distorted information distributed by the cyberattacked web pages reached out the population. As the National Security Concept clearly identified, distorted information is an ever-present menace that can deteriorate international relations. This is the case not just because cyberattacks conducted through information networks can reach and affect several countries, but also because other non-state actors and individuals can find ways to access these networks to conduct their own cyberattacks or espionage activities. Thus, Estonia is recognizing this plurality of actors in the cyber domain and advocates for timely detection of possible attacks. The country's legislation shows that it is following general guidelines and recommendations from international organizations like, for example, a close cooperation between the public and private sector. Additionally, Estonia's Cybersecurity Strategy envisages a better integration between civilian and military resources, which can also be said it goes in line with NATO's procedures of integrating civilian and military bodies in an attempt to improve defensive capabilities that would allow for better responses to cyberattacks.

United States' National Security Strategy and International Strategy for Cyberspace

In the case of the United States, the National Security Strategy (NSS) emphasizes from the very beginning the widespread growth of disruptive and destructive cyberattacks, as well as the susceptibility of globally interconnected networks to cyber threats.[134] The NSS stresses several times the need for collective action to ensure access to cyberspace and also to address malicious activity in the cyber sphere. In addition to collective action,

[133] Ministry of Economic Affairs and Communication of the Republic of Estonia, "2014–2017 Cyber Security Strategy", p. 7 – 9.

[134] Presidency of the United States of America, "National Security Strategy", p. 1, 4.

the USA places significant importance to the role of the military, since strategically it is the military's responsibility to remain ready to deter and defeat any sort of threat to the homeland, including cyberattacks. To achieve this, the USA seeks not only to increase investment in cyber capabilities, but also to work closely with owners and operators of critical and cyber infrastructure to decrease vulnerabilities and increase resilience.[135]

For the United States, a close collaboration between the government, private sector and civil society is necessary to strengthen the country's security and critical infrastructure. The NSS points out that the USA will defend itself against cyberattacks. This is an interesting aspect considering that it has been mentioned that attribution is necessary to determine the type of response to the cyberattack. Nevertheless, the USA will not only seek to respond to the attack, but also to retaliate against cyber attackers through the prosecution of illegal cyber activity. At the international level, the USA seeks to promote rules and norms of responsible behaviour in cyberspace. On the other hand, the USA aims at expanding cybersecurity issues to protect trade and businesses, to defend networks against cyber theft of commercial secrets.[136]

Moreover, the International Strategy for Cyberspace explains in more detail the United States' actions towards cybersecurity. This strategy recognizes that traditional forms of conflict are now taking place in cyberspace. For instance, the disruption of an Internet network in one country can have a cascading effect and disrupt a much larger international network. Thus, the strategy stresses the potential cybersecurity threats have to endanger international peace and security.[137]

This strategy is based on three core principles: fundamental freedoms, privacy and the free flow of information. The first one refers to the freedom of information through any means and regardless of national borders, but always taking into account exceptions to freedom of speech, as in case of incitement to hate speech, for example. Privacy refers to the right every individual has to understand how his/her personal data will be used. The last one, free flow of information, emphasizes that solutions to cybersecurity threats should not affect the network's performance. In the commercial context, it points out that

[135] Presidency of the United States of America, "National Security Strategy", p. 7 – 9.

[136] Presidency of the United States of America, "National Security Strategy", p. 12, 13, 24.

[137] Presidency of the United States of America, "International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World", p. 4

cyberspace must promote innovation and should not be used as a space for creating disadvantages by disrupting the free flow of information.[138]

There are seven interdependent areas of activity for the effective implementation of an international strategy for cyberspace. All of them require strong collaboration between the government, private sector and international stakeholders. These areas include:[139]

1. Economy: Sustain free trade to ensure innovation in the information technology sector; protect information related to intellectual property and trade secrets; and promote international standards for technical requirements of products and services.
2. Protection of networks: Consolidate regional and international agreements on norms for cyberspace, seek international unanimity to ensure networks' stability, and promote international cooperation to develop best practices in the protection and integrity of information and infrastructures.
3. Law enforcement: Recommend to states to have the Budapest Convention on Cybercrime as a reference to formulate national laws related to cybercrimes, foster approaches on preventing and prosecuting cyber offenders rather than limiting Internet access, and encourage tracking of cybercrime financial networks by means of international frameworks such as the Financial Action Task Force.
4. Military: Ensure that the military remains equipped in the eventuality of disruption of systems crucial to national defence, enhance collective self-defence and collective deterrence in cyberspace, and promote exchange of best practices in digital forensics.
5. Internet governance: Prioritize innovation and openness of the Internet, and encourage dialogue on Internet governance.
6. International development: Build cybersecurity capacity in close collaboration with the private sector and international organizations, provide training to promote technical understanding and promote law enforcement, and further collaboration on protection of information and infrastructures.

[138] Presidency of the United States of America, "International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World", p. 5.
[139] Presidency of the United States of America, "International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World", p. 17 – 24.

7. Internet freedom: Advocate fundamental freedoms of association and of expression in cyberspace, strengthen frameworks regarding data privacy, and ensure the integrity of information flows.

Both the National Security Strategy and the International Strategy for Cyberspace of the USA call the attention on the cascading effects of cyberattacks by means of global interconnected networks. Operation Buckshot Yankee reflects such cascading effect when we look at how agent.btz managed to automatically self-replicate and spread to other servers. Due to the fact that global networks have made the international community susceptible to cyberattacks, the USA's strategies focus on strengthening collective action. Additionally, collective action must be coordinated with the military branch, in order to defend oneself from a cyberattack. Such legislation does not only envisage a collaboration with the private sector and with international organizations, but goes beyond what could be a mere political collaboration and emphasizes how the commercial branch is also relevant when dealing with cyberattacks. This is the reason why the National Security Strategy considers that cybersecurity issues should be expanded to the protection of trade secrets and the promotion of trade. This liberal approach is also present in the International Strategy for Cyberspace, for this strategy places significant importance to certain freedoms that should be regarded in the cyber domain too, like freedom of information, privacy and the free flow of information.

At the same time, interconnectedness of economies and information infrastructures due to globalization are enshrined in the USA's International Strategy for Cyberspace. Its international scope encompasses seven areas that go hand in hand with the process of developing a mechanism for better defending from, and responding to cyberattacks. The interconnectedness of these areas reveals not only liberal principles, such as the promotion of free trade in the economy area, innovation and openness in the area of internet governance, or integrity of information flow in the area of internet freedom. These areas also reveal a close collaboration with internationally agreed upon agreements, such as reinforcing guidelines to track cybercrime as proposed by the Financial Action Task Force, international cooperation to protect international information infrastructures, and the collaboration with international organizations to promote law enforcement. The military is also included as part of the interdependent areas as it points out the need for supporting collective defence and the exchange of best practices in relation to cyberattacks.

