NOVAFCSH
FACULDADE DE CIÊNCIAS SOCIAIS E HUMANAS
UNIVERSIDADE NOVA DE LISBOA

Cyberterrorism as Hybrid Threat: a comparison between the Iranian and Estonian case

Natália Gagliardi de Freitas

Mestrado em Ciência Política e Relações Internacionais

Especialização em Relações Internacionais

dezembro, 2022

Dissertação apresentada para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Ciência Política e Relações Internacionais, especialidade em Relações Internacionais, realizada sob a orientação científica da Professora Doutora Teresa Ferreira Rodrigues e do coorientador Comandante Helder Manuel Fialho de Jesus.

Acknowledgments

I am writing this with my heart filled with gratitude to finally be able to say, “I have finished my thesis.” However, this was only possible because some people were there for me when I needed them, so these few words are for them.

Without my parents, I would not have been able to cross the Atlantic and come to this country. I wouldn’t be able to tolerate all the obstacles and challenges I had to face. If it were not for you, I wouldn't be now, concluding a cycle of my life, and I wouldn’t be fulfilling another dream. I am so thankful for everything you have done during my whole life, for teaching me not to give up, to be determined, to work hard to achieve my goals, and to have empathy. This thesis is yours, and I hope to make you even prouder in the future. I love you.

To my grandparents and the rest of my family, that has supported me all the way, giving me strength and reassuring me I was in the right place, doing exactly what I needed to be doing. All of you were essential to make me strong and brave, and sharing nice words when I was facing many doubts.

To my love Francesco, that have supported me every step of the way. You were there for me when I most needed you and didn’t let me give up. You were my home on this continent. You were laughter, smiles, adventures, hugs, comfort, and affection during these two years of my master's degree. I couldn’t have asked someone more supportive and positive, and I thank the universe for meeting you. I love you.

To all my dear friends all over the world, who have sent me so many messages of support and affection during these last challenging moments. Thank you for being present, even if sometimes distant. Thank you for believing in me, even before I have. Thank you for dreaming with me and saying, yes, you can do it.

To my dear colleagues and manager, who have shown so much support and for being so understanding during these last few months. You have proved to me I am in the right place with the right people. Thank you all so much.

Last but not least, to my dear and cherished advisors, Professor Teresa and Captan Helder, I would not have been able to find the motivation and right words to write this thesis without you. I am very grateful for all the help and orientation you gave me and all the empathy during these months. Thank you.

Ciberterrorismo Como Uma Ameaça Híbrida: uma comparação entre os casos iraniano e estoniano

Natália Gagliardi de Freitas

Resumo

PALAVRAS-CHAVE: Terrorismo Cibernético, Ameaças Híbridas, OTAN, Estónia, Irão, Stuxnet

Este trabalho de dissertação de mestrado pretende estudar o terrorismo cibernético no campo dos estudos de segurança e como se apresenta como uma ameaça híbrida na sociedade de hoje, no sistema internacional, e os seus impactos dentro destas fronteiras. Pretende abordar através de uma perspectiva institucionalista como os Estados entendem esta ameaça, que definições têm sobre este assunto, que efeitos este tipo de ameaça causa nas suas sociedades, e que meios de contra-resposta estes actores têm à sua disposição para garantir contra o ciber-terrorismo. Visa, também, expor as várias opiniões que o conceito carrega, como as suas definições e interpretações, e apresentar a conjuntura em que está inserido. A partir daí, os casos da Estónia e do Irão serão apresentados para desenvolver uma análise para compreender se existe uma diferença na resposta de dois Estados com contextos diferentes - um que é membro da OTAN e outro que não é - e como isto se apresenta na forma como abordam a questão, como reagem e como se protegem da mesma. No final, as diferenças e as razões que foram interpretadas serão apresentadas, assim como os possíveis resultados da questão da investigação.

Cyberterrorism as Hybrid Threat: a comparison between the Iranian and Estonian case

Natália Gagliardi de Freitas

Abstract

KEYWORDS: Cyberterrorism, Hybrid Threats, NATO, Estonia, Iran, Stuxnet

This thesis project intends to study cyber-terrorism within the field of security studies and how it presents itself as a hybrid threat in today's society, in the international system, and its impacts within these boundaries. It is intended to approach through an institutionalist perspective how states understand this threat, what definitions they hold on this subject, what effects this type of threat causes within their societies, and what means of counter-response these actors have at their disposal to ensure against cyber-terrorism. It aims, as well, to expose the various opinions that the concept carries, as its definitions and interpretations, and present the conjuncture that it is inserted. From there, the cases of Estonia and Iran will be presented to develop an analysis to understand if there is a difference in the response of two states with different contexts - one that is a NATO member and one that is not - and how this presents itself in how they approach the issue, how they react and how they protect themselves from it. In the end, the differences and the reasons that have been interpreted will be presented, as well as possible results of the research question.

Summary

Introduction

It is no longer something new to hear about society's various developments since the world has become more technological. For some years, the multiple consequences of this new reality have been debated, as how this has negatively impacted human beings and their routine. Obviously, along with technology also came many advances, which also provided more security, life expectancy, and convenience, and helped mankind to achieve goals previously existing only in dreams or Hollywood movies.

The creation of the Internet, following this technological development, culminated in the appearance of the cyber world. At the beginning of its history, it was a place that was not yet fully comprehended, and man did not consider the possible consequences of living so much online. In the late years of the 20th century and early years of the 21st, it became common to hear more about hacking, data theft, and attacks happening within the cyber world. The private and public world was increasingly dependent on the Internet, and it was not yet understood the extent of these attacks and how they could impact businesses, governments, and citizens.

Soon it became clear that cyberspace could be used as a stage for threats that many players in the international system could not imagine. New words and concepts involving the cyber world have started to become popular, drawing the attention of scholars to the problem. In the first instance, some study centers in the United States and some international organizations began to research and analyze what these new concepts circulating in the press and society were all about. Attacks within cyber started to increase, some larger than others, leading to the appearance of the word "cyber-attacks" and, consequently, cyberterrorism.

Similar to following in the footsteps of its predecessor ‘terrorism’, the term cyberterrorism also encountered difficulties regarding a single definition. There have been many attempts by scholars and government organizations to find one definition of cyberterrorism, yet, there has not been one that all actors agree on regarding the meaning, examples, descriptions, and counterparts. Still, even though there is not one true definition, many of those actors in International Relations have put effort into describing their understanding of the term as accurately and detailed as possible and introducing better semantic precision to it. (WEIMANN, 2004)

Within this contextualization, this thesis intends to study, within the field of security studies, cyber-terrorism and how it presents itself as a hybrid threat in today's society, in the

international system, and its impacts within these limits. It is intended to approach through an institutionalist perspective how states understand this threat, what definitions they hold on this subject, what effects this type of threat causes within their societies, and what means of counter-response these actors have at their disposal to ensure against cyber-terrorism.

Calder and Watkins (2015) state that what is known about cyber security and its consequences is the tip of an "iceberg." This is because cybersecurity covers many more sectors than one might think, such as cyberterrorism, cyber-attacks, cyber warfare, fraud, and even the variant of cyber diplomacy. And each of these possibilities consists of different actions, threats, and strategies to get around the dilemmas. (CALDER and WATKINS, 2015)

Dorothy Denning, a professor of computer science, was one of the first to propose a definition. She described cyberterrorism as a convergence between cyberspace and terrorism. She added, "It refers to unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives." Her way of describing cyberterrorism made it possible to differentiate these politically motivated activities from others. (DENNING,2000)

Cyber terrorism for Michael L. Gross, Daphna Canetti, and Dana R. Vashdi is much more complex and difficult to define than conventional terrorism. For them, cyberterrorism may be considered "more subtle" because its consequences are not seen at first, but its repercussions demonstrate anything but subtlety. The fact that cyber terrorism differs from conventional terrorism does not mean ignoring it for Gross, Canetti, and Vashdi. They also explain that this type of threat is less gauged because cyberterrorism has not yet been seen to cause death or injury to anyone. This is why many states still do not warn on this topic, as it does not directly harm the human security of states as conventional terrorism does. (GROSS, CANETTI and VASHDI, 2016).

Also, Johan Eriksson and Giampiero Giacomello (2007) believe that cyber threats are mainly intelligence problems, not physical threats, but like any intellectual challenge, they may lead to or abstract physical attacks. The problems surrounding cyber threats will involve loss or distortion of information, but even in the scenario built by the media as "electronic Pearl Harbor," they are not direct physical threats if compared to missiles or weapons. (ERIKSSON and GIACOMELLO, 2007). Both acknowledge that "Terrorists, organized criminals and other culprits can use cyberspace for mobilization and coordination, harassment, theft and fraud" (ERIKSSON and GIACOMELLO, 2007). On another side,

authors like Gordon and Ford (2003) are willing to consider even the online purchase of an airplane ticket as a part of a terrorist execution, for example, 9/11 (GORDON and FORD, 2003).

Furthermore, to see cyberterrorism as a hybrid threat, one of the main objectives of this project, Håkan Gunneriusson, and Rain Ottis, explain the subject well, addressing both concepts and cases. The authors define a hybrid threat as a set of factors and actions which unfold as a total manifestation of warfare. Hybrid threats cannot be explained by just one type of actor since they can occur by states, non-state actors, and even individuals. According to the authors, it aims to make the other side submit to their will through all possible means (GUNNERIUSSON and OTTIS, 2013). The term first appeared back at the beginning of the XXI century. It had other labels used interchangeably to the phenomenon, such as hybrid warfare/war, "new wars," fourth-generation warfare, or asymmetric warfare. (GIANNOPOULOS et al., 2021). Frank Hoffman is considered the father of the hybrid warfare concept and first used to term in 2005, in one of his articles, with James Mattis. In the article, the authors described what they described as new warfare. They highlighted what can be expected from it "unorthodox attacks or random acts of violence by sympathetic groups of non-state actors against our critical infrastructure or our transportation networks." (MATTIS and HOFFMAN, 2005).

NATO's involvement in the matter resulted from a 15-year commitment, which followed the evolution of technological innovations in telecommunications, the cyber environment, and the interconnectivity synonymous with the 21st century. (PEREIRA, 2018, pg. 7). The Alliance played a significant role in the studies and research surrounding Hybrid Threats and Cyberterrorism. It was one of the first to attempt to conceptualize the problem, creating many centers of research and making an effort to make states aware of the threats.

This research aims to understand, from the main question, what is the role of cyberterrorism as a type of hybrid threat in the current situation and how states and institutions such as NATO understand and defend themselves from these threats. It is first necessary to conceptualize what hybrid threats and cyberterrorism are for the international states system and how states and institutions, such as NATO and the EU, view this issue. As shown above, there is a tendency of confusion around the term, meaning the first chapter will be dedicated to drawing all the concepts and definitions that cyberterrorism has carried so far to give a clear perspective on the subject. Then, it is necessary to understand how these actors are protecting themselves from these threats and what strategies and defenses they are

studying to combat this new type of coercion, which has emerged mainly in conjunction with the new global framework characterized by a strong technological presence.

From this, it will present two case studies examples of cyberterrorism against states: Estonia and Iran. The first country is an example of an attack against a NATO member. At the same time, Iran is not part of the alliance and will represent another type of response and aftermath regarding a cyber-attack. It is hoped to understand how the reaction of two states with different contexts differs and how this presents itself in how they approach the issue, react, and protect themselves from it. At the end of this project, it is expected to understand how States with different backgrounds respond to a Hybrid Threat, in this case, cyberterrorism, and how their action after the events and how this shaped their cyber reality.

To this end, a qualitative methodology will be used, where bibliographic analysis and document analysis will be treated, such as legislation and Strategy reports from States and Institutions, as well as analysis of speeches by responsible politicians on the subject. In this way, the use of the sociological research approach is advantageous since it brings with it values of the social behavior of individuals, states, and international institutions in an empirical way and will be fundamental when it is necessary to understand the impacts that hybrid threats cause to the population of the countries presented as case studies: Estonia and Iran.

Therefore, the research's main question "what is the role of cyber terrorism as a type of hybrid threat within the current conjuncture, and how do states, and institutions such as NATO, understand and defend against these threats? "and the context in which the research design is set, has the desire to answer the following questions: 1) What is the role of cyber terrorism as a type of hybrid threat within the current conjuncture? 2) How do states, and institutions such as NATO, understand and defend against these hybrid threats? 3) What constitutes cyberterrorism attacks? 4) How did the two cases analyzed behave and react after the attacks? 5) What were the fundamental points affected within each State/Society?

Within this, the potential hypotheses are that: states are neither prepared nor aware of the proportions that hybrid threats and, in this case, cyber-attacks, may represent in international politics today and in the future. There are still too many gaps in securing and protecting oneself in this space, and there is still a long way to go in studying this subject. Non-state actors and entities such as NATO are indeed making efforts to create an agenda to debate these threats, but more commitment from other bodies is still lacking.

Therefore, the project will be divided into three main chapters with their sub-categories. The first chapter will present a bibliographical overview of everything discussed

regarding cyberterrorism. First, contextualization of the term ‘terrorism’ will be introduced as to when the term cyberterrorism appears. Next, the concepts and definitions that the word carries according to various actors and organizations will be presented. Subsequently, the ideas surrounding the term 'hybrid threats' and how cyberterrorism is an example will be referred to. The end of the first chapter will allude to how the Copenhagen School theory understands the term and its unfoldings. With this, it is believed that by first presenting all the theoretical framework that the object of study is inserted, it will be possible to use the concepts, definitions, and opinions of authors and theorists in the last chapter to corroborate the analysis that will be presented.

In the second chapter will be described the two cases that will be compared, Estonia and Iran. First, the cases that took place in Estonia in 2007, and all their unfoldings, methods of attack, and the climax of the attacks that started in the first place. Secondly, the Iran case, which became public in 2010, culminated in several other actions within cyberspace. The reasons connected with the attacks, how the international community perceived the malware, and the following developments will be presented. When concluding the chapter, it is expected that the reader has a concrete overview of the facts, and is already capable of noticing similarities or differences between the two attacks, so that, in the end, they are also capable of following the analysis that will be presented.

Lastly, will be given, which were the defense approach of the two countries and their reaction to the attacks, an example of a hybrid threat. In the first part, their strategies and responses will be introduced, as well as any tactic they have used to counter the offensive; at this point, some of the interpretations will start to be pointed out to create an introduction to the analyses. Secondly, it will be developed how these two countries behaved towards cyberterrorism, their main difference, and which characteristics stood out the most for this writer. After this, it will be possible to analyze why disparities exist and how they can be explained with all the concepts and theories mentioned in the first chapter. Finally, together with the conclusion, you will find the final opinions and thoughts regarding the main things the two cases differ, how the writer here interpreted those, and how a connection can be made regarding the studies of cyberterrorism and the security theory, Copenhagen School. It is expected that by the end of this work, the reader will have an understanding of the current set of cyberterrorism, have knowledge about how the two attacks, Iran and Estonia, occurred, and be able to identify and discuss what the differences are between the reactions of these two countries with such different backgrounds that have suffered examples of cyberterrorism.

1. What is terrorism, key concepts

For some years now we see ourselves surrounded by technology. Little tasks that used to be done manually, now can be done in more efficient ways with new tools that many times, we didn't even know about. Human lives are each day more present in the virtual world via social media, shopping, dating, and banking apps, which have as their central core to make life in society easier and faster. And this indeed can be seen in many aspects of daily life. In one way or another, the covid-19 pandemic helped this migration, which was already noticeable for some years, happen faster, increasing, even more, the presence and human dependency in the online world.

Technology has brought out many advantages to humankind for centuries. It has helped evolve human medicine, engineering, research, and so on. The Oxford Dictionary defines technology as "scientific knowledge used in practical ways in industry, for example in designing new machines". And it was in 1983, that humankind with the foundations laid by technology created the internet. However, as John Naughton recounts, the early history of the internet has its origins as far back as the 1960s, when, in a cold war environment, the US Department of Defense started a project to create a new kind of communication system, where it could survive a thermonuclear attack if it happens. When the Soviet Union successfully launched the Sputnik satellite, the US department felt the need to create the Advanced Research Project Agency (ARPA), which was connected to the Department of Defense. The ARPA was constantly dealing with several computer machines, that were incompatible with one another, making it impossible sharing of any type of information. With this scenario, the idea of a network that would enable resources to be shared appeared (NAUGHTON, 2016)

In its first two decades, the internet was an "item" majorly used by the technological, academic, and research elite. After this, from early 1990, it began to percolate into mainstream society, and it is now widely regarded as a General Purpose Technology (GPT) without which modern society could not function. In a considerably short amount of time, this technology went from being something "exotic" to something completely mundane, like having a fridge, which man was fully devoted to (NAUGHTON, 2016).

This was the beginning of what it's called today's cyber world. And together with it, terms such as *hackers*, *cyberterrorism,* and *cyber-attacks* became more and more popular and seen in daily life. This chapter has the objective of presenting what cyberterrorism is, all the concepts attached to it, the many different views the researchers share, how it is

understood by society today, what is their different types and how it is used as means of terror. Together with this, it will be presented the term Hybrid Threats, much used to describe the new types of threats in modern society, and in which cyberterrorism is an example. Also, will be presented the Security Theory, Copenhagen School, focusing on how this theory sees Hybrid Threats, and more specifically, Cyberterrorism. However, before the research jumps to this end, first it is necessary to understand the early days of the word terrorism, how it arose, and how it became to be used in the cyber world.

1.1. Terrorism - from the initial reality to today's cyberterrorism

The term terrorism has always been difficult to define. Many scholars have been reluctant about agreeing on one singular definition since terrorism can be interpreted in many different ways. After the incidents that followed in New York and Washington in 2001, and more than 6 thousand people were killed, the term terrorism became much more popular, but this does not mean that a singular meaning was attached to it. After the event, many theoretical started to formulate theories and definitions of what Terrorism was and how society and the governors could better define these actions, categorize them and also prevent them.

Something that was always very clear was the difficulty of handling such terms and defining them. The word "terrorism" has been used to describe a variety of different violent acts that would go from domestic altercations to workplace homicide. Yet, these are not the acts that people remember when they think about a terrorist attack. This misinterpretation is the key point of why is still so hard to deal with terrorism and all its variants (RUBY, 2002; ERIKSSON and GIACOMMELLO, 2007)

In 1989, NATO introduced a definition of terrorism in its Glossary of Terms and Definitions (2013). They understood terrorism as "the unlawful use of threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives" (NATO, 2014) At the beginning of the century they also defined other two terms which are correlated with terrorism, this being: *anti-terrorism* "all defensive and preventive measures taken to reduce the vulnerability of forces, individuals and property to terrorism" and *counter-terrorism* "All offensive measures taken to neutralize terrorism before and after hostile acts are carried out" (NATO, 2014). After the 9/11 incident, terrorism became again a much-

used term, but yet, not well understood, boosting the need to draw even more the many faces of terrorism.

Therefore, the United Nations Council Resolution 1566 (2004), following the same idea, attempted to provide, as well, some guidance on what they comprehended as terrorism which they described as "criminal acts" that were committed for some particular reasons, such as:

> - Committed with the intent to cause death or serious bodily injury, or taking of hostages;
> - Committed with the purpose of provoking a state of terror in the general public or in a group of persons or particular persons, intimidating a population or compelling a government or an international organization to act or to abstain from doing something;
> - Which constitute offenses within the scope of and as defined in the international conventions and protocols relating to terrorism; (UNSCR, 2004)

The UNSCR also adds that such acts cannot be justified irrespective of considerations of a political, philosophical, ideological, racial, ethnic, religious, or other nature (UNSCR, 2004). This characterization brings out some topics that could be discussed, for example: by this statement, it can be understood that when an act of terrorism just occurred there can be no doubt that the act was in fact terrorism. However, as Ruby (2002) stated in his article, acts of violence resulting from a terrorist attack can generate double or, sometimes, triple interpretations in people's minds, depending on their ideology or political preferences, accentuating again the historical difficulty of defining terrorism (RUBY, 2002).

Another term that always comes along when searching about terrorism is 'violent extremism, which also doesn't have one unique international definition. This term is always correlated with terrorism since both include a direct nexus to violence. In another hand, violence always assembles radicalization and this also can be used from time to time as a word tied up with terrorism or violent extremism. Radicalization refers to the process by which an individual increasingly supports or advocates radical ideas. However, UNODC, highlights that radicalization is not a threat to society if it is not connected to violence or other unlawful acts, and the concept should not be used to stigmatize people or restrict their human rights. And also stress that radicalization can be a force for beneficial change (UNODC, 2018).

One country that used many resources to get close to categorizing what is terrorism was the United States of America (USA). Since 1983, the U.S. Department of State used Title 22 of the United States Code, Section 2656f (d) to define terrorism. In its introduction, terrorism is defined as politically motivated violence perpetrated against non-combatant

targets by subnational groups or clandestine agents, usually intended to influence an audience (U.S. DEPARTMENT OF STATE, 2001).

This definition includes three key criteria that distinguish terrorism from other forms of violence: the first form, according to Ruby (2002), is that terrorism must be politically motivated, which means that when a terrorist attack happens its origins must come with the intent to influence governmental policy. The second criterion is that terrorism will be directed at noncombatants, meaning, people who are not members of the military services or are not involved in the military hostilities. With this, is understandable that terrorism will be focused on those civilians and groups who are not prepared and are not able to defend themselves against political violence.

The last, and third criterion, is that subnational groups or clandestine agents commit terrorist attacks, which occur to exclude nation-states. This, for example, can be exemplified when Japan sent bombs to Pearl Harbor in 1941, this attack is not considered terrorism since it was caused by the Japanese government, during a period of war. The third point also stresses the clandestine features that follow terrorist attacks, based on that, the victims cannot anticipate that the attack will happen. This differs when in times of war, the citizens expect that an attack may probably happen (RUBY, 2002).

Following this definition, is possible to occur some questions regarding the origins of the expression 'terrorism', should the word be used only in a political context? If terrorism is a type of violence, does it always needs to be against persons or also, or could be against properties as well? Since the term is historically connected to terror, should the concept be focused mainly on that, or should also bring the sociology and psychology aspects of it? All these questions were brought up by Igor Primoratz, in his paper "What is terrorism?". According to him, the attempt to try to find one single meaning to the word terrorism is pointless since the word has been used in so many different ways, rather he thinks it is best used of his research to try to find a definition that can capture the traits of terrorism that makes all people fear and repel the word (PRIMORATZ, 1990).

Following the same idea as Ruby, Primoratz start his research reaffirming, terrorist attacks do not happen without purposes, as he describes "for the terrorist does not strike blindly and pointlessly, left or right, but rather plans his actions carefully, weighing his options and trying for the course of action that will best promote his objective at the lowest cost to himself" (PRIMORATZ, 1990). For him, terrorism is basic. It always had two targets, one that he describes as "immediate" or "direct target" and other that has secondary importance and it's the indirect target but is the most important. According to this idea, the

indirect target is important because it aims to force people to do things they wouldn't do otherwise. This is an act of intimidation, and when it happens via violence against innocent people or by threatening, then this can be understood as terrorism.

The terrorists will abuse this technic, and in some cases, they might even target not innocent people, a group of militaries for example, but his secondary and indirect will be. Thus terrorists may attack a group of civilians to intimidate the civilian population at large, coercing them to leave, or pressuring the government to follow their requests and demands. The idea of innocent people is that they will be people who haven't done anything for the terrorist group to use it as a justification for their actions.

By this, it can be understood that terrorist groups choose only to target or attack innocent people. However, this can generate other types of opinions, as did for Walter Laqueur, to think terrorists will consciously choose to spare the "guilty" and will only condemn the innocents is a thought that is not accepted by him. Terrorist groups will be quite indiscriminate in their choice of victims, however, from time to time, they will be quite selective. He uses it as an example of when President Sadat, the Pope, Aldo Moro, or Indira Gandhi were targeted and were not arbitrary (LAQUEUR, 1987).

The idea presented by Laqueur is completely denied by Primoratz, which chooses a fair argument and explanation for what he understands about the matter:

> "What is claimed is that the defining feature of terrorism, and the reason why many of us find it extremely morally repugnant, is its failure to discriminate between the innocent and the guilty, and its consequent failure to respect the immunity of the former and to concentrate exclusively on the latter. The terrorist does not take on the army or the police, nor does he attempt to kill a political official, but chooses, say, to plant a bomb in a city bus, either because that is so much easier or, perhaps, because that will better serve his cause" (PRIMORATZ, 1990).

The explanation he chooses relates to what the U.S. Department of State acknowledges as terrorism, more precisely to its second criterion in which we read that attacks occur to those who do not know and have no preparation for what is about to happen. Innocence then is indeed one of the traits directly associated with terrorism, conceptually and morally.

To conclude his article, Primoratz gives his version of a definition for terrorism, he starts with "the deliberate use of violence, or threat of its use, against innocent people, intending to intimidate them, or other people, into a course of action they otherwise would not take" (PRIMORATZ, 1990). It can be interpreted with this some other important traits that follow all the other definitions presented here before: violence, innocence, and manipulation. All this will can be reached with the terms of terror.

Etymologically, “terrorism” derives from the word “terror”. Initially,

> “was originally constructed not to describe the actions of non-state actors such as al-Qaeda, ETA, or the Fuerzas Armadas Revolucionarias de Colombia (FARC) to whom we are instinctively drawn when we now hear it. Rather, it was created at the time of the French revolution to refer to the actions undertaken by the state against dissidents and dissenters in their own populations.... Moreover, in its original usage it lacked the negative, pejorative connotations that are now inherent to the term. Indeed, even in the aftermath of World War II, when the term became attached to anti-colonial struggles in Asia, Africa and elsewhere, it lacked, for many, the sense of illegitimacy we now frequently attached to it” (JACKSON, JARVIS, GUNNING and BREEN-SMITH, 2011).

With time, the correlation of the word with system or regime lost power, maintaining though, its relation with terror. Terrorism is meant to cause terror or extreme fear, and when victorious, it does so. As it was mentioned before, terrorism is intimidation with a purpose and a goal. Carl Wellman describes

> “the use or attempted use of terror as a means of coercion” and remarks that violence often enters the picture as it is one of the most effective ways of causing terror. It can be comprehended that terror will be linked to violence no matter the circumstances, however, Wellman himself makes an important clarification, “the ethics of terrorism is not a mere footnote to the ethics of violence because violence is not essential to terrorism and, in fact, most acts of terrorism are nonviolent” (WELLMAN, 1979)

Even though, at the time Wellman declare his ideas terrorist attacks were not so violent, making it possible to reassure such a statement, it is important to take his words to acknowledge that terrorism, not necessarily will be committed in violent ways. Take cyberterrorism for example. Cyberterrorist attacks not necessarily will cause physical damage to someone or a group, but rather will use in its favor the probability of violence. Cyberterrorism abuses the psychological effect that its attacks have on its victims, creating the same sense of terror as traditional terrorism.

Kaplan (1978) said it well when describing terrorism as something intended to create an extremely fearful state of mind. He claimed that the fearful state was not intended for the terrorist victim itself, rather, was intended for an audience who may have no relationship with the victims. The same is mentioned by Oots (1990) that also expresses the terrorist intention to create extreme fear and/or anxiety-inducing effects to a large audience. This opinion is only salient that terrorism will happen with a particular intention and this intention will have as its goal, to make a population or a government do something that they wouldn’t otherwise. In other words, manipulation (KAPLAN, 1978; RUBY, 2002).

If the numbers are analyzed, like did Ruby, indeed terrorist attacks create much fewer victims or deaths than other sources of violence. The examples that Charles Ruby did

is pertinent “nearly 42,000 people were killed in car accidents in the United States in 2000 (U.S. Department of Transportation, 2001) and over 15,500 people were murdered in the United States in 1999 (GRISET and MAHAN, 2003)”. And yet, these numbers are not on the front cover of newspapers. In the attacks that took place on September 11, 2001, approximately 6,000 people were killed, a number considerably small compared to the ones cited before, but then, why does the terrorist phenomenon still hold more attention? This is one of the main objectives of a terrorist attack already mentioned here before, creating fear and panic in the larger population (RUBY, 2002).

Big actors in international relations, like, the UN still struggle to have an agreed definition due to differences of opinion between the many members that compose the general assembly of the UN. Yet, the countries that are in the UN’s Security Council managed to consent to one definition:

> “criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act” (U. N. Security Council Resolution 1566 (2004).

This definition has an operative effect and is helpful in case the Security Council needs to have proper action regarding a potential terrorist attack, however, does not mean that this definition binds all states in international law. Meanwhile, the European Union has its own definition of terrorism:

> “According to EU law, terrorist offenses are acts committed with the aim of
> - seriously intimidating a population
> - unduly compelling a government or international organization to perform or abstain from performing any act
> - seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization (Consilium Europa, 2022)”

Is always important to see and understand how these organizations acknowledge the term because their point of view will likely reflect political interests and agenda, more than any analytical or “scientific” purpose. As Lee Jarvis acknowledges, the lack of consensus is something important to be aware, of because it helps to account for the dramatic changes in the understanding of the word terrorism that have taken place over the past 200 years, since the term was first coined (JARVIS, NOURING, and WHITING, 2014).

A worldwide definition of terrorism does not yet exist, mainly because many aspects can create double or even more interpretations. Those interpretations can include, the type of violence, their political motivation, the randomness of targets, theoretical or

spectacular violence, the creation of fear in a secondary audience, an effort at communication, non-state perpetrators, and so on, making a consensus between academics and policymakers difficult (JARVIS et al., 2014).

However, some traits can be noticed in all the definitions that have been presented here so far, these are: 1) the political aspect of a terrorist attack, most will happen with the intention of drawing a country/nation's attention to the executing group; 2) terrorism is clandestine, which means that it will not occur during a time of war, leaving the victims without a clue that an attack may happen, which brings to the third trait much cited by all theorists; 3) the victims of these attacks will always be innocent, there may be some exceptions, but the vast majority will be groups of innocents which will generate the last and final trait noted; 4) terror, the intent of an attack may vary, however, they all at some point aim to create the state of terror, bringing the psychological aspects of terrorism to the center of attention of rulers and theorists.

Now that there is a better understanding of the definitions surrounding the word "terrorism" makes it is easier to start developing this paper. As mentioned many times here, the term terrorism besides its many meanings has also many interpretations. Some of those interpretations become categories of the term, which shall be presented in the next section.

1.2. The different types of terrorism

Within the modernization of the world that started in the 60s, globalization came along and another way of terrorism was born. Today's called modern terrorism started to develop in an environment of cultural differences, poverty, social problems, and economic imbalance that lead to a bunch of conflicts that were not solved. Those conflicts that were created by governments, and left "incomplete" was the appropriate conditions for terrorism to rise as the best answer to solve them.

What is known as 'modern terrorism' has some important differences from conventional terrorism, the differences between those two will be illustrated in Table 1.

Table 1: Differences between Conventional and Modern Terrorism

Conventional Terrorism	Modern Terrorism
The goals are achievable (i.e. demanding ransom for hostages)	The goas are not achievable (i.e. demanding the USA to surrender totally)
Attacking Options are limited	The attacking Options are unlimited
Use of conventional weapons (i.e. guns, grenades)	Use of conventional and non-conventional weapons (i.e. *cyber-attacks, bioweapons*)
The effects are localized	The effects are globalized
Activity is within one state	Activity is transboundary
There are coded warning	There are no warnings
There are no suicide	Suicide Bombings are typical

Source: Dávid Tóth on his research, 'The History and Types of Terrorism.

Following the same idea, Andreas Gofas (2012) (table 2) comes along and explains his understanding of the old and new terrorism, between the two authors can be noticed similarities in what they identify as traditional and modern regarding the shapes of terrorism. Both talk about how the new terrorism is transnational and is not frontiers oriented. The type of violence is also escalated in the new terrorism, as new weapons are used and new ways of recruiting supporters are explored. The organizational structure of those terrorist groups is no longer hierarchical and become networked, meaning that, people all over the world can assume certain responsibilities inside these groups (GOFAS, 2012).

Table 2: Old and New Terrorism by Andreas Gofas (2012)

	"Old" Terrorism	"New" Terrorism
Organizational Structure	Hierarchical	Networked
Operational Range	Within home region (territorial orientation)	Outside home region (transnational orientation)
Motives	Political/Nationalist Ideology	Religious Fanaticism
Tactics	Restrained Violence	Extreme Violence
Attitude towards Westphalian System	System-Affirming	System-Threatening

Source: Andreas Gofas (2012)

Amy Zalman (2012) in her book/article did a great job when identifying six types of terrorism that are worth mentioning here. Most importantly, she also identified cyberterrorism, the object of research in this paper (ZALMAN, 2012). She starts with:

I.State Terrorism

Zalman defines this type as one of the most intriguing to understand. It is often recognized that terrorist attacks will be caused by non-state actors. However, according to this definition, there will be occasions when States will create terror. States occasionally can use their forces without declaring war, to terrorize citizens and achieve their political goals. She uses as an example the Jacobin Dictatorship (ZALMAN, 2012).

States can also perform terrorism often by proxy. For example, the USA tends to consider Iran one of the most prolific sponsors of terrorism, because of groups such as Hezbollah, that help carry out its foreign policy objectives. The United States itself has been called a terrorist in the 1980s when it sponsored Nicaraguan Contras (ZALMAN, 2012).

II. Bioterrorism

Some may think that bioterrorism is something of the present times. However, in history, it is possible to see that this phenomenon has its origins long ago when in human warfare, efforts were made so that germs and disease were used as weapons or as advantage strategies. Zalman defines bioterrorism as "the international release of toxic biological agents to harm and terrorize civilians, in the name of a political, ideological or other cause". There are many viruses, bacteria, and toxins that are considered to be dangerous and potential "weapons" in an attack, such as Anthrax (*Bacillus Anthracis*); Botulism (*Clostridium Botulinum Toxin*); the Plague (*Yersinia pestis*); Smallpox (*variola major*); Tularemia (*Francisella Tularensis*); and Hemmorrahagic fever, due to Ebola and Marburg virus (ABRAMSON, 2012)

The first dated records of bioterrorist attacks are in the 14th century, in pre-modern times. In the late 18th century, during the French Indian War, the British army reportedly delivered blankets to Native Americans which were contaminated with the Variola virus. This event is a good example of the use of bioterrorism as a war strategy.

Already at the end of the last century, violent non-governmental actors started to develop biological agents to be used as weapons against civilians in their attacks. However, it is important to mention that there are very few of these groups and almost no records of attacks by them. Surprisingly, the ones that have more records on those types of terrorism are the States. Also in the 20th century, Japan, Germany, the former Soviet Union, Iraq, the USA, and Great Britain had biological warfare development plans, meaning that, an arsenal was being created by those countries during the cold war. However, again, there are not many confirmations on bioterrorism attacks.

In 1984, a cult in the US called the Rajneesh (later known as Osho) poisoned hundreds of people when Salmonella Typhimurium was added to an Oregon Salad bar, and hundreds of people got ill. The attacks were done during an election period, and the group wished that their candidates had enough chance to win the election. Even though many people contracted Salmonella, and many were hospitalized, none died. Following this same trend, a Japanese Cult called Aum Shinrikyo, in 1995, released sarin gas in Tokyo underground, and killed 12 people and injuring thousands. Since 1993, the cult tried to spray botulinum toxin and anthrax in downtown Tokyo (https://web.archive.org/web/20071209163344/http://www.pbs.org/wgbh/nova/bioterror/hist_nf.html, retrieved in 05th July of 2022).

III. Ecoterrorism

Some might disagree with the existence of the term "eco-terrorism". The term is still quite new and tends to be used when describing violence inside the environmental world. It is most common to see the term when reading about environmental extremists that sabotage properties in inflicting economic damage, either on industries or actors, that they understand are harming animals and mother nature. Examples can be said research laboratories that manage tests in animals, fur companies, or logging companies.

Eagan defines the term as "the use or threatened use of violence of a criminal nature against innocent victims or property by an environmentally oriented subnational group for environmental-political reasons, aimed at an audience beyond the target, and often of a symbolic nature" (EAGAN, 1996).

IV. Nuclear terrorism

Nuclear terrorism might be one of the easiest types to understand without going too deep into research, it assembles several different ways nuclear materials can be exploited by terrorist organizations. The tactics behind an attack might include: attacking nuclear facilities, purchasing nuclear weapons, building nuclear weapons, or creating dirty bombs (conventional explosives, such as dynamites, with radioactive components in solid, liquid, or gaseous form) (ALLISSON, 2005)

There is one famous incident connected with a dirty bomb, in which the Chechen terrorist planted radioactive cesium packed with dynamite in a Moscow park. Luckily the local police were capable of quickly locating the dirty bomb before any extra harm was made (ALLISON, 2005).

V. Narcoterrorism

The term was first used in 1983 by Peruvian president Belaunde Terry. At the time, the president described the term within the attempts narcotics traffickers did to influence local politicians and civilians with the use of violence and intimidation in other to stop the enforcement of anti-drugs laws (HARTELIUS, 2008). Since then, there were added several definitions to the word.

The Oxford dictionary defines narcoterrorism as "terrorism associated with the trade in illicit drugs". Many might agree this definition is quite short if compared to the wide scope the terms are allocated. Narcoterrorism cannot be defined without some variables such as ideology, politics and commercial factors, and criminality. In the United States, the Drug Enforcement Agency (DEA) came up with a definition to be used, since the country, since the 1980s has suffered from the problems brought about by drug trafficking, defined as

> a "subset of terrorism, in which terrorist groups or associated individuals participate directly or indirectly in the cultivation, manufacture, transportation, or distribution of controlled substances and the monies derived from these activities. Further, narcoterrorism may be characterized by the participation of groups associated individuals in taxing, providing security for, otherwise aiding and abetting drug trafficking endeavors in an effort to further, or fund terrorist activities" (THACHUK, 2007).
>
> Jonas Hartelius uses different words to describe the expression, a bit more polished, but worth mentioning: "a part of an illegal complex of drugs, violence, and power, where the illegal drug trade and the illegal exercise of power have become aggregated in such a way that they threaten democracy and the rule of law" (HARTELIUS, 2008).

VI. Cyberterrorism

Last but not least, what concerns cyberterrorism, the object of study of this present paper, Barry Collin said, "cyberterrorism is a new phenomenon, and there is still no unified definition for it". Following the same partners as the former term terrorism, cyberterrorism is still hard to define. Collin was the one researcher that came up with the term cyberterrorism in 1997. To him, the term meant the collision of the physical world with the virtual one, where the two meet, and sometimes can generate physical violence. To give the deserved attention to the many other definitions and understanding of cyberterrorism, this type of terrorism will be carefully approached in the next sector of this chapter, where it will have more space for the research to unfold (DOTH, 2015).

1.3. What is cyberterrorism and the use of technology as a means of terror?

The first appearance of the word 'cyber' goes back to the early 1990s when it became common for people who were dealing directly with computers to start to coin new words just by adding "cyber", "computer" or "information" before another word. Thus, a full "library" of new words was created, and cyberterrorism, cybercrime, infowar, netwar, cyberharassment, virtual warfare, digital terrorism, cyber tactics, and cyber-attacks came with it (WEIMANN, 2004). The notion of cyberterrorism has its roots in the same time frame and was often connected to the rapid growth in internet use and the debate of the emerging "information society", where society was each day more highly networked and high-tech-dependent. Within the end of the Soviet Union, the so then known "predictable threats" disappeared, resulting in a change of attention to the "new" types of risks (JARVIS et al., 2014).