Hypothesis' validation

Cyberattacks can take advantage of international network's vulnerabilities and create disadvantages in terms of information sharing and even in terms of trade, thus disrupting the networks and the free flow of information. With these elements in mind, the hypothesis proposed for the liberal theory holds true for Estonia. The analysis shows that Estonia is aware that its security interests are dependent on global information networks. Even though the country's legislation does not explicitly say that the state is improving cooperation with international organizations, the country is indeed collaborating closer with them. The collaboration with NATO by means of the Cooperative Cyber Defence Centre of Excellence in Tallinn is a clear example, since it has proven to be a platform for independent experts to gather and advance knowledge related to cybersecurity issues. Estonia is focusing at the moment on reinforcing its national defensive capabilities in collaboration with the private sector. But at the same time, it is also contributing to international organizations with awareness and expertise on cyber issues. This has served as a baseline for international institutions to develop guidelines on how to better address cyber issues like, for example, the EU NIS Directive.

In the case of the Unites States, the hypothesis also holds true. The USA is quite aware of the existing dependence on global interconnected networks and their interests are inevitably tied to this reality. The USA is also aware of the possibility of being subject to many other cyberattacks because of global information networks and this is the reason why it seeks to improve and further collaboration with international organizations. This position is also supported by the country's International Strategy for Cyberspace, which emphasizes the importance of international cooperation with international organizations to promote law enforcement and the protection of information infrastructures. Like the USA, many other countries have cybersecurity interests and for this reason, it can be said that the USA is trying to consolidate norms for cyberspace at a regional and at an international level because by collaborating with international institutions, cybersecurity interests could be further protected.

CHAPTER FOUR: RESPONSES TO CYBERATTACKS FROM A CONSTRUCTIVIST PERSPECTIVE

Cyberattacks and international norms

When it comes to international norms, principles of international law as enshrined in the Charter of the United Nations are the widely accepted and agreed upon norms of the international system. In the cybersecurity area it is important to look at international law not only because cyberattacks have an international scope, but also because, as mentioned in the previous chapter, it has been recognized that international law applies to cyberspace.

Cyberattacks also pose an interpretation challenge to Article 51 of the UN Charter. Article 51 allows states to exercise the right of self-defence in the event of an armed attack.[140] However, discussions on whether to consider a cyberattack an armed attack continue and there is still no agreement on this matter. If Article 51 is to be invoked, a definition of an armed attack in cyberspace is required. Furthermore, the CCD COE Cyber Security Manual mentions that to this day there have not been cyberattacks brought before the Security Council or any other UN body.[141]

As discussed previously, cyberattacks pose an attribution challenge, which makes it difficult to have absolute certainty of attribution of a cyberattack. Member states of the United Nations are subject to the provisions of the UN Charter and if it is thought that a state is responsible for a cyberattack, then Article 51 of the UN Charter could be invoked, but it must follow the principles of law in armed conflicts. On the other hand, if it is thought that a person was responsible for the cyberattack, then the UN Charter cannot provide guidance on how to respond to the attack. In this case, it must be established if the attack had all characteristics to be considered a cyberattack or if it was a cybercrime. If it was a cybercrime, then criminal law could provide guidance on how to respond to it, but also provided that such criminal law has provisions to punish cybercrimes.[142]

[140] United Nations Organization, “Charter of the United Nations”, p. 32, 33.
[141] Klimburg, ed., “National Cyber Security Framework Manual”, p. 151, 170.
[142] Klimburg, ed., “National Cyber Security Framework Manual”, p. 168.

The possibility of considering a cyberattack as a military attack is contested by scholars as well. Hathaway et. al. emphasize that a state could respond lawfully to a cyberattack under Article 51 only if this attack rises to the level of an armed attack.[143] Brecher contends that cyberattacks cannot be regarded as attacks with conventional weapons because of key attributes of cyberattacks. Cyberattacks' remote access, difficulty of attribution and unpredictable effects, hold no similarity with military attacks, whose effects are predictable and where attribution is possible. Nevertheless, Brecher considers as well the difficulty of invoking Article 51 of the UN Charter when assessing if the effects of a cyberattack are significantly similar to the effects of an armed attack.[144]

For Abebe in "Cyberwar, International Politics, and Institutional Design", a clear definition of what comprises a cyber weapon, an act of war in cyber space or the use of force in cyber space is necessary, in order to invoke provisions under the UN Charter. Even in the case of invoking Article 51, attribution must still be addressed. Abebe also considers that international humanitarian law must be regarded along Article 51 because the principles of law in armed conflicts, such as proportionality, military necessity, distinction and avoidance of unnecessary suffering must be observed vis-à-vis the right of self-defence.[145]

The CCD COE Cyber Security Manual mentions there is agreement that cyber actions could be legitimate military activities. If a state faced a cyberattack that caused equal effects as a conventional military attack, the state could also resort to cyberattacks as a legitimate military response. Nevertheless, there is no agreement on the rules that should govern such situation.[146]

In this regard, the CCD COE manual points out a particular interpretation to be taken into account vis-à-vis the United Nations Charter, especially Article 2 on respecting territorial integrity of states and non-intervention in domestic affairs.[147] Cyberattacks go beyond territorial limits and can thwart this principle of international law. The manual also looks

[143] Hathaway, et. al, "The Law of Cyber-Attack", p. 844.
[144] Brecher, "Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations", p. 430, 431.
[145] Abebe, "Cyberwar, International Politics, and Institutional Design", p. 6.
[146] Klimburg, ed., "National Cyber Security Framework Manual", p. 18.
[147] United Nations Organization, "Charter of the United Nations", p. 6, 7.

at Article 39, which explains that any threat to peace or any act of aggression shall be determined by the UN Security Council.[148] Civil wars, degradation of elected leaders or large number of refugees that could destabilize a region are the threats to peace or acts of aggression identified by the Security Council. Nevertheless, the effects of cyberattacks could also fall into these categories under Article 39.[149]

At the UN General Assembly, Russia and China have proposed establishing a code of conduct for information security. However, it is worth noting that information security between East and West is understood differently. Whereas for western countries information security could be viewed as a means to protect free speech in cyberspace, Russia and China could see it as a means of control, in order to avoid the collapse of their political power.[150] Still, one must consider that it is also in the interest of western countries not just to develop measures to respond to cyberattacks, but also to build up the capacity to launch cyberattacks.[151] To this day, there is no international treaty that would regulate cyberattacks. The political context mentioned above might be a reason why there is no treaty for cybersecurity. However, one must not forget that the reality of cyberspace goes along with technological development, which evolves every day and this would quickly render any treaty out of date.[152]

In the absence of a universal-agreed-upon treaty for cybersecurity, there are international agreements that address cyberattacks, like the agreements described in the previous chapter. Additionally, it has already been mentioned that the UN Charter could provide guidance on how to respond to cyberattacks when the responsible is a state, but not when the responsible is an individual. Information security is still debated within the United Nations General Assembly (UNGA). Although UNGA resolutions have so far not required specific actions by member states, steps towards creating an international framework for information security have initiated. On 21 December 2001, the UNGA adopted Resolution 56/183 to support the holding of the World Summit on the Information Society (WSIS) in two phases. The summit's first phase took place in Geneva from 10 to 12 December 2003 and had the purpose of creating a political

[148] United Nations Organization, "Charter of the United Nations", p. 27.
[149] Klimburg, ed., "National Cyber Security Framework Manual", p. 169.
[150] Rid and Arquilla, "THINK AGAIN: CYBERWAR". p. 83, 84.
[151] Galeotti, "The cyber menace", p. 35.
[152] Hathaway, et. al, "The Law of Cyber-Attack", p. 859.

statement on the concrete steps to be taken for an inclusive Information Society. Member states, the private sector, NGOs, international organizations and the civil society participated in this first phase and supported two main outcome documents: The Geneva Declaration of Principles and the Geneva Plan of Action.[153]

Regarding cybersecurity issues, the Declaration of Principles emphasizes building confidence and security when using information and communication technologies (ICTs). According to this document, cooperation with international organizations and relevant stakeholders is necessary to promote a culture of cybersecurity worldwide. Enhancing security and protecting data, privacy, access and trade is considered part of this cybersecurity culture. Furthermore, this declaration points out to the need of preventing the use of ICTs for criminal and terrorist purposes, as well as the need of addressing cybersecurity matters both at a national and international level.[154] Likewise, the World Summit's Plan of Action explains the close collaboration between governments and the private sector to prevent, detect and respond to cybercrime and abuses in the use of ICTs. To achieve this, the Plan of Action suggests developing guidelines, adapt legislation for investigation and prosecution of malicious cyber activities and abuses of ICTs, providing mutual assistance, raising awareness and encouraging education.[155]

The second phase of the World Summit on the Information Society took place in Tunis from 16 to 18 November 2005. Its purpose was to set in motion the Geneva's Plan of Action, find solutions and reach agreements regarding Internet governance, financing mechanisms and the implementation of the Geneva and Tunis outcome documents. As a result of this second phase, the documents agreed upon were: The Tunis Commitment and the Tunis Agenda for the Information Society.[156] The latter of these two documents is the only one that refers to cyber issues. In this regard, the document reaffirms the necessity of fostering a culture of cybersecurity by means of international cooperation and the protection of personal data. At the same time, it reiterates the importance of prosecuting cybercrime, taking into account the effects it can have in more than one jurisdiction. Additionally, states should consider UNGA Resolutions 55/63 and 56/121 on "Combating

[153] International Telecommunication Union, "World Summit of the Information Society – About WSIS".
[154] International Telecommunication Union, "World Summit of the Information Society: Declaration of Principles - Building the Information Society: a global challenge in the new Millennium", p. 5.
[155] International Telecommunication Union, "World Summit of the Information Society: Plan of Action", p. 6.
[156] International Telecommunication Union, "World Summit of the Information Society – About WSIS".

the criminal misuse of information technologies" and the Council of Europe's "Convention on Cybercrime" when drafting or adapting legislation on the prosecution of cybercrime.[157]

Later on, in July 2010, cyber security specialists of fifteen countries including the United States, China and Russia recommended the UN Secretary-General to further dialogue on cybersecurity issues among states, build confidence and reduce risks regarding information security, as well as to agree upon cyber-related definitions and terms.[158]

The Council of Europe is perhaps the organization that has taken more concrete steps in regulating cybersecurity breaches, especially cybercrime. The 2001 Council of Europe's Cybercrime Convention establishes a common criminal policy for offenses related to the integrity of computer systems and access to data. All parties, including the United States, who ratified the Convention in 2006, have agreed to cooperate with investigations in terms of criminal offenses in computer systems.[159] The Convention, also known as the Budapest Convention, is the single legally binding international treaty on cybercrime. Its aim is to harmonize criminal legislation and it stipulates important actions to be taken in order to combat cybercrimes. Articles 23 to 34, for example, include specific considerations regarding the ideal level and type of international cooperation on cybercrime when designing cyber security policies.[160] Although it is a very important instrument, the document fails to explain the repercussions in case of a breach of the Convention.[161]

It can be said that international law, as an overarching norm of the international system, is shaping state's behaviours towards cybersecurity issues. The international scope of cyberattacks is pushing states to further consider exiting norms, such as the UN Charter and its Articles 2, 39 and 51. The right of self-defence could be invoked in the case the effects of a cyberattack are similar to those of an armed attack. Still, there are other considerations that are making states wary about invoking this right and are making them think about the appropriate actions to take when dealing with cyberattacks. Such

[157] International Telecommunication Union, "World Summit of the Information Society: Tunis Agenda for the Information Society", p. 7.
[158] Hathaway, et. al, "The Law of Cyber-Attack", p. 861.
[159] Hathaway, et. al, "The Law of Cyber-Attack", p. 863.
[160] Klimburg, ed., "National Cyber Security Framework Manual", p. 146, 177, 178.
[161] Hathaway, et. al, "The Law of Cyber-Attack", p. 864.

considerations include not just principles of law in armed conflicts, but also the rules that would govern such action. Such appropriate actions must be legitimate, must not violate the principle of non-intervention in domestic affairs and must respect territorial sovereignty according to Article 2 of the UN Charter.

With the guidance of these existing norms, states are trying to establish rules of behaviour or conduct within the cyber domain. The outcome documents of the conferences under the framework of the World Summit on the Information Society prove this reality. State's interactions in these fora are trying to elaborate and adapt institutions and states' approaches towards cybersecurity. The promotion of a culture of cybersecurity is the best example, since states themselves are fostering further collaboration with international organizations and set up mechanisms to build confidence in terms of data protection. Additionally, they are emphasizing the need of joint collaborations between the government and the private sector in this quest.

Even though the Budapest Convention of the Council of Europe does not address cyberattacks, it represents already a significant step for the regulation of cybercrime. This Convention is also a significant instrument because of its legally-binding nature that enshrines states' commitment to collaborate in investigations of criminal offences in computer systems. Such instrument is also shaping and adapting states' behaviour, as well as their appropriate approaches when dealing with cyberattacks.