Very similar to following in the footsteps of its predecessor, the term cyberterrorism also encounters difficulties when it comes to a single definition. There have been many attempts by scholars and government organizations to find one single definition of cyberterrorism, yet, there has not been one that all actors agree on, regarding not only the meaning but the examples, descriptions, and counterparts. Still, even though there is not one single true definition, many of those actors in International Relations have put effort to describe as accurate and detailed as possible their understanding of the term and introduce better semantic precision to it (WEIMANN, 2004).

Dorothy Denning, a professor of computer science, can be the first example of a definition. She described cyberterrorism as a convergence between cyberspace and terrorism.

> "It refers to unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or properties, or at least cause enough harm to generate fear" (DENNING, 2000).

She also added to her definition that attacks that lead to death or any type of injury, explosions, or even severe economic loss could be examples of cyberterrorism, especially attacks against critical infrastructure. Her way of describing cyberterrorism makes it possible to differentiate these politically motivated activities from others (DENNING, 2000).

Several authors, in another hand, prefer a graduated approach, distinguishing between what they called "pure" and other types of terrorism. The first, resign to only attacks on digital targets via digital means, while the other, may also incorporate activities such as propagandizing or fundraising online (MALCOLM, 2004). Two authors that also use a similar term are Desouza and Hensgen (2003), who use "unique" cyberterrorism to describe "the use of legitimate electronic outlets to facilitate communication among terrorist groups" (DESOUZA and HENSGEN, 2003). Some will question this criterion, whether the significant disruption to a computer network can be considered terrorism. For instance, Soo Hoo et al (1997), the question "network attacks like shutting down a long-distance telephone network or a company's internal network (might) be considered terrorism?", and they continue, "no violence is used, and no life-threatening terror is instilled" (SOO HOO et al., 1997).

Following Denning's ideas, Gordon and Ford (2003) used her definition to frame their own. They discuss:

> "We believe that the true impact of her opening statement ("the converge of terrorism and cyberspace") is realized not only when the attack is launched against computers, but when many of the other factors and abilities of the virtual world are leveraged by the terrorist in order to complete his mission, whatever that may be" (GORDON and FORD, 2003)

With this statement, they are allowing a much wider spectrum of actions to be considered cyberterrorism than Denning originally did. The two authors are willing to consider even the online purchase of an airplane ticket as a part of a terrorist execution, for example, 9/11 (GORDON and FORD, 2003). This kind of statement helps the emergence of another kind of comparative approach that other researchers will use. On one side, it can be found authors such as Maura Conway, wants to distinguish between "terrorist use of computers as a facilitator of their activities" with "terrorism involving computer technology as a weapon or target" (CONWAY, 2002). On the other side are those such as Devost et al., (1997) that position a constant between terrorism, information terrorism, and pure information terrorism. They understand, for example, if the target and tool of an attack are "physical" entities, then the attack is an example of "traditional terrorism". But, if either the tools or the target can be considered digital, then the attack will be an example of "information terrorism". Furthermore, they add that if when a target and tool are both digital, this will be considered "pure information terrorism" (DEVOST et al., 1997).

Subsequent to these ideas, Lee Jarvis et al. frame four reasons why it is so difficult to achieve a consensus towards the meaning of cyberterrorism. The first reason they describe

is a temporal factor. The ‘steps’ of an attack - preparation, conduct, and consequence - have a very mutual duration and same possibility to have digital threats, meaning that, to each of the steps can be attached many examples and characteristics, making it harder to create one “rule” to categorize them. They also add that given the myriad ways in which the digital world might be presented in an attack, the question changes to “which, and how many, of these engagements are necessary to designate such an event as “cyberterrorism” (JARVIS et al., 2014)

The second factor they present is due to the “damage” of an attack. While some authors reserve the cyberterrorism label for specific behaviors that leads to destruction or damage, physical or otherwise, others see it differently. One example is, again, Devost et al., (1997), that are willing to soften this condition:

> “there are subtler forms of information terrorism (e.g- electronic fund theft to support terrorist operations, rerouting of arms shipments, etc) which would still be political crimes, but perhaps more dangerous because they are less dramatic than a cyber-Chornobyl’, and thus more difficult to detect and can even appear as ‘common’ crimes (DEVOST et al. apud JARVIS et al., 2014)

Thus, Jarvis et al. (2014) use as an example, the opposing beliefs of Conway and Desouza and Hensgen to exemplify one more reason why consensus is difficult to reach: “while a number of scholars argue that, ‘violence against persons or severe economic damage’ (CONWAY, 2002) must occur for an event to be termed cyberterrorism, others believe that any terrorist usage of the internet to constitute a sufficient criterion (DESOUZA and HENSGEN, 2003; JARVIS et al., 2014).

The third reason presented was the ‘cyber terminology’. As mentioned before, often the mass media frequently fail to distinguish between other types of cyber threats - such as hacktivism - with cyberterrorism, leading to a misuse of the word and concept, corroborating an exaggeration of the latter. Conway (2002), also mentions confusion between the meaning of cybercrime and cyberterrorism. This unstable reality, according to Jarvis et al. (2014), has a real risk of introducing analytical confusion into the concept: confusing what is meant by cyberterrorism and any of its related terminologies (JARVIS et al., 2014).

The fourth, and last reason, is connected to the previous one and it is the misleading hyperbole around cyberterrorism. The way media portray cyberterrorism is a challenge to its conceptualization, given the fact that the media tend to add their voice to the fearful chorus in scary front pages and headlines (WEIMANN apud JARVIS et al., 2014). The media has in their hands a perfect subject since cyberterrorism incorporates randomness,

incomprehensibility, and uncontrollability found in terrorism, but with the complexity and seeming abstractness of technology (CAVELTY apud JARVIS et al., 2014). In this sense, the fear surrounding cyberterrorism produces, together with media hyperbole and a lack of understanding of modern digital technologies adds further confusion to this term (JARVIS et al.,2014).

Research centers were also called upon to deliver a definition of cyberterrorism was. Most of these were North American centers, mostly connected with the government. It was the case in 1999 when the Naval Post Graduate School did one of the biggest research to comprehend what is cyberterrorism for the US Defense Intelligence Agency. The study concluded that "terrorist use of information technology in their support activities does not qualify cyberterrorism", this because at this period the term was suffering many "attacks" coming from the government, and the strategy they used, was to exclude some types of cyber-attacks as examples of cyberterrorism, such as script kiddie techniques including, dictionary attacks, spoofed emails, and bombardment of email boxes - an action very present in the hacktivism, that will be touched later on. To conclude, the research narrowly defined cyberterrorism as "the unlawful destruction or disruption of digital property to intimidate or coerce government or societies in the pursuit of goals that are political, religious or ideological" (SOESANTO, 2020).

According to Soesanto (2020), this definition, considering the time and the materials they had, was extremely accurate and did present a general definition of what the term was. However, there was another problem back then, the cases that could fit into this category, ended up fitting in different ones, like acts of cyberattack under the Computer Fraud and Abuse Act c (18 U.S.C 1030) or pre-action that could put national security at stake. Since then, Soesanto affirms, that the researchers have fought to find one single definition that could finally place cyberterrorism apart from cybercrime, hacktivism, or offensive military cyber operations. Indeed, it can be agreed that some parts of the cyber area can be very grey, meaning that, in some cases, there will only be a thin line separating two definitions. But that is exactly why is important to have wide knowledge about all the big definitions out there (SOESANTO, 2020).

In 2012, Jonalan Brickey (2012) also attempted to have one definition of his own, he started with "the use of cyber to commit terrorism, or use of cyber capabilities to conduct, enabling, disruptive and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of political change". Soesanto inquires that even after years since the first definition came to society, there are still some

that won't exactly fit in what cyberterrorism is, and, mentioned Daniel Cohen and his chapter in 2014 when he attempted to explain cyberterrorism, but exposed great examples of hacktivism instead (COHEN *apud* SOESANTO, 2020).

This argument can then be complemented by the idea proposed by Jarvis et al. (2014) where, due to the numerous difficulties of describing a single concept of cyberterrorism, it is interesting to abandon the idea of finding a "what is cyberterrorism" and instead focus on "how" it is constructed. By doing this, they suggest that scholars take advantage of a constructivist framework, that would help them to engage in the research without aiming only to find the ultimate concept but rather understand the term as a phenomenon. This follows the same idea that terrorism shares, to be a broader historical phenomenon that can be very fluid and changeable (JARVIS et al., 2014).

The first time researchers coined the word was in 1997, by Barry C. Collin, an American researcher that was intrigued by the new society after the internet. He described it as when the two worlds, the physical and the virtual, converge, and since they are inherently different, they create "cyberterrorism". His definition is very similar to Denning's one, and she was inspired by his early thoughts and develop her own "the converge of cyberspace and terrorism. It covers politically motivated hacking operations intended to cause grave harm such as loss of life and severe economic damage" (DENNING, 2000).

Another theoretical, and FBI agent, who followed the same ideas left by Collin and Denning, was Mark Pollit, who describes the expression as:

> "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents" (POLLIT, 1997).

Both of them linked cyberterrorism as a form of politically motivated attack, and the user of cyber to conquer some of the terrorist groups' ambitions. Dávid Tóth gave a very well-established explanation of how he sees terrorists enjoying the cyber world, and performing those attacks described here. He states that there are two types of using information technology as a way to achieve one's needs: the soft and the hard method (TÓTH, 2015).

The "soft" is the one in which information technology will be used by those terrorist organizations/groups as a space to advertise their propaganda to the world. Meaning that they are not actively using cyberspace with violence but just as a stage for their "acts", to reach public opinion (TÓTH, 2015).

As for the “hard” type, it is related to the explicit use of cyber warfare. He describes that those attacks inside the cyber can happen via restricting the operation of the information infrastructure, sending viruses, worms, botnet attacks, phishing, breaking into an electronic bank account, etc. The criminals use those called “botnets” (a certain type of automated robot) to infect a large number of computers and send out spam emails, spread those viruses, attack other computers and servers, and complete more and more kinds of crime and fraud (TÓTH, 2015).

But theorists have not always accepted the term. Many, especially during the early 21st century, denied that cyberterrorism was this threat that everyone was describing. Some believed that all the fear and fuss around the word was created by the media, as a form of control and prevention, so that people would stop trusting cyber. Weimann in 2004, wrote his article “Is the cyber terror threat exaggerated?” and presented many examples of why he believes that yes, the threat was exaggerated, but he also gives examples of why he thinks this happens like this (WEIMANN, 2004).

The first reason why he believes that the threat is smaller than people think is that according to him “cyberterrorism and cyber-attacks are sexy right now, is a novel, original and it captures people’s imagination” he described this quoting Denning’s words. Second, the hype around the subject can make the mass media frequently mention it on the first pages, which combined with the failure to proper distinguishing cyberterrorism from hacking, generates false fear and analogies in which society tends to believe (WEIMANN, 2004).

The third factor according to him is ignorance. Since it is a subject that is still hard to describe and involves two important spheres “terrorism and technology”, can cause many people, including the society´s leaders to not fully understand and therefore fear the word. This factor emerges with the fourth in which politicians will take advantage of the fear and put their agenda on top of this, to “play the role of prophets of doom” (WEIMANN, 2004).

The last factor Weimann presents is indeed something very much mentioned in all articles and studies involving cyberterrorism which is: the ambiguity that surrounds the word, and how a single meaning has not yet been agreed upon. Once the public doesn’t fully understand a topic, it’ll give space to myths and fear to start speculating (WEIMANN, 2004).

Even though, Weimann in his article makes clear what he thinks about cyberterrorism and everything related to it, when concluding it he affirms that “the threat of cyberterrorism may be exaggerated and manipulated but we can neither deny it nor ignore it”. It is important to see that even when theoretical disagree on one point, they agree that, is still needed to address this ambiguity around cyberterrorism. This argument meets that of

Soesanto, who also, in concluding his article, has not shown that he believes in all the possible threats posed by cyberterrorism. He stated that:

> "Cyberterrorism is probably best viewed as an operational tactic aimed at a distinct psychological outcome rather than a field of research that connects the cyber domain at the hip to terrorism in real space. Notably, while cyberterrorism research and policy has hit somewhat of a deadlock in recent years, leveraging tactical approaches to create terror in and through cyberspace is only at its beginning" (SOESANTO, 2020).

It is interesting to see that, two authors, at two different points in time, share similar views regarding the term. Cyberterrorism is indeed important but still has many areas to be explored.

Bogdanoski and Petreski were two of the researchers that defended the importance of cyberterrorism, while it became trendy to say the opposite as early presented. They exposed in their article the one definition they correlate the most to the term: "the use of information technology by terrorist groups or individuals to achieve their goals. This includes the use of information technology to organize and execute attacks against networks, computer systems, and telecommunications infrastructure, and to exchange information and perform electronic threat." Their understanding of the word can be the beginning of what means "cyber as means of terror" (BOGDANOSKI and PETRESKI, 2013).

They presented the multiple ways cyber can be used as a weapon for terrorist groups to exercise terror. The threats can manifest in many ways, such as hacking computer systems, programming viruses, worms, web page attacks, conducting denial of service (DoS) attacks, or conducting terrorist attacks through electronic communications. One of the biggest advantages for terrorist groups to use technology in their favor is the factor that since these groups have limited funds, cyber-attacks can be very cheap, once it requires a small number of people and very little budget. Another benefit is that they allow terrorists to stay unknown, since they can be far away from the place where the act will take place, for example. "Unlike the terrorists that place their camps in countries with weak governance, cyber terrorists can store anywhere and remain anonymous" (BOGDANOSKI and PETRESKI, 2013).

The argument was used to illustrate how this factor is enjoyed by those groups, and they add that the most effective strategy in cyberterrorism is when there is a combination of cyber and physical terrorism. Possible targets of cyberterrorism are government computer networks, financial networks, power plants, and more, they identify those targets as being damaged or put out of operation with the purpose to create chaos. Systems manipulations are also examples of how terrorists can enter secured systems targets, via secret entrance software, stealing classified information, data deletion, website damaging, and virus

inserting. Another potential attack empowered by computer technology is the control of the air traffic control system or RBY emote damage of the power supply network (BOGDANOSKI and PETRESKI,2013).

Terrorist organizations take advantage of all privileges cited above and add to one of the most important tasks every terrorist group needs, which is raising financial funds and distributing their propaganda, and recruiting new members. The internet ends up being the perfect stage to reach their people, or new ones, without the need to use any other type of media; websites are used to highlight any type of injustice the group is against and is seeking "revenge" either by, violence or online activities. They will use this tactic to give the impression they are weak and to present themselves as outsiders, all this with the ambition to recruit new people that will empathize with ideologies.

Another factor most people think about when they recall cyberterrorism is the fact that those organizations tend to take advantage of these websites and post content and instructions on how to make explosive or chemical weapons, for example. By doing that they can already see potential joiners just by how they sympathize with their cause, making it perfect to recruit the right people (BOGDANOSKI and PETRESKI,2013).

Cyber as means of terror will have many examples and many perspectives depending on where you look for information, but most authors will agree that this tactic is used to cause uncertainty to the public. The attacks can occur in two forms, one will be the use of available data and the other will focus on control systems. Data theft and destruction lead to service sabotage and it will be known as the most common type of cyberattack. On the other hand, the attacks focused on systems tend to be used to disable or manipulate physical infrastructure, meaning, they will combine the two worlds, the virtual and physical (BOGDANOSKI and PETRESKI, 2013). Later on, in the second chapter will be presented two cases of cyber-attacks that some consider an example of cyberterrorism, the Estonian and Iranian cases.

Terrorist groups will aim to target weak spots inside infrastructures so they can achieve their goals in faster way. The most critical infrastructures, according to the authors, are prone to be private ones, since they are not always keen on spending budget on cybersecurity. Nonetheless, the attacks will not always occur in the private sector, quite the opposite, some of the biggest examples of cyber-attacks happened in the public spectrum. In 1988 happened the first terrorist attack on government computer systems, a terrorist guerrilla organization flooded the embassies of Sri Lanka with eight hundred emails a day, to disrupt their communication with the outside world (BOGDANOSKI and PETRESKI, 2013).

On another occasion, Romanian hackers managed to infiltrate de computer systems controlling the life support systems at an Antarctic research station, endangering the 58 scientists involved. Any accident was reported. In a second one, during the Kosovo conflict, Belgrade Hackers conducted a DoS in the NATO servers. They flooded NATO servers with ICMP Ping messages, which are typically used for diagnostic or control purposes. DoS attack is meant to shut down a machine or a network making it inaccessible to its intended users, which is why they use as a tactic the "flooding" of the traffic (BOGDANOSKI and PETRESKI, 2013).

Another two authors important to mention when doing bibliographic research about cyberterrorism are Johan Eriksson and Giampiero Giacomello (2007). They believe that cyber threats are mainly intelligence problems, not physical threats, but like any intellectual challenge, they say, they may facilitate or abstract physical attacks. The problems surrounding cyber threats will involve loss or distortion of information, but even in the scenario built by the media as an "electronic Pearl Harbor" they are not direct physical threats if compared to missiles or weapons (ERIKSSON and GIACOMELLO, 2007).

Both acknowledge that fast-growing technology allows rapid global communication that brings together many problems that can be explored by terrorist groups. "Terrorists, organized criminals and other culprits can use cyberspace for mobilization and coordination, harassment, theft and fraud" (ERIKSSON and GIACOMELLO, 2007). And, like many intelligence operations, they may also have secondary effects, like for example, having access to important information that can help in the effectiveness of physical attacks. However, they point out that, yes, cyber-attacks can destroy "bits and bytes" but it is highly unlikely that they will achieve the same effects in terms of fear and destruction produced by a bomb or missile (ERIKSSON and GIACOMELLO, 2007).

Eriksson and Giacomello emphasize how threat framing and policy responses cannot be explained by technological developments or cyber incidents. They believe that they are rather shaped by psychological, bureaucratic-political, and media mechanisms (ERIKSSON and GIACOMELLO, 2007). Meaning that, the threat or, better say, securitization, around the word "cyberterrorism" is a constructive phenomenon, either by the government or mass media.

The lack of consensus among researchers stems precisely from this way of looking at the term. There will be those who believe that cyberterrorism is the Chernobyl Bomb of the 21st century and those who think that the focus on this topic is a social construction. This point brings up an important topic that will be of great use in the last section of this chapter,

which is the securitization discourse. For this, the theory of the Copenhagen School is of extreme importance, since it is the one that has the greatest focus in this regard. The theory will provide resources and a theoretical basis to analyze, from another angle, cyberterrorism.

1. 3. 1. The difference between Cyberterrorism and Hacktivism

There is one concept that is often misinterpreted with cyberterrorism which is Hacktivism, but even though they might share the same grey areas of their definition there are many reasons why they shouldn't be allocated as one thing. Hacktivism was a term coined by scholars to describe the "marriage" of hacking with political activism. Unlike hacktivists, hackers tend not to have a political agenda. UNODC has described hacktivism as

> "the intentional access to systems, websites, and/or data without authorization or having exceeded authorized access, and/or the intentional interference with the functioning and/or accessibility of systems, websites, and data without authorization or having exceeded authorized access, in order to effect social or political change" (UNODC, 2019)
>
> The organization also signaled that how legitimate are the attacks can still vary depending on the point of view (UNODC, 2019).

Hacktivists have four main weapons at their disposal: virtual blockades, email attacks, hacking, computer break-ins, and computer viruses and worms. A virtual blockade is the virtual version of a physical sit-it blockade, this political activist will visit a website and attempt to generate so much traffic to congest the navigation for other users. By doing this the group is winning publicity, via media reports and winning attention for their cause, which they are protesting. Another term for that would be "swarming" which is when those large numbers of individuals simultaneously access a website and cause it to collapse. Email attacks will be related to "email bombing", where hacktivists will "bomb" the target with thousands of messages at once, which potentially will clog the system. The group has then a card to play, potentially using to achieve goals by threatening (WEIMANN, 2004).

The third weapon those groups have in their arsenal will help them achieve restricted information, communication facilities, financial information, and so on. The high rate of these types of events shows that cyber-attacks happened together with the growing popularity of the internet at the end of the last century. By then, and even today, there are a vast number of vulnerable targets that hacktivist use to claim attention and even to promote how easy hacking tools can be.

The fourth weapon relates to viruses and worms, which are forms of malicious code that can infect computers and propagate over the network. Even though they are harmless to the human eye, their impacts can be enormous. In 2000, sites like Amazon, e-Bay, and Yahoo were stopped for several hours due to a DoS attack. In 2002, the Washing Post reported that the internet had just experienced the largest and most sophisticated attack ever existed.

Although politically motivated, hacktivism does not amount to cyberterrorism. The hacktivists want to protest and bring awareness to their cause, however, they do not intend to kill or warm, or terrify a population. Hacktivism can be seen as an example of why cyberterrorism needs to be taken seriously, and be a highlighted threat to governments and entities. Once, the possibility that any individual, with no moral restraint, can use similar methods to cause terror is a threat. It is very important to highlight that, yes, there can be a very thin line between the two, and sometimes the definition of both cab blur, especially in cases where terrorist groups will use the internet to recruit and hire those hacktivists, or when they will decide to escalate their actions by attacking systems that are critical for the national infrastructure. When this is done, the act can already be considered by some as an act of cyberterrorism (WEIMANN, 2004).

It is fair to mention that, by the beginning of the century, the mass media didn't do a great job of distinguishing between the two terms. Many were examples in each the media was boosting around the cyber events and if we look back, some might not describe it as cyberterrorism. This was the main reason why authors such as Weimann and Soesanto used their influence to alert the public that the threat of cyberwar existed, but at the time, many things were exaggerated. However, as mentioned here, following the same idea other scholars went against this and did not like the use of the word "exaggeration" in the same sentence as cyberterrorism (SOESANTO,2020).

To bring light to the case, and a possible example of hacktivism, the group Anonymous can be a good fit. In 2012, the group, a non-state actor, perform an attack where its members hacked several hundred websites and published information on thousands of Israeli government officials as a response to Israeli efforts to shut down the internet in the Gaza Strip. This was the message they shared (see the image below). The act was not well received by the Israeli government, which declared to be the country was also waging war on a cyberspace level. As mentioned here before, hacktivist attacks tend to bring attention to a more social or humanitarian agenda, which doesn't occur in cyberterrorism groups, being this one of the biggest differences between the two (GUNNERIUSSON and OTTIS, 2013).

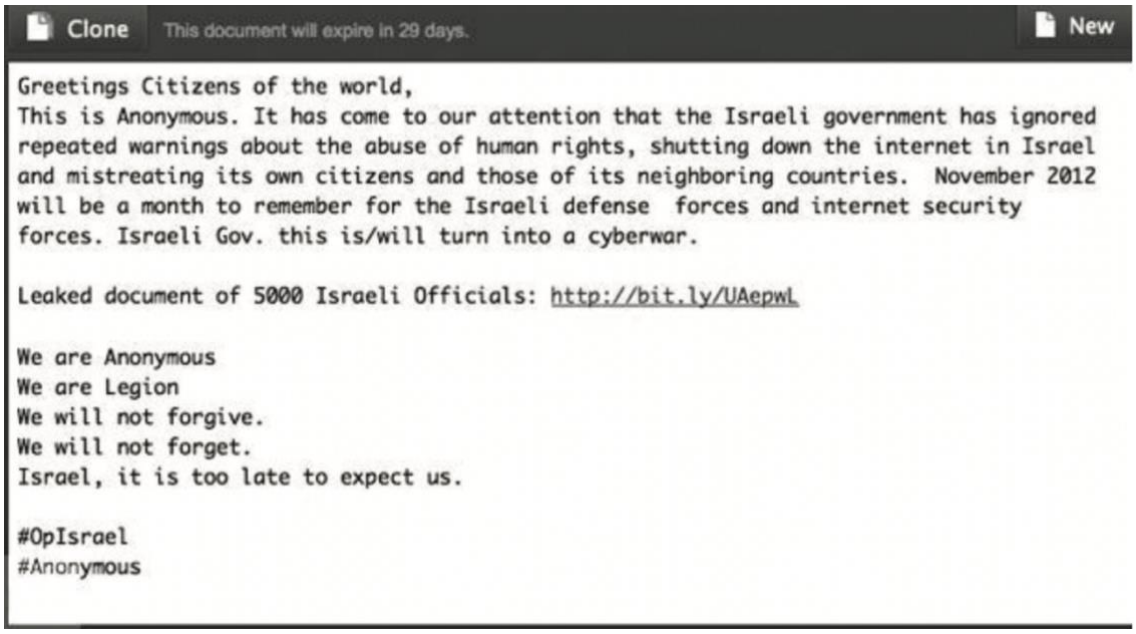

Figure 1: Message from hacktivist group Anonymous (2012)

1.4. How do International actors see Cyberterrorism?

In the same way, it is important to approach how researchers comprehended the term and definition of cyberterrorism it is also very important to gather how the biggest International Relations actors reacted and reflected such a threat. Some organizations took more time to start adding in their agenda the word "cyber", regardless of what would come after the name: cyber-attack, cyberterrorism, cyber war, and so on. With time a certain expectation came along so that those important organizations would too share their thoughts on how to describe cyberterrorism.

For obvious reasons the USA was the one country that spent budget and time on understanding the different variables of the cyber world and how it has come to be used as a tool of power and terror by criminal organizations. The US Defense Intelligence Agency spent some time with some studies at the end of 1999, to comprehend "cyberterror". In their report, they excluded some activities as an example of cyberterrorism, as mentioned here before. , such as scrip kiddie techniques, spoofed emails, and bombardment of email inboxes. The upcoming, at the time, was the definition here presented before cyberterrorism is the unlawful destruction of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious, or ideological. Nonetheless, after 9/11 the US government stood differently concerning the whole cyber threat. As a reaction to the

event, the US Patriot Act of 2001 and the Terrorism Risk Insurance Act of 2002 provided law enforcement with new tools to detect and prevent terrorism, as mentioned:

> "authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses" (Section 202), "emergency disclosure of electronic communications to protect life and limb" (Section 212), and "interception of computer trespasser communications" (Section 217) (BOGDANOSKI and PETRESKI, 2013).
>
> This act also included as their definition the cyber part concerning a terrorist attack.

But, according to the Department of Justice in the 2005 Report, section 202, there are only a few occasions in which this federal law was induced, not for a cyberterrorist attack but a case of drug trafficking. Since then, the US and its departments changed their approach to cyberterrorism and the topic was more frequently seen in its agenda of security.

What concerns European grounds the European Commission adopted a provision that all members of the European Union would have to consider cyberterrorism if any "attack through interference with information systems" would occur and with the intentional goal of "serious alteration or destruction of political, economic or social structures". These actions were part of the mission to establish the wanted level across Europe to define the term "terrorist crime". As an example, Germany's government cuts the limits under monitoring telephone calls, emails, and bank accounts, and also restored a previous limitation that existed between the Secret Service and the police. The United Kingdom, with the excuse to counter-terrorism, tried to (relax) regulations so all local and national government agencies would be able to access data communication traffic without the need for a warrant (BOGDANOSKI and PETRESKI, 2013).

The Organization for Security and Co-operation in Europe (OSCE) increased its attention to the matter. By the first decade of the century, OSCE Ministerial Council started to make its definition of cyber-attacks finer. They added that the extended use of the internet by the terrorist organization should be also considered a part of the attack, as examples, they explained the activities those groups do to recruit new followers and the propaganda they perform to achieve faster their goals. Following those measurements, the OSCE also salient expressed their desire to make greater cooperation and effort to protect "vital critical information infrastructures and networks from the threat of cyberterrorism" (OSCE, 2022).

The member countries were asked to closely monitor the web pages of terrorist organizations and to be constantly exchanging information with other governments in the OSCE and other relevant forums. Another point brought to the table was the civilian institutions' participation together with the private sector in preventing and countering the

use of the internet for terrorist purposes. In 2008, the Estonian Defense Minister, Jaak Asviksoo expressed how far society still was from being completely secure against cyber-attacks, and there was still a lot of work to be done and also mentioned "Yesterday, NATO defense ministers in Brussels commonly agreed that urgent work is needed to enhance the ability to protect information systems of critical importance to the Alliance. I think that this is definitely a step towards the right direction" reaffirming the need for international cooperation (AAVIKSOO, 2008)

The council of Europe (CoE) was an important actor in the awareness of cybersecurity. In 2001 happened the Convention on Cybercrime which was the first step for many countries to start debating cybersecurity. The Convention was signed by 46 countries, until 2004, however only 26 ratified it. It was so important because it brought to light many aspects between those countries, including the detailing of what were the illegal activities and practices that featured across the umbrella of cyber security threats; the establishment of common standards and procedures binding all the countries that signed. Being used as a guideline and instrument for the signatures' and even non-signatures countries, to start adapting their national legislation (BOGDANOSKI and PETRESKI, 2013).

Another important organization, The United Nations (UN), always had as one of its main subjects' cyber security, especially in the debates about security policies in the UN system. The problem is always addressed in the debates related to the threat of terrorism and the form of the Resolutions of the UN Security Council. It is treated as a part of the Counter-Terrorism Committee established by the Security Council, and it is mentioned in the UN Global Counter-Terrorism Strategy.

In the UN's agenda, the theme does not only appear as a counter-terrorism strategy against all forms and manifestations on the internet, but rather a more active approach to the use of the internet itself as a tool for countering the spread of terrorism. The UN sees cyber security as a central feature that will be constantly developed in the international agenda for international security purposes.

Now regarding the North Atlantic Treaty Organization (NATO) response to cyberterrorism? As mentioned in the introduction part of the project, NATO is one of the points of analysis here presented. Understanding how NATO sees, comprehends, and responds to cyberterrorism is crucial to analyze how countries that are part of the organization are oriented to react and how other countries don't, in this case, Estonia and Iran.

By many, NATO's way of treating cyber threats is very experienced and mature. For years the topic is being discussed on NATO's tables, with the attempt to transform the military organization and conduct of operations by "networking-oriented warfare" and "network-enabled capabilities". In 2002 happened the Prague Summit, in which many initiatives started. For example, the new NATO Cyberterrorism program which involved many NATO bodies was described as the first line of defense against cyberterrorism. In 2007, the following events that occurred in Estonia changed completely how NATO responded to those threats, the development and aftermath of the events will be more detailed described, and examined in the next chapter of this project (BOGDANOSKI and PETRESKI, 2013).

1.5. What are hybrid threats and how is it understood in nowadays society?

Cyberterrorism and its many manifestations are considered to be an example of, what is today known as, Hybrid Threats. A term that first started its appearance back at the beginning of the XXI century and had other labels being used interchangeably to the phenomenon, such as hybrid warfare/war, "new wars", fourth-generation warfare, or asymmetric warfare (GIANNOPOULOS et al., 2021). The conceptualization of this phenomenon is important to understand more deeply the premises of cyberterrorism, and how it fits into the term.

Frank Hoffman is considered to be the father of hybrid warfare concept and first used to term in 2005, in one of his articles, with James Mattis. They argued, "in Hybrid Wars we can expect to simultaneously deal with the fall out of a failed state that owned but lost control of some biological agents or missiles while combating an ethnically motivated paramilitary force, and a set of radical terrorists who have now been displaced" (MATTIS and HOFFMAN, 2005). And they also add,

> "we can also expect to face unorthodox attacks or random acts of violence by sympathetic groups of non-state actors against our critical infrastructure or our transportation networks. We may also see other forms of economic war or crippling forms of computer network attacks against military or financial targets" (MATTIS and HOFFMAN, 2005).

Even though the concept has changed over time, Hoffman and Mattis gave a good idea of what these "new wars" meant at the time as a new type of threat to which the military had to adapt. As Berdal has well emphasized "these were being used by analysts to conceptualize changes in contemporary warfare in line with the idea that war had become "substantially distinct" from older patterns or conflict (BERDAL, 2011).

Giannopoulos et al., (2021) in their Hybrid CoE paper describe “the concept of Hybrid Threats, however, is the only one that raises the issue of systemic vulnerabilities of democratic systems as particular targets and argues for comprehensive approach with civil-military cooperation from the very beginning”. All this to also say something quoted here many times, hybrid threats have been increasingly being debated in the academic circles, however, “this does not mean the concept if fully accepted and understood” (GIANNOPOULOS et al., 2021).

Hybrid Threats and warfare were also used in the political context which first started with the annexation of Crimea in 2014. The political use of Hybrid Threats refers to the manipulative, unwanted interference through a set of tools: “spread of disinformation/misinformation, creating of strong (but incorrect or only partially correct) historical narratives, election interference, cyber-attacks, economic leverage, to name just a few” (GIANNOPOULOS et al., 2021). Since the threats will be characterized as a combination of actions, some academic analyses will mention that one action alone cannot be defined precisely as an active hybrid, and sometimes even the threat aspect will be questioned. But, in the end, they will all belong to the landscape of Hybrid Threats (GIANNOPOULOS et al., 2021).

But some other scholars will debate if the use and application of a “hybrid threat” label is beneficial for politics or strategies, as mentioned by Mikael Wigell

> “many scholars and analysts contest the utility of the hybrid label, criticizing it for conveying little that is new, for being imprecise or outright misleading. When coupled with the term “warfare”, critics warn, there is the danger of unnecessarily militarizing the language of international politics with potentially dangerous consequences” (WIGELL, 2019)

However, Giannopoulos et al (2021), describe in great words that the Hybrid Threats concept does not seek to explain policy or strategy, or even analyze capabilities. The concept's main objective is to characterize Hybrid Threats as a multiplier force and/or a coercion tactic used to support a strategy or a policy that so far didn’t deliver the desired outcomes (GIANNOPOULOS et al., 2021).

When in Hybrid Warfare, future enemies will exploit access to modern military capabilities, and those can include: encrypted command systems, man-portable air-to-surface missiles, and other modern lethal systems. Hoffman, also includes “states blending high-tech capabilities, like anti-satellite weapons, with terrorism and cyber-warfare directed against financial targets” (HOFFMAN, 2007). The author describes hybrid wars as “polymorphous by their nature” and highlights that they will be conducted by both states

and a variety of non-state actors, finally state his view on the phenomenon: “Hybrid Wars incorporates a range of different models of warfare including conventional capabilities, irregular tactics and formations, terrorists’ acts including indiscriminate violence and coercion, and criminal disorder” (HOFFMAN, 2007).

William J. Nemeth was, also, one of those who started this debate, according to him, the concept of a Hybrid “War” referred to “the hybrid nature of societies, apparently less structured and less socioeconomically developed”. For him, countries that were not as developed would employ hybrid forms of confrontation to make up for their inferiority in fields like politics, economy, technology, and military weapons. With this, using disinformation campaigns and guerrilla tactics that would not comply with international law and the so-called conventional forms of armed confrontation (NEMETH, 2002 apud PEREIRA, 2018).

Håkan Gunneriusson and Rain Ottis (2013), in their paper about “Cyberspace from the Hybrid Threat Perspective” when trying to describe the idea behind this concept, used excellent words “perhaps the best way to put it, the hybrid threat is a manifestation of total war. It is about making the other side submit to one’s will, with any means available” (GUNNERIUSSON and OTTIS, 2013). In other words, the authors define a hybrid threat as a set of factors and actions, which unfold as a total manifestation of war. Hybrid threats cannot be defined by just one type of actor, since they can occur by states, non-state actors, and even individuals. It aims, according to the authors, to make the other side submit to their will through all possible means.

Following this same thought, Andersson and Tardy (2015) state: to understand hybrid threats it is necessary to understand all the points where it diverges from non-hybrid threats. This means, for a threat to be considered "hybrid" it has to be the product of several ways of threatening or attacking its intended target. It is the mixture of different methods, conventional or not, military or non-military of attacking to achieve an intended goal (ANDERSSON and TARDY, 2015).

These hybrid threats are mainly the result of the rapid technological development of the last decades, which has provided a new type of more elaborate and often silent threat (DETLEFSEN, 2015). Gunneriusson and Ottis would also add that hybrid threats tend to target civil society rather than the military, making it sense why cyberterrorism is considered one of those Hybrid Threats (GUNNERIUSSON and OTTIS, 2013).

Following this argument, the two authors elaborate on how they see cyberspace overlapping the hybrid threat parameters. For them, convergence can happen in three ways,

with many examples: first, cyber capabilities would support conventional forces. Second, as an asymmetric and irregular attack on its own. Third, as an enabler or disabler of events and social movements. With this, it is interesting to present each of these aspects and their examples, which, above all, present more possibilities for cyberterrorism to happen (GUNNERIUSSON and OTTIS, 2013)

As concerns the "supporting conventional forces" they start saying that at some point in time cyber capabilities will be considered as part of the conventional toolkit in an offensive environment, even though at the moment they are still very rare in military combat operations. The slightest presence of an offensive cyber operation during a military time will, therefore, be considered "hybrid" or "unconventional". Possible examples of a cyber operation include sensors, computer-controlled systems (drones, guided missiles, etc) command, control, and logistics systems (GUNNERIUSSON and OTTIS, 2013).

Since, to remotely control drones operating in air, land, sea, or space, you will need a computer and their network to function, those activities will fall into the domain of cyber-attacks. A similar example happened in 2011 when Iran was able to manipulate a US drone to land in Iran, performing what was called a "hijack of the drone". This episode brought up much speculation about how it occurred, and it is believed that it involved jamming the control signal, so that the drone would be forced to go into autopilot mode, and faking the GPS so the drone would have wrong coordinates and land in a different location (GUNNERIUSSON and OTTIS, 2013).

However, as Gunneriusson and Ottis highlighted, cyberterrorism when facing the modern military won't rely on a majority in operating drones or other tactical weapon systems, they will rather focus on what the military heavily depends on, which is the logistics and communication systems. Besides the fact that those systems are much more vulnerable to a cyber-attack, they most likely have very important data that can be used in many ways by the terrorist groups that perform the attack. For example, by attacking a major logistics hub like a port, the cyberterrorist would scramble the data in a way the entity cannot restore it and won't be able to know which container is where, what is in that container, who is the owner of that goods, and when they need it, for example. The attack would perform chaos, and impact many parties. That is why the authors strongly defend that the military must be able to protect their systems from those possible cyber-attacks (GUNNERIUSSON and OTTIS, 2013).

As for non-military targets, those can be considered the ones that can more cause chaos or terror, depending what is the objective of the terrorist group. For example, attacking

a civilian infrastructure can cause civil unrest or a mass evacuation in the area it happened. An obvious example of the target would be a Critical Information Infrastructure system, known as CII. Attacks on CII will happen especially if an actor wants to influence a state or a population. Since nowadays society is very dependent on CII, which are information systems that sustain today's way of life, those become very big targets once they have been more automated with time to increase efficiency. And another factor that increases the chances is the very fragile security systems they have, with this, the systems that are used to control power grids, water treatment plants, air traffic control, and banks can sometimes be easy targets (GUNNERIUSSON and OTTIS, 2013).

A great example is the Stuxnet case, which is one of the two study cases here analysed. This is because, when a CII attack is successful can cause serious harm to human life, infrastructures, the economy, ecology, and other areas. Stuxnet was a case that could bring great damage if it succeeded, and an example of cyberterrorism that can cause physical damage. More details and information will be explored later in the second chapter of this project.