Estonia's Cyber Security Strategy

Cybersecurity awareness in Estonia is achieved by addressing cyber issues at all educational levels and by extensive use of information media to maintain public awareness as well. The purpose is to inform the general public of risks in cyberspace and to prevent cybercrime. The government of Estonia is further working on strengthening the current law enforcement structure, to improve efficiency on detecting and prosecuting cybercrime. Furthermore, the resources at the disposal of the state will enable the development of national and military capabilities for cyber defence along with training, research and the exchange of best practices and solutions regarding cybersecurity.[162]

The Estonian National Defence Strategy has already identified the national institutions that have certain responsibilities regarding cyber issues. Additionally, the cybersecurity strategy establishes the Ministry of Economic Affairs and Communication to be the responsible body for directing and coordinating cybersecurity policies, as well as in implementing the cybersecurity strategy. Along with the Ministry of Defence, the Ministry of Interior and the Police and Border Guard Board, the Information Security Authority, the Ministry of Justice, the Government Office, the Ministry of Foreign Affairs, the Ministry of Education and Research, NGO's and businesses all take part and cooperate with the implementation and appraisal of this strategy.[163]

It can be said that these specific considerations of Estonia's Cyber Security Strategy are the ones that relate more to a constructivist view. The strategy reveals that the 2007 cyberattacks against Estonia had a strong influence in shaping the country's identity. This is seen with the several national institutions that have been assigned specific tasks related to the implementation of the cybersecurity strategy. In this regard, cybersecurity issues are seen as a crosscutting issue that is not only dealt by the Ministry of Defence, but also by others such as the Ministry of Foreign Affairs or the Ministry of Economic Affairs. Furthermore, the 2007 cyberattacks have been considered as a cornerstone example to raise awareness of the importance of cybersecurity issues. In this regard, the establishment of the CCD COE based in Tallinn can also be seen as part of this adapted identity of Estonia because now the Centre of Excellence and the country itself are seen as initiators and developers of knowledge and expertise related to cybersecurity matters.

Based on guidelines and international agreements, such as those from the World Summit on the Information Society, Estonia is adapting and shaping its legislation towards a closer public and private partnership, as well as steps towards addressing cybercrime issues. The Tunis Agenda for the Information Society explained previously, pointed out the necessity of having states properly prosecuting cybercrime and Estonia's Cyber

[162] Ministry of Economic Affairs and Communication of the Republic of Estonia, "2014–2017 Cyber Security Strategy", p. 9 – 11.
[163] Ministry of Economic Affairs and Communication of the Republic of Estonia, "2014–2017 Cyber Security Strategy", p. 13.

Security Strategy is following such recommendations. For this reason, partnerships between several governmental and non-governmental entities, as well as the private sector are important in implementing the strategy. At the same time, such collaboration is shaping Estonian institutions, as well as the reality of the country regarding cybersecurity issues.

United States' Department of Defence Cyber Strategy and International Strategy for Cyberspace

On a general perspective, the Cyber Strategy of the Department of Defence of the USA stresses as well the importance of having a close collaboration between the DoD and other national Departments and Agencies, local governments, the private sector and international partners. Its purpose is to promote global norms on responsible behaviour in cyberspace. In this regard, this cyber strategy supports information sharing and lessons-learned sharing, since it allows countries to significantly ameliorate their abilities to counter cyberattacks.[164]

The United States envisions international collaboration as a key feature to sustain an environment of innovation in cyberspace, where partnerships are crucial for establishing norms of behaviour that support the rule of law in cyberspace. To achieve this, the strategy explains there must be a shared responsibility at every level starting with the network's users all the way to nation states. Effective law enforcement, international norms of state behaviour in cyberspace, enhanced transparency, and information sharing between the government, private sector and the international community are some of the measures that could reduce risks in cyberspace at a global level. However, the challenge of effectively regulating cyberspace remains to this day and this strategy mentions that the USA will continue to work in building consensus to define what acceptable behaviour entails.[165]

[164] Department of Defense of the United States of America, "The DOD Cyber Strategy", p. 2, 3.
[165] Presidency of the United States of America, "International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World", p. 8, 9.

Furthermore, the international strategy for cyberspace details certain considerations that must be present when establishing regulations for cyberspace, these include:[166]

- States must respect, online and offline, fundamental freedoms of expression and association.
- States should respect intellectual property rights, trademarks and trade secrets.
- States must protect their citizens from unlawful interference with their privacy online.
- States must timely cooperate to identify and prosecute cybercriminals.
- States have the right of self-defence, as established in the United Nations Charter, which could be invoked when facing aggressive cyberattacks.
    - This point also reveals the USA's recognition of actually pursuing self-defence to respond to a cyberattack.
- States should ensure Internet access to all.
- States should ensure the free flow of information at a national level and with international interconnected networks.
- States should not deprive individual access to the Internet.
- States must build partnerships with relevant stakeholders for effective Internet governance.
- States should be aware of their responsibility to protect information networks and to secure infrastructures from misuse and damage.

The international strategy for cyberspace considers dissuasion and deterrence as part of the defence objective of the United States. Dissuasion comprises a national and an international component. The national aspect entails that the USA works towards effective risk mitigation and incident response, as well as the adoption of sound practices regarding information technology. Information sharing among public, private and other relevant stakeholders has been further strengthened to enhance computer security. Within the international context, it seeks to improve and generate response capabilities to enhance defence of computer networks on a global scale. On the other hand, deterrence on the domestic level requires having processes in place that allow for the investigation and prosecution of those who compromise networks. At the international level, deterrence

[166] Presidency of the United States of America, "International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World", p. 10.

aims at harmonizing procedures that allow for the rule of law and prosecution of attacks/crimes committed in cyberspace. In this regard, self-defence is particularly emphasized, for the USA also recognizes that certain aggressions in cyberspace could result from actions required or taken to comply with obligations the country has under military agreements.[167]

The description above of the USA's Cyber Strategy, as well as of the International Strategy for Cyberspace contains elements that refer to a constructivist view, especially in terms of proposals for establishing norms and rules of behaviour in cyberspace. The DoD Cyber Strategy explains very generally that sharing information and lessons learned with local and international institutions can improve and benefit each other's abilities to counter cyberattacks. Thus, the USA is adapting its cyber identity in terms of what the country's institutions learn about cyberattacks. Operation Buckshot Yankee was a learning experience because its aftermath led to the creation of USCYBERCOM as a unit designed to protect computers and communication systems of the military. Additionally, the USA is also pushing for constructing norms at an international level, so to have a common ground for addressing and dealing with cybersecurity issues.

On the other hand, the International Strategy for Cyberspace explains in further detail the importance of setting up international norms for cyberspace. In this regard, these attempts of furthering interactions to shape norms and behaviours are present especially when the strategy points out the USA will foster consensus-building to define rules of acceptable behaviour in the cyber domain. Furthermore, establishing these norms are not regarded just as a one-sided involvement from states, but partnership between governments, the private sector and international organizations is crucial for establishing such norms of behaviour. The strategy takes a step further by already defining certain regulations that should be taken into account in the process of establishing norms of behaviour in cyberspace. These proposed regulations make reference not just to the respect of fundamental freedoms, a norm all countries are expected to comply with, but also on the protection of unlawful information interference, the protection of networks and the free flow of information.

[167] Presidency of the United States of America, "International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World", p. 13, 14.

Unlike the strategies in Estonia, the USA’s International Strategy for Cyber Space explicitly mentions the right to self-defence as part of the tools available for dealing with cyberattacks and cybercrimes. In this regard, it can also be said that the USA is not just supporting establishing norms of behaviour and agreed upon processes that would allow for the prosecution of crimes committed in cyberspace, but it is also calling upon Article 51 of the UN Charter. As discussed previously, the rules that should govern the right for self-defence in the case of a cyberattack are still debated. As a consequence, the USA has also shaped its policies based on the threats cyberattacks can pose to the country. The USA is not discarding the possibility of resorting to self-defence. It will invoke such right not just in the case a cyberattack has effects equal to those of a conventional armed attack, but also when attacks in the cyber domain may need actions to fulfil obligations the USA has under military agreements.