Other types of CII can also be targeted since Programmable Logic Controllers (PLCs) are used everywhere from elevators to nuclear power plants. But it is also necessary to know that not always physical damage will be sought, there are other forms of attacks on CII that can have a serious outcome. Take for example an attack against the banking sector that leads to bank runs, causing an economic problem for a state, sometimes more costly than a bomb (GUNNERIUSSON and OTTIS, 2013).

The authors as well draw attention to one fact that is well-known in human daily life: the fact every day more and more life gets entangled with information technology empowering services and devices. As an example, a smartphone has access to the owner's location, schedules, contacts, sometimes passwords, and bank details. Or even, the medical devices that are surgically implanted into people - like pacemakers, insulin pumps, etc. Some researchers did experiments to see if they could remotely manipulate those devices, and cause any harm to the person wearing them. They found out, on their lab conditions, that one can manipulate such devices if they want. (GUNNERIUSSON and OTTIS, 2013).

Those examples help clarify why a hybrid threat actor would consider using cyberspace conditions to create an offensive situation with non-military targets. There is an ongoing list of potential victims and many ways to achieve their ends. Unfortunately, many CII will have an unsecured system making them a potential target to some groups, this being

said, the military of a country should be ready to provide any type of assistance in case of crises in any CII. (GUNNERIUSSON and OTTIS, 2013).

The third reason, according to the two writers, to consider cyberspace from the hybrid threat perspective is that it offers new ways of achieving goals that normally are very expensive or complicated. The internet made possible global communication, wherever the other part is located in the world. Take the Arab Spring, as an example, cyberspace did not motivate the events but was a very important tool to achieve the aimed consequences. On one side, you had people using the internet to gather and share information about the current situation, and the government and to self-organize using social media and messaging tools. On the other, many governments tried to limit access to the internet or specific services to regain control and quell the riots (GUNNERIUSSON and OTTIS, 2013).

The main and biggest reason why cyberspace, and thus, cyberterrorism is so appealing to some groups is that the internet provides accessible, cheap, free, and anonymous ways to spread information, propaganda, recruit people, share materials plan, and coordinate attacks. And, sometimes, not only terrorists or hacktivists will be enjoying cyberspace, but in many situations will be States taking advantage of this environment. Intelligence agencies are actively monitoring the internet with the excuse of national security. To conclude their thoughts, Gunneriusson and Ottis state that "the old definition of hybrid threats that non-state actors wield state actor capabilities seems to be in reverse here, as state actors try to masquerade as non-state actors" and they add that in their opinion national security implications of cyberspace are growing, and many states are starting to understand that having a counter strategy against cyber-attacks is a necessity in today's world. (GUNNERIUSSON and OTTIS, 2013).

With their study is possible to conclude that Hybrid Threats are a result of contemporary society due to the many aspects of human life being encircled by technology and the internet. The consequence will lead to the bad use of cyberspace, leading to cyber-attacks and cyberterrorism. For the executor, cyberspace enables a free, anonymous space to perceive his goals and achieve a broader audience. As a result, state and non-state actors started to have a more cautious approach regarding hybrid threats and cyberterrorism, hence the many potential targets and many different ways to perform it.

1.6. NATO's point of view

In the same way, cyberterrorism was a present subject on NATO's agenda so were other hybrid threats. Since 2015, NATO has had a strategy in place to counter hybrid warfare and has taken the responsibility to ensure that the Allies and Allies are sufficiently prepared to counter any hybrid attacks regardless of the form they have. The Organization can deter any attack against the Alliance and any other ally that feels threatened. To achieve this intention, NATO continuously keeps gathering, sharing, and assessing information to detect and attribute any occurring hybrid activity. Also, this provides the necessary information so that the Alliance can support the Allies' efforts to identify any vulnerabilities and strengthen their resilience in case any of them request it (NATO, 2022).

For many years, parts and members of NATO worked firmly to find concepts and create realistic counterattacks to those threats. In 2016, NATO described hybrid threats as

> "a broad complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary, and civilian measures, are employed in a highly integrated design by state and non-state actors to achieve their objectives" (NATO, 2016).

Hence upcoming debates about this subject, NATO, together with the EU, created an organization responsible for dealing with hybrid threat topics known as the European Centre of Excellence for Countering Hybrid Threats. The center has spent most of its time attempting to describe the Hybrid Threats phenomenon instead of defining its specific conceptual delimitation. This reality arises due to the phenomenon's complexity, as well as from the multiplicity of actors that may be involved, and because, so far the concept still needs to be sufficiently studied to understand its full scope (HYBRID COE, 2022).

Nonetheless, The European Centre of Excellence for Countering Hybrid Threats did try to define and go deeper into the research regarding hybrid threats. They defined Hybrid Threats as coordinated and synchronized actions deliberately aimed at affecting the vulnerabilities of democratic states and their institutions, employing various political, economic, military, civilian, and intelligence means. The center also adds to its characterization of Hybrid Threats:

- Activities that exploit the thresholds of detection and attribution, as well as the different interfaces (war-peace, internal-external security, local-state, and national-international).
- Activities aimed at influencing different forms of decision-making at the local (regional), state, or institutional level and designed to further and/or fulfill the agent's strategic goals while undermining and/or hurting the target (HYBRID COE, 2022).

Besides the Centre, NATO also installed the Joint Intelligence and Security Division at its headquarters in Brussels, in 2015, to collect, process, and analyze hybrid threat information. The division would function as an information provider so that member nations could benefit from better information and facilitate decision-making in the future. In 2018, a declaration was issued after a meeting with the Heads of State and Government at NATO's headquarters, where it stated the acknowledgment that the biggest part in recognizing hybrid threats would come from each State in their premises; however, NATO would stand ready, upon Council decision, to assist an Ally at any stage of a hybrid campaign (NATO, 2018).

The 21st article of the declaration reads:

> In cases of hybrid warfare, the Council could decide to invoke Article 5 of the Washington Treaty, as in the case of armed attack. We are enhancing our resilience, improving our situational awareness, and strengthening our deterrence and defense posture. We are also expanding the tools at our disposal to address hostile hybrid activities. We announce the establishment of Counter Hybrid Support Teams, which provide tailored, targeted assistance to Allies, upon their request, in preparing for and responding to hybrid activities. We will continue to support our partners as they strengthen their resilience in the face of hybrid challenges (NATO, 2018).

In this declaration, NATO provides its member with a set of collaboration strategies and mechanisms to help each state increase expertise in the matter. They would support the countries to I) prepare effective responses to any accident that would involve chemical, biological, radiological, or nuclear weapons, II) protect critical infrastructures, III) develop modern and strategic communication with the Alliance, IV) protect their civilian population, V) defend their cyberspace or energy institutions, and VI) combat terrorism (NATO, 2018).

NATO would also give formation, training, and capacity to member states to react in case of a hybrid threat attack, including military and non-military response mechanisms, and the potential cooperation with other entities such as the EU, for example. This gives a strong signal that the Alliance improved both political and military responsiveness and its ability to deploy the necessary forces to the right place at the right time (NATO, 2022).

1.7. How does Copenhagen School analyze Cyberterrorism?

Now, after the overview on where cyberterrorism is allocated was presented and why it is considered to be an example of a hybrid threat, and also, after exploring how the International actors see this problem, it is possible to analyze how the Copenhagen School and its theory of securitization understand and address the problems surrounding the cyber threats. Normatively, Securities Studies will engage in the conceptualization of securities that are mobilized in the political discourses of countries, such as environmental, health, or cyber security. However, despite widespread references to cyber insecurities in political, media, and IT discourses, there has been surprisingly little explicit discussion within Security Studies. This sector of the chapter seeks to understand why there is a gap between the Securities Studies led by the Copenhagen School and the cyber threats, and especially, regarding its Securitization Theory (HANSEN and NISSENBAUM, 2009).

Since the 1980s, the Copenhagen School has been a point of reference on the issues and debates within Security Studies. Strongly known for its concepts of securitization and social security, it has been applied to numerous empirical contexts including diverse security topics, e.g. ethnic conflicts or trafficking. More importantly, became the stage for discussions about the normative implications of security discourse, the consequences of speech act epistemology, the Westend-centric status of security, and the importance of the media and visual representations in theoretical debates (HANSEN and NISSENBAUM, 2009).

The two notable names of this school are Barry Buzan and Ole Waever and have three main theoretical roots: one concerning the debates in Securities Studies and whether is applicable to widen the concept beyond its traditional state-centric and military focus; another in speech act theory, and another in a classical Schmittian understanding of the state and security politics (WILLIAMS, 2003). When combining these three influences, the general concept of security is drawn from its regular national security discourse, implying a

emphasis on authority, confronting threats and enemies, the ability to make decisions, and the adoption of emergency measures (HANSEN and NISSENBAUM, 2009). Security will then have a particular discursive and political force that will securitize conditions.

And within this, Buzan, Waever and Wilde, (1997) delineate their idea “Thus, the exact definition and criteria of securitization are constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects” (BUZAN, et al., 1997). To say the word “security” would then mean something as threatening and in need of an urgent response, rather “securitization” would need further study of the discourse. Security will frame issues either as a “special kind of politics” or as above politics, this means that public issues will whether be nonpoliticized (the state does not deal with the matter, and it is not made as a public debate) or politicized (the issue is part of public policy, the government will need to take decisions on the matter) or even, “securitization” (when a problem or threat is no longer debated as a political question but dealt with an accelerated pace and in ways that may violate normal legal and social rules (BUZAN et al., 1997).

In this way, the securitization model will be defined as the state that demands threat-urgency, and can, according to the Copenhagen School, constitute as well, other types of objects rather than the state/nation and bring in, other sectors than the military. But this will happen as long as there is “drama” and saliency of national and international security and it is accepted by the relevant audience HANSEN and NISSENBAUM, 2009).

The theory of securitization, then, has its premises in the power of speech, which states do to their populations. Thus, this extension led to a theory of "social security" where "the ability of a society to persist in its essential character under conditions of change and possible or actual threats," is an expansion that allowed for the identification of security problems where national, religious, ethnic, or racial groups feel threatened rather than protected by "their" state (WAEVER, BUZAN, KELSTRUP and LEMAITRE, 1993) The factor of urgency and extreme measures is thus central to the Copenhagen School’s delineation of the boundary between ‘‘security proper’’ and concepts that bear only a semantic semblance to ‘‘security’’ (HANSEN and NISSENBAUM, 2009).

As for how threats are understood in securitization theory,

> In security discourse, an issue is dramatized and presented as an issue of supreme priority; thus, by labeling it as a security, an agent claims a need for and a right to treat it by extraordinary means. For the analyst to gasp this act, the task is not to assess some objective threats that “really” endanger some objective to be defended or secured; rather, it is to understand the processes of constructing a shared

> understanding of what is to be considered and collectively responded to as a threat (...) The securitization approach servers to underline the responsibility of talking security, the responsibility of actors as well as analysts who choose to frame an issue as a security issue. They cannot hide behind the claim that anything in itself constitutes a security issue (BUZAN et al. 1997; WAEVER, 1995).

The Copenhagen school tends to assume that the connotations of security are givens (existential threats requiring emergency measures) and that only the threats and the core values of security are variables. But, Bendrath et al, (2007) for example, inquire that not all threats frames will fall into a life-and-death category of existential threats, and big "hard power" measures that would be applied in democratic procedures are not always legitimized by certain threat frames (BENDRATH et al, 2007).

It can be understood that the Copenhagen School argues that security is a speech act that securitizes, that is constitutes one or more reference objects, historically the nation or the state, as threatening to their physical or ideational survival and therefore in urgent need of protection (WAEVER, 1995); (BUZAN et al., 1997). The School has dealt with cyber security, in the past, and considered it as an example of an attempted securitization that is ruled out on the grounds that it has "no cascading effects on other security issues" (BUZAN et al., 1997). With this, 1998, in one of its seminars studies, stated that "there is no need to theorize cyber security as a distinct sector akin to the military, the political, the environmental, the societal, the economic and the religious ones" (BUZAN et al., 1997). But since then, much has changed regarding cyber threats, and cyberterrorism, including examples of securitization speeches done by States and International Actors on the matter (HANSEN and NISSENBAUM, 2009).

Cyber security has been securitized, via "speech acts", by President Clinton in 1996, when establishing the Commission on Critical Infrastructure Protection and by locating cyber security within the Department of Homeland security. Also, by President Bush's formulation of the "National Strategy to Secure Cyberspace" in 2003, and finally by NATO with the creation of a backed cyber defense center after the Estonian events in 2007, analyzed in this same paper. All this to say, cybersecurity shouldn't be held together with other sectors of security, and, should be identified and allocated as a particular sector on the broader terrain of Security Studies, more precisely, by the Copenhagen Schools and its securitization theory just presented here (HANSEN and NISSENBAUM, 2009).

Following the same paths as the definitions of cyberterrorism, one also finds disagreement about this securitization agenda. There will be authors such as Eriksson and Giacomello, (2007) who will recognize cyberterrorist agendas but will question whether all

examples should be characterized in the same way. And there will be authors, such as Hansen and Nissenbaum, (2009) who believe that security theories such as the Copenhagen School, should adapt to the current conjuncture. The last section of this project will try to analyze how the non-consensus of the term cyberterrorism modifies the reactions of actors, and how the securitization theory can be a theoretical support to show this difference in discourse.

2. The Estonian and the Iranian Cases

In order to achieve any of the proposed hypotheses and to perform the wished analysis, it is necessary to explain the two case studies examined in this work. The choice of the two cases was made given the objective of analyzing how a NATO member country and a non-member country behaved during and after a cyberattack. There are not many examples of cyber-attacks that have occurred against whole nations so far, however, the cases of Estonia and Iran are great examples as they fit the profile seen here and both demonstrate the abilities of cyber-attacks against nations. Since Estonia is a NATO member state and Iran is not, it is possible to analyze behaviors, containment strategies, and responses that were understood after the events, between the two countries, and how being part of such an organization can differentiate counter activities.

In this following chapter, you will be able to understand how the two cases occurred, what escalate them, what was the response of each country, and once it was finished, how the countries reacted to the attacks. First, it will be presented the case in Estonia, together with NATO's reaction to the event and how the organization defines cyberterrorism. After this, the Iranian case will be described following their aftermath reaction. Once the overview was presented it will be possible to develop a debate about a comparison between the two cases given the whole theoretical arsenal that has already been raised in the previous chapter.

2.1. The Estonian Case

In 2007, Estonia a European country and EU member, known to be one of the most technologically advanced countries in the world, experienced a cyberterrorism attack that lasted 22 days, and target many governmental and private institutions. The cyber-attacks lasted from 27th April to 18th May of 2007. But all the fuss started some days before as the Estonian Government announced plans to move a monument located in the city center of Tallinn to a military cemetery located downtown. The relocation would follow the plans to celebrate those who died in the Soviet Union war (OTTIS, 2008).

The monument in question was a Soviet-Era statue depicting a Soviet soldier originally built in 1947 when the major affairs In the Socialist Soviet Republic of Estonia were still controlled by Stalin. The monument was known as "Monument to the Fallen in the Second World War" and was located at the burial area of Soviet troops who died while invading Tallin in World War II. The statue portrayed an unnamed soldier, that was wearing a uniform of the Red Army, holding his helmet in the left hand, slightly bowing his hand over his nearly 11 million fallen comrades, as a gesture of respect for the deceased. When in 1991, Estonia regained its full political sovereignty, this monument became a point of conflict in the domestic affairs of the country. (OTTIS, 2008).

The statue has always carried two different feelings from those who lived in Tallinn. For the Estonias, the monument represented the oppressor, the one who came to conquer their country and obstruct Estonian independence. And for the minority, local Russians would represent the "liberator", a site where different interpretations of the Red Army's role were expressed in demonstrations and a place where veterans of the Soviet armed forces would meet on civic holidays. Due to this, over the past few years, the statue became a point of tension between pro-Kremlin and Estonian nationalist movements (SCHMIDT, 2013).

Aiming to avoid any other tension regarding the statue, and to relocate the war dead to a more peaceful resting place, the Estonian government used the argument to move it, and place it in a military cemetery in Tallinn. This announcement didn't go unnoticed by Moscow, which didn't appreciate the fact that its former Soviet Republic was aiming to cut ties with its WWII and post-war history. In January 2007, the Russian government filed a resolution in order to demand that Estonian congressmen would halt the law allowing the removal of the statue (SCHMIDT, 2013).

The work began on the 26th of April, where they fenced off the statute in the center of Tallinn, removed it, and exhumed the bodies of the Red Army soldiers that were buried underneath it, transferring everything to the military cemetery. Some mostly non-violent protests started at the site after the Russian government took a stand against it, moving Russians, the ethnic minority of Estonia, and citizens of the Russian Federation. However, the circumstances changed in the evening when a much more violent crowd emerged, and riots started. Stores were vandalized, cars were burned and one person was stabbed and passed away (OTTIS, 2008; RUUS, 2008).

Following this scenario, the 27th of April marked the day the cyber-attacks started. They were targeting Estonian internet information systems, both governmental and private. The attacks, known as Distributed Denial of Service (DDoS) flooded the computer systems

with more connections than the network could handle, and the systems started to appear unresponsive to the public. The methods that were used are well known, including ping flood, UDP flood, malformed web queries, email spam, and others. A DDoS is not difficult to be performed and can be considered easy to execute, but it tends to require a large number of computers that are being coordinated by many people or botnets, to achieve the big results that the Estonian government faced. (OTTIS, 2008; RUUS, 2008).

Once it was understood that this type of attack couldn't happen without some type of greater coordination, speculations started to appear. They found out that the vast majority of the malicious traffic came from outside Estonia. This traffic contained clear indications of political motivation and a clear indication that came from Russian servers. Instructions for the attacks were found using Russian language forums and websites. They would include motivation, where to target, the timing, and more information on how to proceed with the attacks. You can see in the picture below a copy of an email that circulated between forums (OTTIS, 2008; RUUS, 2008).

The cyber-attacks, coincided with physical street riots involving thousands of ethnic Russians living in Estonia, together with the Russian government, arguing this situation was blasphemy (DETLEFSEN, 2015). May 9th marked an important day for the attacks because this was when Russians celebrated victory over Nazi Germany. On many websites and forums, you were able to find propaganda similar to the previous example, where the organizers were calling the sympathizers to attack again on that important political date (OTTIS, 2008).

As mentioned before, much of the malicious traffic originated from outside the country, so to combat this at some point, some banks cut off all their foreign traffic, temporarily, while remaining accessible to their clients inside Estonia. This strategy was one of many to avoid greater damage. The attacks can be considered economical as well, hence the trade relationship between the two countries deteriorated.

Aside from the attacks and the riots that were taking place simultaneously, another event marked these days. At the Estonian embassy in Moscow, youth groups were gathering in front of the embassy and preventing Estonian workers to enter or exit the building, including diplomats. The climax came when on the 2nd of May the Estonian ambassador was physically attacked during a press conference. Most of this news was not being reported by Russian Media, and if so, it was being reproduced as "peaceful" protests. (RUUS, 2008).

It is very important to highlight that Estonia, by then, and until now, is a highly networked country, which means that an attack with the characteristic that happen in 2007,

targeting public digital services, has a significant impact on the daily lives of ordinary citizens and businesses. The Estonian government issues electronic identity cards that enable each citizen to perform daily tasks that impact their lives, such as voting, paying taxes, paying parking meters or bus fares, or even viewing their children's grades online. Another proof of how Estonia was technologically advanced was the accomplishment Estonian computer programmers achieved by inventing Skype software (RUUS, 2008). Therefore, as Ottis mentioned in his report, the cyber-attacks the Estonian government faced can not be disregarded as a mere disturbance, but should be considered a threat to national security hence the fact the country was highly dependent on the internet and information technology (OTTIS, 2008).

Eventually, during the attacks, the Estonian Computer Emergency Readiness Team (CERT) developed tree steps strategy to contain the problems the attacks caused. The first was to increase their server capacity so that their system could handle more traffic. The second was to develop a filtering system to distinguish the malicious messages from the good ones, that were associated with the attacks. The third was to work with authorities to identify the botnets that were used during the attacks. Accordingly, in May 2007, the Estonian State Procurature made a formal request so an investigation was properly run to find out those responsible for the attacks. The request was sent to the Russian Supreme Procurature, however by January 2008, no response was yet identified (OTTIS, 2008).

Only by 2009, a member of the Kremlin's official movement, known as Nashi, claimed to be responsible for the attacks that happened in the Spring of 2007. According to the New Your Times, the group Nashi ("ours") is the largest of a handful of youth movements created by Mr. Putin's Kremlin to fight for the hearts and minds of Russia's young people in schools, on the airwaves and, if necessary, on the streets" (SHACHTMAN, 2009). However, what is most intriguing is the fact that even though there was a Nashi's involvement, a State Duma member claiming responsibility, and a failure to prosecute those who claimed some or any credit for the attacks, the Russian government denied responsibility all the way. Because many Estonian forensic investigators were finding proof that could be linked to Russia's involvement in the attacks, Russian security officials started to speculate that attackers could have taken advantage of the Russian Internet Protocol and used it to perform the attacks (DETLEFSEN, 2015).

The attacks were politically motivated. Many of the found messages were related to the overall conflict regarding the statute. High-rank Russian politicians openly expressed hostile rhetoric that was published in the media and propagated further in forums and web

portals. In some of these forums were found open discussions about Estonian Systems and how to attack them, as well as, collecting resources to rent botnets that would be used. The connections between the attacks and Russia are many, and the denial that came from the government seems misplaced (OTTIS, 2008).

The spark for the conflict can be related to Estonian identity, its relation with Russia, and its perception of the World War II period. Both nations saw the period with different eyes. For the Russians, it represented the defeat of the German war machine, which cost the lives of almost 27 million Soviet citizens who fought to uproot the Nazis from those lands. But in Estonian eyes, the defeat of the Nazis only gave way to five decades of another occupation, the Soviet one, which continued, as did the previous ones, to suppress the country, which longed for independence (SCHIMIDT, 2013).

There are many theories and speculations surrounding the reason why the attacks happened, what were the intentions of the attackers when they orchestrated the tactic, and what was the expected outcome of the events. The chances of Russia being involved are high, first because of the many indications pointing to Russian servers as the executors of the attacks, and second due to their point-of-view they expressed when finding out the Estonian desire to move the statute and all the consequences that this would implicate. Some of the reasons that may have intrigued the events will be explained in the next chapter.

2.2. How NATO perceives cyberterrorism and possible motivations for the attack

That might be those who can consider the Estonian case as just a cyber-attack, not showing a type of physical threat to the population. However, as presented, the attack was orchestrated together with physical manifestations and some people were hurt. Despite this fact, the attacks did compromise Estonian communication with the international and impacted badly the economy and social environment in the country. There's a development of new terrorist capabilities, provided by modern technology, also acknowledge as Hybrid Threats. It was earlier presented how NATO sees and defines the concept, and now, after this overview of the attacks suffered by the Estonian government, it is relevant to indicate how the organization defines Cyberterrorism, a form of hybrid threat (TIKK, KASHA and VIHUL, 2010).

NATO, being an important actor in International Relations, had been long familiar with the many threats the misuse of information technology can develop. For years now,

NATO is involved in efforts, together with other actors, to standardize the conduct of operations and military involvement when talking about "networking-oriented warfare" or "network capabilities". In 2002, at the Prague Summit, NATO leaders took the decision of strengthening their capabilities regarding their defense against cyber-attacks. This summit resulted in many initiatives (NATO, 2002).

One of them was the NATO Cyberterrorism Program, which involved many parts of the organization, such as NATO's Communication and Information Systems Services Agency (NCSA), NATO INFOSEC Technical Center (NITC), NATO Information Assurance Operations Centre (NIAOC) and NATO Computer Incident Response Capability (NCIRC) (BOGDANOSKI and PETRESKI, 2013) After 2007, NATO's definition of cyberterrorism was "a cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal". This definition was first seen in a NATO document where it could also be written that due to its non-physical nature, an accurate definition of cyberterrorism was not easy to produce (EVERARD, 2008).

Given the fact that became very feasible to exploit many types of vulnerabilities in cyberspace, NATO ministers agreed to outline the cyberspace concept, which was brought in Noordwijk, in October 2008. Later on, this same concept became a NATO Policy on Cyber Defense, which was better developed in a Summit held in Bucharest, in the same year. As a result of this summit, the organization established a Cyber Defence Management Authority (CDMA), to bring together all the keys players in NATO's activities regarding cyber defense, and also facilitate a better management of cyber defense support to any member of the alliance, upon request, in case of a cyber threat. Together with this move, the leaders also agreed with a formal establishment of the NATO Cooperative Cyber Defence Center of Excellence (CCD-COE). CCD-COE was based in Tallin, following the Estonian attack in 2007, and the year after the council granted the Centre "full NATO accreditation" and then gain the status as an International Military Organization (BOGDANOSKI and PETRESKI, 2013).

As for the Centre's mission and vision were described as:

> "enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defense by virtue of education, research and development, lessons learned and consultation" and to be "the main source of expertise in the field of cooperative cyber defense by accumulating, creating, and disseminating knowledge in related matters within NATO, NATO nations and partners" (BOGDANOSKI and PETRESKI, 2013).

Since then, NATO has equipped itself to prevent, mitigate and respond to any type of hostility in cyberspace, building on its respective mandates. For example, NATO has adopted stricter technical criteria for its network and beefed up its Baseline Requirements so that the resilience of critical national infrastructure is ensured. The Alliance and its member have agreed on having a Guide for Strategic Response Options to Significant Malicious Cyber Activities, for those activities that don't rely upon armed conflict. This would create a mechanism for integration with some offensive cyber tools, known as "Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA), that would be used in missions and operations, if necessary. And in 2014, the Alliance reviewed its 2014 Enhanced Cyber Defence Policy (MISSIROLI, 2021).

IN 2016, NATO and the European Union acknowledge the increasing need to identify countering hybrid threats as a priority for cooperation. They then decided to establish a new Centre known as the Hybrid CoE, or Centre of Excellence for Countering Hybrid Threats, the main purpose was to focus on developing resilience and building capabilities to counter Hybrid Threats via research and practical training and exercises with cross-sector participants. The Centre would also allow strengthening the alignment between private and public, civil and military, as well as academic sectors. In 2017, the Joint between the EU and NATO explicitly encouraged their members and allies to support the center. Since then, Hybrid COE has acquired 32 participating states, being Estonia part of the Centre since 2017 (HYBRID COE, 2022).

2.3. The Iranian Case (Stuxnet)

Some may think that the Iranian case is slightly more complex to fully describe since it was the first of its kind and brings to the table many background events that are connected to the cyberattack and the unstable relations between Iran and the USA. In 2010, a Malware program was discovered to be making its way through thousands of computers all around the world, especially in Iran's devices, searching for something very specific. At the time, no one understood the complexity of this computer virus, nor what it was targeting and who were its perpetrators. (BAEZNER and ROBIN, 2017).

The worm was discovered by an Anti-Virus company, called VirusBlokAda, based in Minsk, Belarus. It was Sergey Ulasen who received a complaint from one of his clients in Iran, that his computer would not stop rebooting. At this moment, when making a copy of

the virus to check what was causing the problem, Ulasen was first in contact with Stuxnet. Ulasen realized that the virus was infecting Microsoft's Windows operating system, using a vulnerability never seen before. When a new vulnerability is detected for the first time, is called a "zero day" in the words of computer security. This fact surprised the specialists because its use of a zero-day exploit was not usually found in computer worms (GROSS, 2011) (BAEZNER and ROBIN, 2017).

After the news of a discovery of a new virus that uses zero-day exploit goes public many antivirus and technology people started working hard to investigate the one-of-a-kind malware virus (GROSS, 2011) At this time was still uncertain what was the purpose of the worm, but it was most likely believed to be a spying tool, and its sophistication suggested that many resources were needed to develop it (BAEZNER and ROBIN, 2017).

Stuxnet was the name given to this specific worm, a piece of computer malware, which targets supervisory control and data acquisition (SCADA) systems in industrial controllers. To know exactly how the malware was developed It took several months for the anti-virus maker, Symantec, to determine with more certainty what was this program searching for inside the computers. According to Symantec, the purpose of the worm was to sabotage not to spy. They also proclaimed that the development of the worm would require a great team of programmers, working full-time for at least six months. Stuxnet's size was bigger than other "ordinary" worms, and was written in many different programming languages, together with encrypted components, and did not use one, but four "zero-day" vulnerabilities to infect each computer (BAEZNER and ROBIN, 2017).

At first instance, they found out that the virus was spreading when a USB, that was infected with the virus, would go into a laptop and when entering the machine, it would, surreptitiously, upload two files: a rootkit dropper (a mechanism that allowed the virus perform any type of activity inside the computer) and an injector for a payload of malicious code heavily encrypted. Stuxnet seemed to infect computers working with the Microsoft Windows operating system using one of its vectors. When it found one, the virus used valid driver certificates, more like a digital signature that is legitimate a software program, from RealTek and JMicron to download its rootkit. Those companies were one of the most trusted names in the business making the virus even more sophisticated (BAEZNER and ROBIN, 2017).

Using those driver certificates, the worm could search inside the computer for the Siemens Simatic WinCC/Step-7 software, a program used to control industrial equipment. Once they found and infected the files that were using this software by siemens, the worm

would have access to and control the Programmable Logic Controllers (PLCs), which are tiny computers about the size of a pack of crayons that regulate the machinery in factories, power plants, construction, and engineering projects. PLCs perform very critical detailed work, opening and shutting valves in water pipes, speeding and slowing the spinning of Uranium centrifuges, and meting out a dollop of cream in each cookie, for example. When all these requirements were met, Stuxnet would be able to launch its attack by changing the speed of the centrifuges rotators and causing damage (BAEZNER and ROBIN, 2017).

Later on, started the assumption that the true target of Stuxnet was the Iranian nuclear plan and uranium enrichment site in Natanz (image below) This is because the largest part of the computers that were infected by the virus was situated in Iran. Another possibility was the power plant in Bushehr, but since it enriched plutonium, would require another type of configuration for the centrifuges, not found in Stuxnet. Iran uses a European model of centrifuges from the late 1960s and early 1970s meaning they are not as efficient and can be considered obsolete with nowadays technology, however, due to their status, any type of change in their settings could mean damage or even breakage. The ones creating Stuxnet were aware of this flaw and exploited it (BAEZNER and ROBIN, 2017).

Figure 2: *Satellite image of the Natanz nuclear enrichment plant in Iran taken in 2002*

(Source: DigitalGlobe and Institute for Science and International Security) (ZETTER, 2011).

The nuclear plant of Natanz has air-gapped and a close computer network, which means it does not have an open connection to the internet. The interesting thing about Stuxnet was how well-developed was the virus once in the computer. Since the virus would need someone to introduce it into a computer using a memory stick, it could also enter air gap computers, as was the case, once, inside the computer, it would determine what operations were normal, and record data, that could potentially be used for espionage, but in Stuxnet case, were used as deception information. The virus is also looking to find if that computer has indeed siemens software running, if the answer is no, then the virus becomes useless but if it is yes the worm checks if the machine is connected to a PLC or waits until it is (GROSS, 2011).

Once it is possible, Stuxnet goes from passive to active, using the pre-gathered information to deceive the personnel monitoring the uranium enrichment process so they don't notice what the worm is performing and think all is normal. While the centrifuges are spinning irregularly and tearing themselves apart, the monitoring personnel are unaware of any problem because the virus did the pre-recorded data, that are now showing in their monitor. As a final touch, Stuxnet deletes itself from the system to cover any tracks (DETLEFSEN, 2015).

Other industrial-control systems have been sabotaged before, however, what makes Stuxnet remarkable is the possibility of programming the attack remotely, physically impacting hardware, without needing someone to damage it with his hands. Gross defined Stuxnet as "a self-directed stealth drone". The first known virus that is released into the wild, can seek out a specific target, sabotage it, and hide both existence and its effects until after the damage is done" (GROSS, 2011).

It is not surprising to know many of the people and institutions that were involved in the process of revealing the worm were questioning who was the actor behind such an act. Many antivirus experts claimed that only a state could have developed Stuxnet because of its complexity level, resource investment, and the fact that seemed to be precisely designed to target the uranium centrifuges in Natanz. As mentioned before, many tips pointed to the US, as both countries had a history in place, given the assumptions that Iran was refining uranium to develop a nuclear weapon. Unsurprisingly, the US was very against this, as were Israel and other regional countries that shared frontiers with Iran (DETLEFSEN, 2015; BAEZNER and ROBIN, 2017).

The Iranian government took some time to admit that some of its dependencies were compromised by a computer virus. Iranian officials issued mixed messages, calling the attack not serious while, at the same time, claiming that they had arrested nuclear spies. The country didn't want to report the nature of the attack to its computers, many speculating that the scientists in the country didn't even notice for a time that they were suffering a cyberattack. Only after the news regarding Stuxnet was revealed that they understood what has been going on with their centrifuge's failures. Some analysts estimate that these attack cost months, maybe years, of Iran's nuclear weapon development timeline (DETLEFSEN, 2015).

The pieces of evidence that were claiming the US and Israel to be the perpetrators of Stuxnet are easy to understand. Symantec claimed that they saw shreds of evidence inside the coding lines that could prove Israelian involvement, for example, the presence of the

word “Myrtus” in the code, which was the name of the file where they stored the worm while being developed. This word makes reference to Queen Esther, the one who saved the Jews from a massacre by the Persians in the Bible, and whose name in Hebrew was “myrtle”. Later on, David Sanger shared in the Times suggesting that Stuxnet may have been part of a covert US intelligence operation to sabotage Iran’s nuclear program that started during the government of George W. Bush and was accelerated during Obama's governance (GROSS, 2011). Also, Eugene Kaspersky, founder of the world’s fourth largest company, shared his ideas on whether the US government received some type of assistance from Microsoft to write the program.

2.4. What were the motivations for Stuxnet?

As cited before, Stuxnet and its unfolding are not from unprecedented consequences. The unstable relations between USA and Iran come from 2002, when former president Bush, in his speech, claim North Korea, Iraq, and Iran as an “axis of evil” for seeking to develop weapons of mass destruction, meaning, nuclear and chemical weapons. In this same year, an Iranian rebel group shares that its government is enriching uranium in its nuclear facilities at Natanz. With no surprise, North-America government reacts to this statement by asserting that Iran is indeed trying to produce nuclear weapons. Some months later, the Iranian government admits to be enriching uranium at Natanz, making as a consequence the first visit of the International Atomic Energy Agency to happen, and setting it to happen regularly from now on (BAEZNER and ROBIN, 2017; ECONOMIST, 2002)

In 2006, as mentioned above, the international community started a diplomatic appeal so that Iran stops its nuclear program. However, Iran does not respond positively to these requests, becoming the target of international sanctions. It is to be expected that these events have shaken up relations between the two countries. The so-called “Olympic Games” is believed to have started this same year and intensified during Obama’s administration and, can also be an indication of Israelian participation (BAEZNER and ROBIN, 2017).

Both countries always shared the same view regarding the ambitions Iran had to produce enriched uranium and it is believed that Stuxnet was only one piece of a whole strategy to prevent Iran from achieving its nuclear goals. These operations were not limited to cyberspace and had as other steps, the assassinations of Iranian scientists in 2010 that were also attributed to the USA and Israel. It was also later argued that if the USA had developed Stuxnet, then Israel might have been the one helping the project by providing a testing site with a similar sample to the IR-1 centrifuge (BAEZNER and ROBIN, 2017).

It is also believed that both US and Israel did an agreement where instead of air striking Iranian nuclear facilities, they would perform a cyber-operation, as known as, Stuxnet. Israel throw in the past, airstrikes against Iraq's nuclear program in 1981, and intended to do the same to Iran to enforce its Begin Doctrine of preventing any of its enemies from obtaining nuclear weapons (DETLEFSEN, 2015). Many legal parties categorized the attacks as an illegal "act of force" because they physically destroyed government equipment. But it is also taken into consideration what those three countries have done to each other. Iran was responsible for sponsoring terrorists and insurgents that were responsible for the death of hundreds of Israelis and Americans over the last thirty years, due to the many conflicts they shared.

Other specialists, like Rafal Rohozinski, director of the advanced network research group, and the defense consultant James Farwell speculated that some pieces of circumstantial evidence like parts of the code, the relationship between countries, and the correlations in cyberspace, may suggest that there is a link between the code used by worm and Russian offshore programming community. They still claimed that the USA would still be the main developer, but opened the opportunity for the cybercrime community to have helped with some parts of the code, since it was argued to be many people involved to write such worms (LACHOW, 2014; BAEZNER and ROBIN, 2017).

However, Lachow affirmed that the most difficult part of the attack was not the coding part itself but rather launching the attack, once the computers presented inside the nuclear plants were all air-gapped and they would need someone who would have some type of access. In other words, the attack required very detailed intelligence gathering and planning so the coding would get back to the actual malware. The fact that Stuxnet is a malware very specific, targeting exclusively for the PLCs found in nuclear centrifuges, and those could only be found in two countries in the world: Finland and Iran. This design required very specific knowledge and technical understanding of the interaction of computer systems, industrial control systems, and the Uranium enrichment process. Due to this patchwork of conditions, is hard not to agree that this worm is so targeted-oriented, the multi-stage attack could only be developed by a nation-state or multiple ones (LACHOW, 2014).

Whether US or Israel are the ones involved in the planning of Stuxnet, it cannot be argued that those countries are the ones considered to be beneficial from the attacks. As mentioned, the contrived long shared an opinion against the Iranian plan to become uranium enriched, since the beginning of the XXI century. Both countries had a direct problem with the Middle Eastern country as much as others in the region. However, revelations made by

Wikileaks also pointed out that other Arab Countries in the area felt threatened by a “nuclear Iran”, sometimes “begging” the US to intervene. Other nations that could also be affected by a slowdown in Iranian nuclear production were China and Russia. Finally, it is important as well to take into consideration, the potential desire of one country wanting to frame another as guilty, just to make political tension increase between Iran, Israel, and the USA (LACHOW, 2014).

No doubt that Stuxnet destroyed and damaged a great deal of the equipment used by Iran in its nuclear program, but it did without any death or injury of personnel. Although the attacks started there in 2008, it was only in 2010 that Iranian scientists began to suspect that there was something out of the ordinary. For some time, they believed that the machine failures were nothing more than the wear and tear of time. The reaction of Iranian officials only came to light in 2010, and it was not until 2011 that the country announced the creation of a plan to protect itself against cyber-attacks. It is not known for sure what the precise damage of the attack was, but it is believed that the attack was enough to slow down production and damage some machinery permanently (GROSS, 2011; LACHOW, 2014).

3. The defense approach of two opposing countries toward cyberterrorism

Succeeding these two previous chapters, where a theoretical background was painted and the two study cases were presented, it is time to analyze how those two countries with two different frameworks reacted to the cyber-attacks. One country is a NATO ally and an EU member and the other is an Arab country with customs very different from those of the West, and very present in foreign policy matters on the international scene.

In this chapter it is interesting to present what distinguishes these two actors, the characteristics contained in one and absent in the other, and how they reacted to this hybrid threat, cyberterrorism. Based on this, it will be possible to design which strategies are present in their policies, understand why they are different, understand if being part of an organization such as NATO has presented Estonia in a more advantageous stage, and how Iran has defended itself against its attacks with a more individualistic approach.