Hypothesis’ validation

Based on the aforementioned paragraphs, the hypothesis proposed for this chapter holds true for Estonia and for the United States. Both states have been trying to adopt an appropriate behaviour with respect to cyberattacks. Thus far, an appropriate behaviour has entailed that each country has been complying with principles of international law. That is the reason why discussions around the possibility of having a military response to a cyberattack have always been put in the context of regarding the principles of law in armed conflicts, as well as of Article 2 of the UN Charter on respecting territorial integrity.

Additionally, in the quest of defining appropriate responses to cyberattacks, partnerships between the government, the private sector and international organizations are needed to collaboratively come up with norms and rules of conduct and of acceptable behaviour in cyberspace. International agreements on the protection of information networks and advancements towards establishing processes for investigating and prosecuting crimes in cyberspace also reveal how such agreements are making states adapt their legislation. At the same time, legislation on cybersecurity is shaping the countries’ national institutions, so that they can address cyber issues and can cooperate in the fight against cybercrimes. Even though the World Summit on the Information Society and the Council of Europe’s

Convention on cybercrime particularly refer to crimes in cyberspace, they definitely represent a first step in establishing processes, which can eventually allow for the definition of norms and procedures to deal with cyberattacks in the future.

By abiding to the existing international norms, Estonia and the United States as well as other countries, are adapting and shaping their institutions and norms. This means they are willing to keep up with current cybersecurity developments and want to develop the procedures that would allow them to eventually go beyond than just defending themselves from a cyberattack, but actually responding to it. These international norms are shaping the identities of the states in terms of cybersecurity issues. For Estonia, its identity after the 2007 cyberattacks focused on defending the country from future cyberattacks and on building up partnerships among several governmental institutions and the private sector, while cooperating with the international community. For the United States, its identity in terms of cybersecurity issues has also been shaped by cyberattacks. In the case of the 2008 Operation Buckshot Yankee, it can be seen how after the cyberattack the USA focused on developing a new institution, the USCYBERCOM, and on strengthening policies to defend the country from cyberattacks. Furthermore, it can also be said that the right to self-defence has also shaped USA's policies because of the several references made to it. Especially in the International Strategy for Cyber Space, self-defence is seen as a tool at the disposal of the USA and which will be invoked if required when facing an aggression in cyberspace.

CHAPTER FIVE: CONCLUSIONS

Based on the explanations and descriptions of the previous chapters, cybersecurity represents a cross-cutting domain. It does not only have an impact in the military and information technology sphere, but it also affects the economic, political, social and cultural environment of a country. Cybersecurity is an area that is constantly developing and for this reason it is not yet possible to have a unique theoretical framework to address attacks in cyberspace, nor to have universally agreed upon concepts regarding malicious activities in this domain.

The validation of the three hypotheses proposed for this research reveals that a theory for cybersecurity and specially for understanding what the responses of a state to a cyberattack are must take into account elements of mainstream IR theories. Because of the cross-cutting nature of a cyberattack, a state responds to it by a combination of a realist, liberal and constructivist approach. In other words, this is a combination of: (1) improving defensive capabilities when the state perceives its security is threatened by a cyberattack, (2) a closer collaboration with international organization when the state's cybersecurity interests depend on global networks, and (3) abiding by identity-constructing norms when the state adopts an appropriate behaviour towards cyberattacks.

The technical aspect of dealing with a cyberattack must not be neglected. Both case-studies demonstrate that information technology skills were required to respond to the attack at an early stage because the infection or intrusion of the malware was taking place in information networks and systems. The technical response in combination with elements of mainstream IR theories shows that states' responses to cyberattacks involve: (1) having the military much more involved in cybersecurity issues while developing the mechanisms and procedures to improve defensive capabilities, (2) collaborating closer with international institutions in terms of security interests that depend on global networks, and (3) adhering to constructing and internationally agreed upon norms by adopting and aiming at establishing appropriate rules of behaviour and codes of conduct towards cyberattacks.

Cybersecurity works under certain assumptions worth mentioning. First, cyberattacks and the means to respond to such attacks have been developed in an information technology and wired world. Second, defining a response to cyberattacks displays the plurality of actors in the cyber domain. Even though states remain the most important actors in the international system, it must be regarded that media outlets, banks, the military, information experts and individuals play a role in this domain, too. At the same time, all actors result affected to a certain degree because of interconnected networks and the fast spread of information circulating through them. Third, there exists a plurality of cyber threats, which range from cybercrimes and acts of espionage, to cyberattacks and eventually in the future cyberterrorism and cyberwarfare. To this day, an attack can be attributed when and if the perpetrator claims responsibility for the attacks, but since this happens on counted occasions, attribution remains a challenge. A hundred percent certainty of attribution is not possible, yet. However, technology is improving and the recognition of the applicability of international law in cyberspace, confidence building measures and attempts towards establishing rules of behaviour in cyberspace represent steps forward in terms of regulating cyberspace and solving the attribution challenge.

Cyberattacks are gaining ever-increasing importance in the international arena because of the threats they pose to international security. A cyberattack represents a threat because: (1) the uncertainty of the type and purpose of the attack, (2) complex responses that can be involved to deal with an attack, (3) the actual consequences (stolen information, physical damage or death) of a potential attack. These considerations bring consequences to international security. For instance, the threat/attack can have similar effects to those caused by a conventional armed attack and/or it can target infrastructures and networks that are necessary either for the functioning of the state or for the welfare of the state and its population. Furthermore, the possibility of states resorting to cyberattacks is no longer neglected, especially for the attractive benefits states would have when using them. The anonymity that interconnected networks allows is desirable for states that are willing to gain an advantage over a country they do not like. This can be done without the risk of being identified because final attribution is complex. States want this advantage because they would be able to further their national interests.

If we look at the example of the cyberattack to Sony mentioned at the beginning of this thesis, the announcement of the ongoing investigations by the FBI at the time of the attack and of the possibility of retaliating those responsible for the attack shows that the statement itself served as an effective response to diminish the attack. If we turn to the case-studies, they reveal that an effective response to a cyberattack has not been the result of already-established measures and procedures, but on an immediate identification of the behaviour of the attack and on finding a mechanism to defend the country from it. Neither the 2007 cyberattacks against the government of Estonia nor the 2008 cyberattack against the USA's military systems involved a counter reaction or counterattack to combat the cyberattack. Both countries relied on information technology solutions: improving firewalls, making encryption stronger and installing security packages in the case of Estonia; and designing a program that could doze off the malware in the case of the USA. This shows that to this day responses to cyberattacks, of those whose information has been disclosed by its governments, have been relying primarily on information and communication technologies.