Another point that will be of great importance in this last chapter is to understand if being part of an international alliance gives you more protection against unconventional threats, that is, hybrid threats. Are all states prepared and aware of these new types of threats? What are the real consequences for governments when facing such threats? To answer as many of these questions, this chapter will be divided into two subsections, the first will present which were the strategies applied by both countries as a reaction to the cyber-attacks they faced. And lastly, an analysis will be performed where comparisons between the two countries will be made, demonstrating the main differences noted and using the theory of the Copenhagen School to support any possible conclusion.

3.1. Strategy ends of both countries and their reactions to the attacks

The attacks Estonia and Iran faced in 2007 and 2010, respectively, were one of the first cyber-attacks to be evidenced against State Nations. Both attacks put the Government's technological information centers at risk and jeopardized the status quo of both. Each country enjoyed a pack of strategies to counter these attacks, which are significant to understand their different approaches and the characteristics they bring with their tactics.

As mentioned before, Estonia is one of the smallest countries part of the NATO alliance, however, is the most interconnected one, which means its day-to-day life relies heavily on its IT systems. Hence, Estonian society's ubiquitous IT dependence has also made the country highly vulnerable to cyber-attacks that could potentially paralyze its everyday

activities, making the attacks, when they occurred, not something unpredictable. The attacks Estonia faced were DDoS targeting websites and email servers and a few SQL attacks on key servers and routers. Based on that, the attacks were not considered to be sophisticated but they were aggressive in terms of numbers (JOUBERT, 2012).

To contain the attacks that lasted 22 days, the Estonian government made some decisions that helped to reduce the consequences of the attacks, making it possible to say that the attacks did not represent a possible collapse of the Estonian computer network. The cyber-attacks did not consist of a single, recurrent, steady campaign, but rather, consisted of several distinct attacks over a period of almost four weeks. This means that the strategy the Estonian government had to build was not simple, and immediatist, but rather flexible and adaptable for a longer period (JOUBERT, 2012).

This being said, in the first phase of the attacks, the Estonian community of technical experts had to have support from the international community. When the attacks started the CERT became the central hub of information exchange and the site to coordinate some of the defensive measures of operational IT units in Estonia organizations. Estonian CERT was leading a team of experts from many departments like the Departments of Commerce and Communications, the military, and the intelligence community, all with the same goal. Hilla Aerelaid, one of the two full-time staff-member and head of CERT-EE at the time, listed all the parts involved in the counter team: "national crisis committee, DNS / TLD, ISPs, telcos, banks, "cyber police", intelligence, counterintelligence, CERT-EE, [the] community, some friends, [the] Government Communication Office, [the] National Security Coordinator, [the] Ministry of Foreign Affairs, MoD, 'helpers', NATO, DHS, [and the] embassy's" (SCHMIDT, 2013). However, even with this massive help, the most significant role in the technical response activities came from the Estonian CERT.

As a member of NATO, Estonia requested emergency assistance to defend its digital network infrastructure against the ongoing attacks. The Estonian Minister of Defense, Jaak Aaviksoo, stated that the attacks "were aimed at the essential electronic infrastructure" and "this was the first time that a botnet threatened the security of an entire nation". In response to the request and the danger it represented, NATO sent experts to assist the CERT, and in parallel with that NATO became aware of the threats cyber-attacks could mean to its members and started an internal awareness of the matter, especially given the fact that if the attacks against Estonia had been more sophisticated it would have posed a much greater risk to the sovereignty of the state (JOUBERT, 2012).

Once the attacks entered what is known as the “second phase” and it was botnet-based, international collaboration and coordination became essential. The Ministry of Defense was mainly responsible for organizing international support in the political sphere, and this responsibility didn’t include the organization of operational teams or technical experts’ teams. The Estonian internet security experts collaborated with the global Internet security operations community and CERTs of other countries, like Finland, Germany, and Slovenia (SCHIMIDT, 2013).

Alongside the international collaboration, came as well other types of actors, that had the better infrastructure for some phases of the counter back, such as the operational control over networks and systems. These were network companies, vendors of security appliances and network hardware, law enforcement and other security authorities, non-profit internet security organizations, and a number of IT individuals coming from Estonia, Russia, and other places around the world. Important to salient that with the Estonian government framing the DDoS attacks as a security issue caused by Russia, the Western media was drawn attention to the attacks, also attracting attention from other countries. (SCHIMIDT, 2013; DETLEFSEN, 2015).

Eventually, the Estonian CERT, together with international support, developed a three-pronged approach to contain and fix the problems caused by the attacks. The first step was to increase the server capacity for their systems to handle more traffic. The second step was to develop a filtering system to be added to the structural layout of the Estonian Internet, these would separate the good message traffic from the bogus message associated with the attacks. The third and final step was to work with authorities responsible for the root Domain Name System servers so they would be able to identify the botnet and make them offline. By doing so, Estonia had to close and block access to its computer systems from outside the country. These measures made the systems unavailable from abroad, an act that was widely reported by the international media (SCHIMIDT, 2013; DETLEFSEN, 2015).

The Estonian cyber-attacks revealed substantial malfunctions in NATO’s cyber defense arrangements. The acts forced the Alliance to re-evaluate its strategy toward this growing threat. NATO’s rearrangement of cyberterrorism and hybrid threats can be considered the biggest reaction after the events. For NATO the attacks meant addressing issues that would help prepare the Alliance for the future, this means the technical challenge of identifying those threats and vulnerabilities on the Alliance's network, and the political difficulty of defining a defense strategy to be implemented by NATO with the consensus of all members (NATO, 2016).

The three challenges and areas NATO would need to address to put in place a strategy were: the legal, operational, and strategic aspects. First, regarding the legal factor, NATO needed to understand the aspects that cyber-attacks assionate on Articles 4 and 5 of the alliance, where collective defense mechanisms are assigned. The articles "indicate that it is the Nation's prerogative to determine whether they consider themselves exposed to a threat or under an armed attack. However, they do not create any automaticity whatsoever concerning the response in such cases" (JOUBERT, 2012).

The problem with cyber-attacks is that it is hard to be in place with Articles 4 and 5 since there is no practical experience on the basis, and because of this, each case would therefore need to be assessed separately. Since not all states think the same in this matter, the decision on whether to invoke Article 4 or 5 would "depend on political perceptions (...) and the different roles played by the government agencies involved in the examination and assessment of cyber threats and incidents, and competent to adopt or contribute to actual responses". (JOUBERT, 2012). In the end, most of the law aspects that concern cyber-attacks are connected to the existence of international and national laws that can provide an adequate framework to manage those threats. By some, cyber-attacks, if taken into consideration as a "consequence-based approach" can be sufficient to make Jus in Bello applicable, given the technological progress in modern warfare. This being said, NATO will play an important role in those parts of the alliance to implement a type of suitable strategy, and for those who are not part of the alliance to feel inspired by it (JOUBERT, 2012).

As for what concerns the operational aspect, after the attacks in 2007, it became obvious to the organization that they needed to extend their cyber defense capabilities. The NATO Computer Incident Response Capabilities (NCIRC) couldn't alone handle all the demands they start having, since the attacks have shown an increase in numbers and actions. NATO needed then to improve the protection of its own internal information infrastructure and also, help defend the Allies. This would create a challenge on the technical side, once some countries would prove to be a political obstacle due to sensitive information. Therefore, what the alliance had to do was, achieve the right balance to implement a clear, consistent, and non-redundant chain of command, mean, NATO had to focus on ensuring a rapid and efficient response in case of a cyber-attack, while not overstepping its prerogative (JOUBERT, 2012).

Lastly, from a strategic point of view, NATO had to reinvent itself since none of the defense strategies and doctrine they had for other aspects could be simply transposed to the uniquely complex digital domain. However, finding a strategy has become a challenge

for the alliance since there are many diverging political views on cyber-attacks, because of this, NATO is now trying to implement an active strategy for the cyber scenario, with better security standards and requirements. But even with this set of strategies or actions, it is still not considered a proper real deterrent against cyberterrorism or attacks, and for this, there is still the possibility of using Article 5 of the North Atlantic Treaty (NATO, 2016).

In this respect, the NATO Policy on Cyber Defense reiterates that any collective defense is subject to political decisions of the North Atlantic Council and that the Alliance will remain flexible on how to respond to the attack. Cyber-attacks can take various forms, depending on their objectives and tactics, and can lead to the many examples here already explained. Determine which category an attack falls into will most likely depend on legal and political considerations at the national level of each country (JOUBERT, 2012).

Now, as for what concerns Iran's reaction to Stuxnet, it is first important to remember Iran has a different international positioning than Estonia, so it is not surprising that its response to attacks will be different. In some ways, their response, and their way of portraying themselves in the International System will provide enough information to be analyzed in the next point, where a comparison between the two countries will be made, regarding their reaction to cyber-attacks.

The Stuxnet attacks started in 2008, and it is not clear if the Iranians were aware of it. Different from what was expected, Iran's reaction did not become public until 2010 and it was not until the following year that Iran publically announced the creation of its cyber unit capable of offensive operations. At first, the Iranian government denied such malware as Stuxnet, saying instead that they had found a "worm" and contained it, thus the reason for taking some time to first admit it and then do a public reaction. The chief of Iran's Passive Defense Organization, General Gholamreza Jalali, announced at the time that the Iranian military could fight back against its enemies in cyberspace and Internet warfare (SANGER, 2012).

At the time, many believed that such a statement was a clear message warning of a potential strike back, at anyone who attacks Iran. Based on the assumptions that Iran was refining uranium to develop a nuclear weapon, it is possible that this gave the government a reason not to truthfully report the nature of the attack and how they responded to it. Iranian officials issued miscellaneous messages, some defining the attack as not serious while others claimed they arrested nuclear spies (GROSS, 2014).

This covers the communication component of a deterrent threat. Since, by then, Iran didn't have a counter plan against cyber threats, misleading information or the current status

of the attack was a way to not show its weakness in cyber capabilities. Afterward the discovery of Stuxnet, Iran increased their budget and research for cyber security by around 1200%, and by doing so, raised the suspicion as to why, and what were they looking to achieve. Andretta Towner, a Senior Intelligence Analyst at CrowdStrike, said "they're building this up as they would any other capability, but it seems that when we look forward we want to know are they building it up specifically to use it or are they just building this up in case they need it" (SEN, 2015).

In August 2012, Iran's hackers attacked the Saudi oil company, Aramco and the Qatari natural gas company, RasGas. The virus names "Shamoon" deleted important data on 30,000 Aramco's computers. Experts familiar with the incident claimed that Shamoon seems to be a reverse-engineered version of malware that was used against the Iranian energy company. This case showed how counter-back activities can run the other way around, when hackers can reverse back a malware and use it again, as a way of response, which was the case of Shamoon's lineage (DETLEFSEN, 2015).

In the same year, multiple financial businesses like JPMorgan, Bank of America, and Chase, reported that they were victims of sustained DDoS attacks. Due to the events of the time, attention was brought back to Iran being blamed for the attacks. Some American officials speculated that those attacks might have been a retaliation for the West's sanctions on Iran due to its nuclear programs. Since the attacks occurred only months after *The New York Times* article claiming confidential confirmation of the US government's role in creating Stuxnet, one is led to believe that the attacks on US banks were a response by the country to the attribution of the attack. Although they were simply DDoS attacks against commercial websites, it was the best way Iran found to demonstrate its new capability and attack what it saw as the U.S.'s center of gravity - its economy (NAKASHIMA, 2012).

Taking into consideration that in 2012, possibly, Iran's capabilities were still low since they only started their cyber defense activities the year before (if you take their announcement of creating a cyber unit as true), their capabilities would have been incipient, and DDoS may have been the best they could do in a year. Since then, however, they seem to have significantly improved their capabilities. In 2013, A year after the attacks on American financial firms, the US Navy reported that Iran had hacked into their email and intranet network. The Navy stated that it took about four months to completely eliminate Iranian hackers from its systems. This network penetration shows a higher level of expertise and sophistication than previously seen from Iran and means that its capabilities have increased since the Stuxnet attacks. More recently, a cybersecurity firm published a report

stating that Iranian hackers have penetrated at least fifty different organizations in sixteen countries since 2012. Many of them, including oil companies and airlines, have denied any compromise of their security (NAKASHIMA, 2012; BARNES and GORMAN, 2013).

Iran's response after the events that linked to Stuxnet showed how every action has a disclaimer, which may or may not be predicted. Attacks on the structures of one country can mean retaliation from the other side. Iranian involvement in the cyber sector has further culminated to shake Tehran and Washington relations, as well as their allies. There is much question as to why Iran has not admitted the effects of Stuxnet, but this is very much tied to how the country conducts itself within the international system of states. What follows is finally an analysis of the differences between these two cases of cyberterrorism, Estonia and Iran, and how these differences can be interpreted according to what was presented so far in terms of concepts and theories.

3.2. How did the two countries behave toward cyberterrorism and the main differences?

After all the considerations that have been made so far in this paper, this last point will be dedicated to answering the central research objective that culminated in the development of this project, where we sought to understand cyberterrorism as a type of hybrid threat and to understand how states, in this case, Iran and Estonia, combat and react to this threat. To do this, first, it is necessary to understand what were the main differences observed between the two cases, and their ways of dealing with cyberterrorism attacks. Were there similarities? If there were differences, is there a reason?

To achieve the answers to these questions, along with the objective of this case study, we will make use of the concepts and theories mentioned in the first chapter, which will provide the basis for the interpretations derived from the explanation of the cases and their characteristics, which are covered in the second chapter. In addition, necessary backing will be provided throughout this sector because, as has been observed during this project, researchers and theorists tend to disagree on certain issues, making it necessary to outline the points of view that are in fact taken into account here.

But in the end, what were the main differences observed between the two states in their reactions to the attacks? One of the most striking differences, which one can perceive, is the support from the international community that Estonia received during and after the attacks, and is not perceived in the case of Iran. Both countries suffered unexpected cyber-

attacks, which hung on for weeks/months. Still, the first, received international reinforcement and support, along with media coverage, while the second, received almost no help or resources to combat its attacks (SCHMIDT, 2013).

The international support point can be perceived in many sectors like assistance with counter-back strategies, a skilled workforce to cease the attacks, a foundation for creating knowledge, and measures to prevent future cyber threats which can all be recognized in the case of Estonia but not in the case of Iran. The Estonian community of technical experts had support from the international community, and after the attacks, Tallin became the base of NATO's Cooperative Cyber Defence Center of Excellence (CCD-COE) proving to be a central hub for research related to this field of study. The 2007 attacks presented to be the kicks off for the organization and its allies to add the topic of "cyberterrorism" to their political agendas and to start an internal process of understanding the term and concept (BOGDANOSKI and PETRESKI, 2013).

NATO's support for the events came as a team of experts that was sent to the country to help compose the group of people responsible for stopping the attacks, CERT (JOUBERT, 2012). During the second phase of the attacks, CERTs of countries like Finland, Germany, and Slovenia also collaborated with Estonian internet security experts, and this cooperation was essential to cease the attacks. The Western media also played a big role, drawing attention to the attacks, creating international support, and widely reporting the attacks as much as their immediate consequences like, when the Estonian network systems became unavailable from abroad (SCHIMIDT, 2013).

Also, the consequences of Estonian attacks were mainly on economic and social aspects. As the country is super dependent on its network infrastructure and electronic communication channels, the daily business workflow was heavily damaged since they had to face an overload of emails servers, network devices, and on web servers of internet service providers. Large entities such as banks, media corporations, and governmental institutions were strongly affected, but also the small and medium-sized enterprises whose daily business activities were severely impaired. This all meant that in fact, the cyber-attacks had a perceptible effect on the functioning of domestic economy (TIKK et al., 2010).

In the social effect, due to the significant dependence of the government on its electronic practices, the other means of communication that did not depend on the Internet were already much reduced at the time, not to mention that the population was no longer used to doing daily tasks without these electronic tools, not knowing how to obtain information other than online. Due to the unavailability of government websites, everyday

communication with any government channel was affected, making it impossible to perform some ordinary actions such as submitting documents or paying taxes. This can be clearly seen when State Portal "eesti.ee", widely used for filing tax reports, applying for state benefits and subsidies, received attacks and impacted directly the monetary situation of the people who would need this assistance. It is comprehensible that, only because the unavailability of government websites was temporary, the estimated consequences of the cyber-attacks were not so critical and didn't mean bigger damage. However, it is still impossible to estimate what was the real damaged experienced by the population (TIKK et al., 2010).

While Estonia expressed these characteristics/responses, the Iran case proved to be quite different in other esteems. The most notable difference is the fact that while the first quickly claimed to have suffered a cyber-attack, Iran preferred to follow contrary paths, first by denying the existence of Stuxnet and second by admitting the attacks, but not sharing what their real effects were. By doing so, the country also lost the opportunity to have any type of available international assistance that they could enjoy to cease the virus (SANGER, 2012).

In 2010, instead of admitting that they were victims of cyber-attacks, they said that they found a worm and contained it, not giving any other information, or confirming that the virus they found on their systems was indeed the malware Stuxnet, which was circulating in thousands of computers, and especially in Iran's devices (SANGER, 2012; BAEZNER and ROBIN, 2017). This move taken by the Iranian authorities can be related to the speculations at the time that the technical experts took some time to be aware that Stuxnet was present in their computers and systems connected to the Uranium centrifuges in Natanz. It is believed that the malware was present since 2008, and the fact that the country took more or less two years to be conscious that they were suffering attacks, could give the impression that the country was not strong and able to defend itself in the cyber sector, demonstrating weakness to the international community (BROWN, 2011; GROSS, 2011; LACHOW, 2014).

The fact they didn't have any type of support coming from other countries, as Estonia did, and for positioning themselves in a more individualistic way, resulted in another key difference between the two cases which was the Iran's announcement of an existing capability of offensive operations to protect themselves from any future cyber-attacks. All the investment that the government has allocated to the cyber defense sector has shown a country concerned with being able to defend its status quo in any field, including the cyber,

since the consequences of Stuxnet did not remain only in the digital world but were physical and costly to the country's uranium production (SEN, 2015; DETLEFSEN, 2015)

Iran, also, received many accusations of posterior cyber-attacks that happened in 2012, in the USA and Saudi Arabia, one year after the announcement of their cyber defense center, raising awareness from the international community of possible counter back activities after Stuxnet. By positioning themselves as autonomous and capable of defending against cyber-attacks, the Iranians have come to be known as a nation with a strong cyber defense structure which has culminated in their enemies also fearing stronger retaliation, demonstrating the Stuxnet attacks as the instigating factor (NAKASHIMA, 2012; SEN, 2015)

There were differences between the way both countries reacted to the attacks and also how they develop. One took twenty-two days to cease the attacks, the other took months/years to be aware they were suffering an attack. One received international support, and collaboration, while the other had to compose itself a center of defense against cyberterrorism. One became a hub for research about cyberterrorism and threats, while the other received accusations of orchestrating other cyber-attacks. So what could have instigated these differences in reactions between the two cases?

One of the reasons for the differences may be linked to the fact that there is no common understanding of what cyberterrorism is and how to defend against it. There have been many attempts by scholars and government organizations to find one single definition of cyberterrorism, yet, there has not been one that all actors agree on, regarding not only the meaning but the examples, descriptions, and counterparts (WEIMANN, 2004). As described in the first chapter of this project, authors tend to disagree when it comes to conceptualizing cyberterrorism into a single concept. Jarvis et al. (2014) offered four possible reasons why it is difficult to reach a consensus on one meaning of cyberterrorism. The first is regarding the temporal factor linked to how hard it is to define a “standard” which is connected with the difficulty in finding a pattern for the phases of an attack. Each attack can have its timing and characteristics, making it difficult to create "rules" to facilitate the identification of a cyber-attack if it occurs. The second reason is related to the damage that a cyber-attack can cause. Some authors/states only consider a cyberattack to be one, if it causes physical damage at some point, while others will disagree, and say that even if the damage is only in the digital world, it is still a cyberattack (JARVIS et al., 2014).