Another important consideration is that only after each state came up with a mechanism to defend itself from the cyberattack is that legislation on cybersecurity was drafted. This means that the reaction of the state to the attack set the foundations for identifying the governmental bodies in charge of defending the country from cyberattacks, and of coming up with effective ways to respond to them.

In the case of Estonia, the country had by 2010 its National Security Concept with references to cybersecurity and the prevention of cybercrime, where the protection of information and communication systems is a security consideration. This document has been complemented with the arrangements set up in the 2011 National Defence Strategy, where a gear assembly of governmental bodies is envisaged. Here, even though the Ministry of Defence is the responsible entity for cyber defence, it is not alone and the success of cyber defence depends also on a close collaboration with other bodies. This includes the Ministry of Interior, in charge of establishing the procedures for classifying information, the Police and Border Guard, in charge of anticipating and preventing cyberattacks, and the Ministry of Economics, which assures the correct functioning of communication networks that are essential for national defence. The National Defence Strategy clearly shows the cross-cutting nature of cybersecurity because both the military and civilian institutions must synchronize their work to combat cyberattacks, while at the same time maintain their institutional independence. Moreover, the 2014 Cybersecurity Strategy reinforces the need of integrating civilian and military resources to prevent and deter cyberattacks, as well as developing military capabilities for cyber defence. Then again, we see the current importance placed on defence rather than offence.

When looking at the United States' legislation on cybersecurity, we also see that cybersecurity considerations where further incorporated after the 2008 cyberattack. The 2011 International Strategy for Cyberspace shows a gear assembly between cybersecurity considerations and strategic areas for the USA government such as the economy, networks, law enforcement, military, internet governance, international development and internet freedom. This document is also explicit in terms of self-defence because it clearly points out that the USA will resort to this mechanism to respond to cyberattacks. Additionally, in the case of the USA, the country places much more importance on the military to respond to cyberattacks. The 2015 National Security Strategy clearly indicates that the military must remain ready to deter and defeat cyberattacks, whereas the country as such is ready to attack and retaliate against cyber attackers. Although, it does not say how it will do so, such action remains unclear because no mechanism for effective attribution is outlined in this strategy. The military readiness is complemented with the 2015 Cyber Strategy from the Department of Defence, where it is mentioned that the DoD is the responsible entity for defending the country from cyberattacks. It is interesting to note that the task of defending the country from a cyberattack is not limited to defensive activities, since the DoD is also in charge of providing cyber capabilities to support military operations. The USA even considers the possibility of disrupting an adversary's infrastructure in the case it threatens USA's interests. Thus, an offensive capacity of the USA in cyberspace, in addition to the defensive capacity, will be gaining importance, as well.

Interestingly, the legislation in both countries, Estonia and the United States, outlines the government bodies in charge of responding to cyberattacks. However, it does not outline concrete measures and steps to respond to them. This is mainly because of the attribution challenge, which is still unsolved and which is also the reason why a set of rules to respond to cyberattacks has not been established. The case-studies reveal that in order to respond to cyberattacks, states had to analyse and identify the nature of the attack on the spot. Unlike a nuclear weapon, whose nature, effects and consequences of a nuclear attack are the same regardless where the nuclear weapon has been detonated from, the effects of the cyberattack are unpredictable because of the nature of the attack and because its effects are unknown and become known only after being analysed. There cannot be a standardization of cyberattacks yet and the attacks in Estonia and in the USA confirm this fact. In Estonia, the attack consisted on flooding the networks with junk emails and defacing web sites, which were countered by improving firewalls and contacting CERTs in other countries and together blocked the outsider attacks. In the USA, the attack consisted in stealing documents and attempting to send them back to the malware's maker. But the nature of these attacks was known only after the attack started and only after experts analysed what the attack sought to do and how. Beforehand, it was not possible to know what the attack was going to do.

Thus, for the time being, states respond to cyberattacks by coming up with an information technology solution that would allow the country to defend itself from the attack. To this day, no counter attack or retaliation measures are possible to respond to a cyberattack as long as the attribution challenge has not been solved. The cyberattacks in Estonia and in the USA further show two important considerations: (1) that internal collaboration among national entities, like in Operation Buckshot Yankee, is crucial for responding to a cyberattack, and (2) that international collaboration, like in the attacks against the government of Estonia, provides additional tools and inputs for responding to a cyberattack.

Based on these experiences and on the challenge of attribution, a general procedure that could be adopted for responding to cyberattacks includes the next four steps: (1) taking measures to trace back and finding out the origin of the attack as accurately as possible. When the attribution challenge is solved, detecting the origin of the attack will be much faster. (2) Determining the type of attack and the structure it has, (3) identifying the purpose of the attack i.e. identifying what the attack is seeking to obtain or cause, and (4) establishing the entity responsible for responding to the attack.

Thus far, a response to a cyberattack involves a technical aspect, which is a combination of developing an information and communication technology solution and information-sharing among countries. However, the implications behind the mere technicality of the response must also be taken into account. In terms of power, states will defend themselves from cyberattacks as they would defend themselves from any other threat. A cyberattack poses a threat to a state's share of power because the cyberattack can undermine a state’s institutions, as seen in Estonia. Under this situation, states are not willing to cede any of its power-share to any other country in the international community and to keep their share of power they will resort to defending themselves. For the time being, emphasis has been put into defence rather than offence. Thus, the strategic response of states to cyberattacks is not just to protect and defend the country, but to keep the status quo of the international system by improving their defensive capabilities, collaborating closely with international organizations and complying with international norms.

Nevertheless, defence will not be enough for states to maintain their share of power in the international system. As technology evolves and further collaboration and information-sharing among countries develop, it would be much easier for all states to reinforce their networks and set up the necessary mechanisms to anticipate and defend their networks from a cyberattack. Moreover, with technology developments it would become much easier for states, non-state actors and individuals to conduct offensive cyberattacks because their defensive infrastructures would already be strong enough to resist and counteract a cyberattack. In that case, cyberattacks could become a status quo changer, especially between powerful and less powerful states, because those countries that have highly developed defensive and offensive cyber capabilities will be able to conduct cyberattacks against those countries who might not possess offensive capabilities at all and whose defensive capabilities are not as strong as those of the state conducting the attack. On the other hand, cyberattacks could still be seen as keepers of the status quo because the development of defensive and offensive capabilities could strengthen deterrence among powerful states. In this case, powerful states will become much more aware of other powerful states’ capabilities in cyberspace. Therefore, they would think twice before cyberattacking another powerful country because, as they are aware of the cyber capabilities of the counterpart, this also raises the possibility of being retaliated against the cyberattack. In this regard, once defensive capabilities have been improved and strengthened, states must also focus in developing their offensive capabilities because eventually defence alone will not be enough for a state to keep its share of power.

Influencing international developments can also be seen as another strategic response to a cyberattack. The 2007 cyberattacks against Estonia raised worldwide awareness about cybersecurity issues and prompted other states to start addressing cyber issues at a country level and developing national cyber security strategies. In this regard, a not so powerful and small country like Estonia became a leading player and reference to other countries in the development of cyber security strategies. Since the 2007 attacks were viewed as the first of its kind, it can be said that Estonia used its response to the cyberattack to leverage its position regarding cybersecurity. Thus, the establishment of the Cooperative Cyber Defence Centre of Excellence in Tallinn and of the EU Agency for large-scale IT systems could be seen as this attempt to leverage Estonia's international position not only by developing expertise in cybersecurity issues, but also by collaborating closely with international institutions such as NATO.

In the case of the United States, as a powerful country, it has always been present in all international developments. However, Operation Buckshot Yankee has strengthened the USA's position not just to influence international dialogue on the need of defending the country from cyberattacks, but it has also influenced in other areas many countries have not thought of, such as trade and commercial secrets. In this case, the USA made use of the 2008 cyberattack not just to call upon on the need of improving defensive capabilities, but also on the need of going beyond defence and incorporating other topics to the cybersecurity agenda. Thus, influencing discussions related to cybersecurity issues in the aftermath of a cyberattack can be seen as a strategic response to a cyberattack as well.

Some cybersecurity aspects are recommended to be developed further. Despite the fact that international law applies in cyberspace and for that matter that the UN Charter applies, since it enshrines the principles of international law, discussions around legally binding regulations other than international law should be further discussed. This is necessary, in order to advance not only concepts and definitions such as cyber weapons or cyber war, but also to define the framework that would allow for effective attribution. This would set the foundations for eventually determining the types of punishments or retaliations against a cyberattack, whose origin could then be known.

Partnerships between governments and the private sector have proven to be effective when it comes to information-sharing and in identifying common strategies to respond to cyberattacks. The aforementioned case-studies reflect such exercise. They show that a broader collaboration in terms of sharing what states did, in order to respond to similar or other cyberattacks can provide further inputs not only to strengthen the defence from attacks, but eventually to come up with offensive measures to respond to them. However, information-sharing to come up with better responses to cyberattacks entails that governments would have to decide which information has to be disclosed. Most cases of cyberattacks are kept as national security secrets and in order to have a more collaboratively cybersecurity agenda within the international community, countries could strengthen information-sharing by disclosing information related to cyberattacks. Later on, this could evolve into a mechanism to effectively attribute cyberattacks because more knowledge would exist on the nature of the attacks and on the ways to identify the person, entity, or government behind them. Effective attribution would be much more precise and faster in the future because such collaboration among countries would allow for identifying the perpetrator of an attack. Information sharing among countries and greater technological advancements would remove the obstacles in solving the attribution challenge and would lead to effective deterrence in cyberspace.

Cybersecurity considerations will evolve along with technological advancements. To this day, not all information regarding cyberattacks has been disclosed because it is considered a matter of internal security in many countries. The possibility of having states, non-state actors and individuals conducting cyberattacks is real. But because of undisclosed information and the attribution challenge, it is not possible to know exactly whether terrorist groups or individuals have been responsible for conducting cyberattacks against other states or other non-state actors. For the time being, stability in the international system is reflected by the existent balance of power among states and their attempts in improving their defensive capabilities against cyberattacks. However, and as mentioned before, defence is not enough and developing strong offensive capabilities will become as important as having strong defensive capabilities. Offensive capabilities will be possible to develop not just with technology, but also with the cooperation and information-sharing among countries, both of which would also facilitate solving the attribution challenge. By that time in the future, the balance between defence and offense would allow for effective deterrence because countries would be aware of each other's cyber capabilities, as well as of the consequences of engaging in a cyberattack. Thus, a model that would allow for stability in the international community includes a system where technological developments, political cooperation among countries and international institutions, and adherence to norms would allow for the development of both defensive and offensive capabilities in such a way that deterrence is effective and peace within the cyber domain could be assured.

BIBLIOGRAPHY

Abebe, Daniel. “Cyberwar, International Politics, and Institutional Design”. The University of Chicago Law Review. The University of Chicago Law Review. Vol. 83. No. 1 (Winter 2016).

Brecher, Aaron P. “Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations”. The Michigan Law Review Association. Vol. 111. No. 3 (December 2012).

Brenner, Susan W. “At light speed: Attribution and response to cybercrime/terrorism/warfare”. Northwestern University School of Law. The Journal of Criminal Law and Criminology. Vol. 97. No. 2 (Winter 2007).

Cerf, Vinton G. “Safety in Cyberspace”. The MIT Press on behalf of American Academy of Arts & Sciences. Daedalus. Vol. 140. No. 4. Protecting the Internet as a Public Commons (Fall 2011).

Collier, David. “The Comparative Method”. In Ada W. Finifter, ed. 1993. Political Science: The State of the Discipline II. Washington D.C.: American Political Science Association. http://polisci.berkeley.edu/sites/default/files/people/u3827/APSA-TheComparativeMethod.pdf.

Department of Defense of the United States of America. “The DOD Cyber Strategy”. 2015. Accessed: April 10, 2017. http://www.dtic.mil/doctrine/doctrine/other/DoD_cyber_2015.pdf.

Dunne, Tim; Kurki, Milja; and Smith, Steve. *International Relations Theories – Discipline and Diversity*. Oxford University Press. 2007.

Eriksson, Johan; and Giacomello, Giampiero. “The Information Revolution, Security, and International Relations: (IR) Relevant Theory?”. Sage Publications, Ltd. International Political Science Review. Vol. 27. No. 3 (Jul., 2006).

European Commission Press Release Database. “European Commission - Fact Sheet: Directive on Security of Network and Information Systems”. Brussels. 6 July 2016. Accessed: April 17, 2017. http://europa.eu/rapid/press-release_MEMO-16-2422_en.htm.

Galeotti, Mark. “The cyber menace”. Royal Institute of International Affairs. The World Today. Vol. 68. No. 7 (December 2012 & January 2013).

Hansen, Lene; and Nissenbaum, Helen. “Digital Disaster, Cyber Security, and the Copenhagen School”. Wiley on behalf of The International Studies Association. International Studies Quarterly. Vol. 53. No. 4 (Dec., 2009).

Harknett, Richard J. “Integrated Security: A Strategic Response to Anonymity and the Problem of the Few”. Contemporary Security Policy. 24. No.1 (April 2003).

Harknett, Richard J. “Leaving Deterrence Behind: Warfighting and National Cybersecurity”. Journal of Homeland Security and Emergency Management. Vol. 7. Art. 1 (Spring 2010).

Harknett, RJ; and Goldman, EO. “The Search for Cyber Fundamentals”. Journal of Information Warfare. 15, 2 (2016).

Harknett, Richard J., and Stever, James A. “The New Policy World of Cybersecurity”. Wiley on behalf of the American Society for Public Administration. Public Administration Review. Vol. 71. No. 3 (May | June 2011).

Hathaway, Oona A. Et. al, “The Law of Cyber-Attack”. California Law Review. Inc. Vol. 100. No. 4 (August 2012).

Hayes, Jarrod. “Securitization, Social Identity, and Democratic Security: Nixon, India, and the Ties That Bind”. Cambridge University Press on behalf of the International Organization Foundation. International Organization. Vol. 66. No. 1 (Winter 2012).

Infosecurity Magazine. “Worm that wreaked havoc for US Military likely a progenitor of Red October”. 12 March 2014. Accessed: April 12, 2017. https://www.infosecurity-magazine.com/news/worm-that-wreaked-havoc-for-us-military-likely-a/.

International Telecommunication Union. “World Summit of the Information Society – About WSIS”. Accessed: April 14, 2017. http://www.itu.int/net/wsis/basic/about.html.

International Telecommunication Union. “World Summit of the Information Society: Declaration of Principles - Building the Information Society: a global challenge in the new Millennium”. Geneva, 12 December 2003. Accessed: April 14, 2017. https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf.

International Telecommunication Union. “World Summit of the Information Society: Plan of Action”. Geneva, 12 December 2003. Accessed: April 14, 2017. https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-E.pdf.

International Telecommunication Union. “World Summit of the Information Society: Tunis Agenda for the Information Society”. Tunis, 18 November 2005. Accessed: April 14, 2017. http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.pdf.

Kello, Lucas. “The Meaning of the Cyber Revolution”. International Security. 38, 2, (Fall 2013).

Klimburg, Alexander. Ed. “National Cyber Security Framework Manual”. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn 2012.

Knowlton, Brian. “Military Computer Attack Confirmed”. New York Times. August 25, 2010. Accessed: April 12, 2017. http://www.nytimes.com/2010/08/26/technology/26cyber.html.

Lindsay, Jon R. “Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack”. Journal of Cybersecurity. 1(1). 2015.

López, Juan J. “Theory Choice in Comparative Social Inquiry”. The University of Chicago Press. Polity, Vol. 25, No. 2 (Winter, 1992).

Lynn William J. III. “Defending a New Domain: The Pentagon's Cyberstrategy”. Council on Foreign Relations. Foreign Affairs. Vol. 89. No. 5 (September/October 2010).

Ministry of Defense of the Republic of Estonia. “National Defense Strategy, Estonia”. 2011. Accessed: April 5, 2007. http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf.

Ministry of Defense of the Republic of Estonia. “National Security Concept of Estonia”. 2010. Accessed: April 5, 2017. http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia_0.pdf.

Ministry of Economic Affairs and Communication of the Republic of Estonia. “2014–2017 Cyber Security Strategy”. 2014. Accessed: April 5, 2017. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

Nakashima, Ellen. “Cyber-intruder sparks massive federal response – and debate over dealing with threats”. The Washington Post. December 8, 2011. Accessed: April 12, 2017. https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_print.html.

Nakashima, Ellen. “Defence official discloses cyberattack”. The Washington Post. August 24, 2010. Accessed: April 12, 2017. http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html.

NATO. “Cyber defence”. Last updated: 17 February 2017. Accessed: April 17, 2017. http://www.nato.int/cps/en/natohq/topics_78170.htm.

NATO. “NATO and the European Union enhance cyber defence cooperation”. 10 February 2016. Accessed: April 17, 2017. http://www.nato.int/cps/en/natohq/news_127836.htm.

NATO. “NATO Cyber Defence Fact Sheet”. July 2016. Accessed: April 17, 2017. http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf.

NATO. “NATO Summit Updates Cyber Defence Policy”. 24 October 2014. Accessed: April 17, 2014. https://ccdcoe.org/nato-summit-updates-cyber-defence-policy.html.

NATO. “The North Atlantic Treaty (1949)”. Accessed: April 11, 2017. http://www.nato.int/nato_static/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf.

Nye, Joseph S. Jr. *The Future of Power*. Public Affairs. New York. 2011.

Presidency of the United States of America. “International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World”. 2011. Accessed: April 9, 2017. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Presidency of the United States of America. “National Security Strategy”. February 2015. Accessed: April 8, 2017. https://ccdcoe.org/sites/default/files/strategy/USA_NSS2015.pdf.

Quackenbush, Stephen L. “Deterrence theory: where do we stand?”. Cambridge University Press. Review of International Studies. Vol. 37. No. 2 (April 2011).

Rid, Thomas; and Arquilla, John. “THINK AGAIN: CYBERWAR”. Washington Post. Newsweek Interactive. LLC. Foreign Policy. No. 192 (March / April 2012).

Schmidt, Andreas. “The Estonian Cyberattacks”. Delft University of Technology. January, 2013. Chapter prepared for the edited book *The fierce domain – conflicts in cyberspace 1986-2012*, edited by Jason Healey, Washington, D.C.: Atlantic Council, 2013. Accessed: June 9, 2017. https://www.researchgate.net/publication/264418820.

Schmitt, Michael N. Ed. *Tallinn Manual on the International Law applicable to Cyber Warfare.* Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge University Press. 2013.

Shachtman, Noah. “Insiders doubt 2008 Pentagon hack was foreign spy attack (updated)”. August 25, 2010. Accessed: April 13, 2017. https://www.wired.com/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/.

Shakarian, Paulo; Shakarian, Jana; and Ruef, Andrew. *Introduction to Cyberwarfare - A Multidisciplinary Approach*. Elsevier. Inc. 2013.

Sterling-Folker, Jennifer. “Competing Paradigms or Birds of a Feather? Constructivism and Neoliberal Institutionalism Compared”. Wiley on behalf of The International Studies Association. International Studies Quarterly. Vol. 44. No. 1 (Mar., 2000).

Taliaferro, Jeffrey W. “Security Seeking under Anarchy: Defensive Realism Revisited”. The MIT Press. International Security. Vol. 25. No. 3 (Winter, 2000-2001).

The Organization for Security and Cooperation in Europe (OSCE). “Confidence building measures to enhance cybersecurity in focus at OSCE meeting in Vienna”. 7 November 2014. Accessed: April 14, 2017. http://www.osce.org/cio/126475.

The Organization for Security and Cooperation in Europe (OSCE). “Decision No. 1106 - Initial set of OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies”. 3 December 2013. Accessed: April 14, 2017. http://www.osce.org/pc/109168?download=true.

The Organization for Security and Cooperation in Europe (OSCE). “OSCE milestones in cyber/ICT”. Accessed: April 14, 2017. http://www.osce.org/cio/299291?download=true.

United Nations Organization. “Charter of the United Nations”. Department of Public Information. New York.

Zetter, Kim. “The return of the worm that ate the Pentagon”. Wired Magazine. December 9, 2011. Accessed: April 13, 2017. https://www.wired.com/2011/12/worm-pentagon/.

Pledge of Honesty

On my honor as a student of the Diplomatic Academy of Vienna, I submit this work in good faith and pledge that I have neither given nor received unauthorized assistance on it.

Maria Jose Alvear Larenas