The third reason given by Jarvis et al. (2014) meets the terminology of the term. The fact that the media is constantly portraying cases of cyber-attacks contributes to a

misinterpretation of the word and culminates in confusion about this topic. The fourth and last reason, the authors mention how the media hyperbole around cyberterrorism misleads the concept, making something that has already proven to be hard to define, even harder. Weimann also mentions the media factor and expresses that the way they tend to portray the problem attracts even more challenges for a "universal" conceptualization becoming yet another challenge that researchers face (WEIMANN apud JARVIS et al., 2014).

The divergence of authors is a contributing factor to the fog that surrounds the events of cyber-attacks. While Denning, (2000) describes cyberterrorism as illegal attacks on computers, networks, and information centers to intimidate and coerce a government and population to act in a certain way, authors such as Soo Hoo et al., (1997) question whether these types of attacks can even be considered examples of terrorism. Others such as Gordon and Ford, (2003) have further narrowed the definition by including the simple act of buying an airline ticket, which will be used by terrorists, as the beginning of the execution of cyberterrorism. Conway, (2002) disagrees, considering that the use of computers as a facilitator of their activities cannot be considered the beginning of cyberterrorism, but rather the use of technology as a weapon or target. But, even though this is the academia's reality that studies the phenomenon many authors such as Weimann, Denning, or Jarvis affirm the need for study and conceptualization of the term so that security policies can be designed in the most effective way possible, providing national and international security (SOO HOO et al., 1997; DENNNIG, 2000; CONWAY, 2002; GORDON and FORD, 2003).

This uncertain and somehow "bipolar" landscape on the topic affects the development of containment policies, either individual or shared, in the case of organizations. In the case of NATO, even though there is already a more established political environment when the subject is cyberterrorism, the rules of these policies still have a certain "gray area" since some actions require interpretation and acceptance by each state, according to their laws. In other words, they do not act like, for example, in the collective defense in the 5th article of NATO in all the cases (NATO, 2022). As an example, there is

> In cases of hybrid warfare, the Council *could decide to invoke Article 5* of the Washington Treaty, as in the case of armed attack. We are enhancing our resilience, improving our situational awareness, and strengthening our deterrence and defense posture. We are also expanding the tools at our disposal to address hostile hybrid activities. We announce the establishment of Counter Hybrid Support Teams, which provide tailored, targeted *assistance to Allies, upon their request*, in preparing for and responding to hybrid activities. We will continue to support our partners as they strengthen their resilience in the face of hybrid challenges (NATO, 2018)

As cyberterrorism is one example of Hybrid Threats, any cyber-attack would fall into this categorization, but would still require the State to request help. This brings us to the other noticed reason why there are differences between Estonia's and Iran's reactions. Estonia had the support from NATO that, in one way or another, helped to cease the attacks and also brought international attention to the events, culminating in more international assistance from other countries. In response to Estonia's request for immediate assistance, NATO sent a group of experts to help set up the team responsible for stopping the attacks. In addition to the support of the organization, other countries that helped either by sending human resources or by helping to access information systems also proved essential (JOUBERT, 2012).

However, this type of help and support is not perceived in Iran's case. Possible reasons for this include: Iran suffering lack of popularity internationally due to accusations that it had a nuclear program. This may have made some states uncomfortable, and thus, preferring not to send help for the containment of Stuxnet (GROSS, 2014). Iran's foreign policy, since the government chose not to share that they were suffering a cyber-attack and then when they finally acknowledged the existence of Stuxnet, they chose to keep the real consequences of the attacks hidden. This resulted in limited knowledge of other countries as well as the media (SANGER, 2012).

This whole scenario culminates even more in an uproar in the media, which tends to mention cases of cyber-attacks frequently in their "headlines". The more one reads about a topic the more fear tends to grow around it, causing even more insecurity in the population about the ability of their governments to keep them safe. This media hyperbole that was mentioned by Jarvis et al. (2014), can be related to the Copenhagen School's securitization theory, mentioned earlier (JARVIS et al.,2014).

Copenhagen School's securitization theory argues that security is a speech act that securitizes, that it, constitutes one or more reference objects, historically the nation or the state, as threatening to their physical or ideational survivor and therefore in urgent need of protection (WAEVER, 1995; BUZAN et al., 1997) In the past, as claimed by Buzan, the School has dealt with cyber security issues, but considered it an "attempted" securitization, since according to them, it didn't have cascade effects on other security issues, meaning that, it didn't treat other security's sectors (BUZAN et al., 1997)

Starting in 1998, the School of Theorists stated that there was no need to theorize cybersecurity as something distinct from the military, political, environmental, social, economic, or religious sectors, the problem could be dealt with within them according to the

demand (BUZAN et al., 1997) However, as Hansen and Nissenbaum pointed out, since then, much has changed, many events have taken place that has emphasized the Copenhagen School's existing demand to be up-to-date on issues surrounding cyber security (HANSEN and NISSENBAUM, 2009).

If securitization takes place in an act of speech, then, already by that time, cyber security had been securitized by President Clinton in 1996, by President George W. Bush in 2003, and after by NATO when the Estonian events took place, with the creation of a counter cyber defense center. In other words, if the securitization model has to be defined as a state demands threat-urgency (in their speech), as say the Copenhagen School, these sectors can also constitute threats rather than the military (HANSEN and NISSENBAUM, 2009). And if this can only happen as long there is "drama" and saliency of national and international security, then positively, cyber security and all its variation should be treated separately by the theory. Here are the reasons why: first, the drama can be noticed by the media hyperbole already mentioned by Weimann (2004) and Jarvis et al. (2014). As was described many times here, media has been an important part both of spreading the word about cyberterrorism and attacks and also, for causing confusion regarding the meaning of the concept and what it implicates (WEIMANN, 2004; JARVIS et al., 2014).

Second, there have been occasions during history, as well as during the events portrayed here, where there have been acts of discourse that can be understood as the securitization of the issue. In Estonia this can be noticed, for example, when the Minister of Defense, Jaak Aaviksoo, did a statement about the attacks, claiming that "this was the first time that a botnet threatened the security of an entire nation" (JOUBERT, 2012). In Iran's case, this can be seen when General Gholamreza Jalali, Chief of Passive Defense Organization, announced that Iran's military was capable to fight back its enemies in cyberspace and internet warfare due to the creation of a counter cyber defense system (SANGER, 2012).

Third, for example, in both cases, the cyber-attacks represented a threat to their *status quo*, meaning that they represented both a national and international threat. For Iran, it meant having the Natanz nuclear enrichment plant hit, and its machinery damaged and broken, and it is estimated that the attacks cost months or even years of uranium production (BAEZNER and ROBIN, 2017). For Estonia it meant having the government websites attacked, blocking any kind of communication from the government with its population, having its financial centers attacked, and damaging the daily lives of its population,

culminating in the growth of the sense of fear, and made it impossible for the state to perform its number one obligation, to protect its population (SCHIMIDT, 2013).

That is, within this it is possible to conclude that yes, there is a gap between the way the Copenhagen School acts concerning cyberterrorism and these three examples, of why the theory should establish better relations with the concept, demonstrating that the two case examples analyzed here can be explained with securitization theory. According to Hansen and Nissenbaum (2009), the ability of Estonian securitizing actors to have the attacks accepted as ‘‘the first war in cyberspace’’ and to have them prominently covered by the world press makes for at least a partially successful case of cyber securitization (HANSEN and NISSENBAUM, 2009). The press media of the time published articles defining the attacks as a “very real example of cyberwarfare” and the “first real war in cyberspace” urging NATO to take an important role in “collective cyber-security” (HANSEN and NISSENBAUM, 2009).

The attacks are also important because the securitization of hacking was boosted by Estonian officials describing it as ‘‘terrorism’’. Adding to the specter of the ongoing War on Terror, the Estonian case raised ‘‘the possibility of an Al-Qaeda- type group replicating it’’, securing, even more, the topic (HANSEN and NISSENBAUM, 2009) In Iran’s case, phrases like the one from Michael Gross and Jonas Kargsson, where they describe Stuxnet as “the Hiroshima of cyber-war” has a significant meaning, as well as, the awareness the attacks brought to cybersecurity issues, as mentioned Baezner and Robin in 2017 (GROSS, 2011; BAEZNER and ROBIN, 2017).

The most significant lesson of bringing the Copenhagen School to cyber security may be to bring the political and normative implications of ‘‘speaking security’’ to the foreground. Cyber securitizations are particularly powerful precisely because they involve both the political realm, as much as the securitization, and the technical aspects of a cyber-attack, for example. It is in the end, an interdisciplinary effort to understand it, and to try to find common grounds on how to effectively counter it (HANSEN and NISSENBAUM, 2009). In the end, cyberterrorism is an example of Hybrid Threat, and as mentioned here before, this is characterized as the product of several ways of threatening or attacking its intended target. It is the mixture of different methods, conventional or not, military or non-military of attacking to achieve an intended goal (ANDERSSON and TARDY, 2015). So its multidisciplinary aspect is a point to be considered by authors, either from the Copenhagen School or any other that attempts to conceptualize cyberspace and its threats.

To achieve a better understanding of the phenomenon, events, and attacks, a commitment on the part of theoreticians, theories, and policy-making is necessary for there to be a global understanding of what cyberterrorism and its variants and examples are. Without this, there will be no policies and strategies that all countries can follow, and the confusion over the term will not cease to exist.

Conclusion

The Technological development, characteristic of the late 20th and early 21st centuries, has brought many benefits to society but has also been responsible for a new kind of threat, cyberterrorism. The cyber-world started to be also used as a tool of terror to carry out attacks by terrorist groups, non-state actors, and states. Because of this, theorists, and researchers, began to study the concept to conceptualize and understand what could or could not be considered an example of cyberterrorism since it affected the behavior of states that did not know how to react to these threats, culminating as well for international organizations and governments to include the topic within their political and international security agendas. However, it was noticed since the beginning there was a great divergence in how some security theories, including the Copenhagen School, reacted to and understood this problem.

This master's thesis aimed to understand how the two cases presented here, Iran and Estonia, behaved when they suffered cyberterrorism attacks. In addition to this goal, there was also the ambition to analyze the differences between the countries' reactions and why they existed. Because of this, the first chapter presented the theories and concepts related to cyber terrorism and how it is seen as an example of hybrid threats. In addition, this first chapter presented how the major international organizations understand the concept to contextualize the framework in which cyberterrorism is inserted. Next, it was discussed that the two chosen case studies demonstrated all the characteristics that made up the attacks and states' reactions. Then, in the last chapter, after presenting the reactions of the two countries, it was possible to analyze the main differences between them and think about why they were different.

The main differences perceived between the two cases were: the international support offered to Estonia; the media attention received by Estonia; the creation of a defense security center for cyber threats in Iran; the positioning of Tallinn as a pioneering center for cyber studies and defense; the pragmatic positioning of Iran that culminated in the denial of Stuxnet in its first year after it was discovered; the allegations of potential involvement in subsequent cyber-attacks by Iran against other countries.

Within this, the states' responses differ for two reasons observed. Primarily, it is noted that the fact that Estonia is part of NATO provided the country with an international aid privilege, which was not pointed out in the case of Iran. Estonia's help came not only from the organization but also from other countries and the international media that followed the attacks with constancy. Second, Iran's foreign policy positioning makes it unsupported

internationally during Stuxnet attacks, even though the malware has been found on several other foreign computers. The Iranian government's choice of not admitting the attacks at first and then announcing a cyber defense center culminated in an "individualistic" positioning noted for the lack of international support, whether by international institutions or other countries.

It is essential to note why the cases of Estonia and Iran were chosen as case studies here. Although both countries have such different geopolitics and have suffered attacks with other characteristics, it is still possible to exercise an analysis since both suffered from cyber-attacks for a specific moment of time. The central fact that both countries have such a different conjuncture is already an exciting factor for analysis since one is a NATO member and the other has a pragmatic international policy. Both cases were analyzed separately, comparing only their responses to the attacks. It is also important to emphasize in this paper that there is an awareness that will always be disagreement on topics, such as whether the Estonia and Iran cases are examples of cyber terrorism, but that is why the third chapter presents the authors that are taken into consideration here. There is also an awareness that other cases could also be analyzed. Still, from this author's point of view, Estonia and Iran presented themselves as two opposing countries that suffered similar attacks, which intrigued the author.

So then, the main point perceived when doing the analysis was the lack of consensus perceived in all branches - theoretical, organizational, and political - which contributes to a more significant ambiguity on the subject and makes it difficult to conceive a matrix concept where new policies and strategies would be inspired to reach standard solutions on cyber-terrorism.

This reluctance on the part of theorists to agree on examples and explanations of what cyber-terrorism is, as with the term ‘terrorism’ itself, it’s the main reason why it’s so difficult to reach a consensus, why the cases studied had different reactions, and why many countries and institutions still don’t recognize cyberterrorism as a multifactorial threat, that needs attention. It has been shown at several points that authors tend to disagree and are even aware of the situation. And as one example here, it was presented the famous Copenhagen School and its theory “theory of securitization” and how their authors have denied cyberterrorism to be treated and studied as a separate branch of security as many other topics have in the past and present.

For this, it was presented why, following three reasons, the Copenhagen School should reconsider and start examining the many variants cyberterrorism can be executed: I)

Cyberterrorism was described by the media with drama; II) In history, one notes acts of speech being made about cyber terrorism, this being an example of securitization of an event; III) cyber-attacks do pose a national and international threat, threatening the status quo of the countries that have suffered the attacks. So, from this, it is possible to conclude that there is a gap between how cyberterrorism is seen and how it is understood by theories, as is the case of the Copenhagen School. The exposed examples can be used to explain why it is necessary for a consensus study within the School and among the authors and the international system and organizations. Therefore, it is possible to recommend that the efforts to raise awareness of the term be reallocated to understand what an act of cyberterrorism consists of. From that moment, policies, strategies, and international cooperation will be possible and feasible, and countries and institutions will be better prepared to defend themselves and contain cyber threats.

Thus, it is possible to state that the central objectives of this work were achieved since cyberterrorism was framed within the concept of hybrid threats, and it was possible to outline how NATO and countries perceive this problem. It was identified that there is a lack of consensus, that countries and their policies are still reluctant to categorize cyberterrorism as a top priority in their agendas, but that there is also an effort on everyone's part to describe as much as possible what for them is the phenomenon. Having said that, it is possible to emphasize that the hypotheses that were initially thought have not been fully proven: yes, states are not fully prepared for the culmination of cyber-terrorism; however, it was noted that in recent years, there had been an action taken by states and institutions to have more understanding about the concept, especially by NATO and EU.

Furthermore, it is established that Estonia's reactions differed from Iran's, mainly because it is backed by NATO. However, it was not expected that the Iranian defense center would become so promising, resulting in a fear shared by some states that this center would exceed their expectations and become a more significant threat. The primary hypothesis that there are still too many gaps in ensuring and protecting oneself within cyber-space was met, and that much progress still needs to follow on the studies of this subject. In addition, the author was surprised to discover a great divergence of opinion regarding concepts and definitions inside the cyber world and even hybrid threats. There is still much to be studied indeed, and the author is also engaged to start contributing to this research.

5. Bibliography

Aaviksoo, J. (2008). **Cyber defense – the unnoticed third world war**. *Proceedings of the 24th International Workshop on Global Security, Paris, 2008*. Retrieved from:https://kaitseministeerium.ee/en/news/defence-minister-jaak-aaviksoo-cyber-defense-unnoticed-third-world-war

Allisson, G. (2005). **Nuclear terrorism: the ultimate preventable catastrophe**. Owl Books, New York. Kindle edition (e-book).

Andersson, J. J.; Tardy, T. (2015). **Hybrid: what's in a name?**: European Union Institute for Security Studies, out. 2015. ISSUE Briefs, *32*. ISSN 2315-1110.

Baezner, M.; Robin, P. (2017). **Hotspot analysis**: Stuxnet, out. 2017. Center for Security Studies (CCS), ETH Zürich.

Barnes, J. E.; Gorman, S. (2013, september, 27). **U. S. says Iran hacked navy computers**. *The Wall Street Journal*. Retrieved from:: http://online.wsj.com/articles/SB10001424052702304526204579101602356751772.

Bendrath, R.; Eriksson, J.; Giacomello, G. (2007). **From 'cyberterrorism' to 'cyberwar', back and forth: how the United States securitized cyberspace**. In: Eriksson, J; Giacomello, G. (Eds), *International relations and security in digital age*. London: Tyler & Francis e-books. DOI: https://doi.org/10.4324/9780203964736

Berdal, M. (2011). **The new wars thesis revisited**. In: Strachan, H; Scheipers, S. (Eds). *The changing characterof war*. Oxford: Oxford University Press.

Bogdanoski, M.; Petreski, D. (2013). **Cyber terrorism: global security threat**. In: *International scientific defence, security and peace journal*. In: *Contemporary Macedonian Defence*. 327.88:004.738.5-027.22. Skopje: Ministério da Defesa da República da Macedônia.

Brown, G. (2011, october, 1). **Why Iran didn't admit Stuxnet was na attack**. In: *Joint Force Quarterly*. Issue 63. Washington DC: National Defense University Press.

Buzan, B.; Waever, O.; Wilde, J. (1997). **Security: a new framework for analisis**. Boulder: Lynne Rienner Publishers.

Calder, A.; Watkins, S. (2012). **IT governance: an international guide to data security and ISO27001/ISO27002**. London: Kogan Page.

Consilium Europa (2022). **The EU's response to terrorism**. Retrieved from:https://www.consilium.europa.eu/en/policies/fight-against-terrorism/

Conway, M. (2002). **Reality bytes: cyberterrorism and terrorism 'use' of the internet**. *First Monday. 7*(11). DOI: https://doi.org/10.5210/fm.v7i11.1001

Denning, D. (2000). **Cyberterrorism**. In: *Special oversight panel on terrorism*. Washington DC: Georgetown University. Retrieved

from:https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm

Desouza, k. C.; Hensgen, T. (2003). **Semiotic emergent framework to address the reality of cyberterrorism**. In: *Technological forecasting and social change journal*. *70*(4). DOI: https://doi.org/10.1016/S0040-1625(03)00003-9

Detlefsen, W. R. (2015). **Cyber-attacks, attribution, and deterrence: three case studies**. (Monografia). United States Army Command and General Staff College Fort Leavenworth United States. Forth Leavenworth. Retrieved from:https://apps.dtic.mil/sti/pdfs/AD1001276.pdf

Devost, M. G.; Houghton, B. K.; Pollard, N. A. (1997). **Information terrorism: political violence in the information age**. *Terrorism and political violence*. *9*. DOI: https://doi.org/ 10.1080/09546559708427387

Eagan, S. P. (1996). **From spikes to bombs: the rise of eco-terrorism**. In: *Studies in conflict and terrorism journal*. *19*(1). Retrieved from:https://www.ojp.gov/ncjrs/virtual-library/abstracts/spikes-bombs-rise-eco-terrorism

Economist. (2002, february, 1). **George Bush and the axis of evil – America is set on brave but hazardous course**. *The Economist*. Retrieved from:https://www.economist.com/leaders/2002/01/31/george-bush-and-the-axis-of-evil

Eriksson, J.; Giacomello, G. (2007). **Conclusion: digital-age security in theory and practice**. In: Eriksson, J; Giacomello, G. (Eds), *International relations and security in digital age*. London: Tyler & Francis e-books. DOI: https://doi.org/10.4324/9780203964736

Giannopoulos, G.; Smith, H.; Theocharidou, M. (2021). **The landscapes of hybrids threats: a conceptual model**. Retrieved from:https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf DOI: https://doi.org/10.2760/44985

Gofas, A. (2012). **'Old' vs. 'new' terrorism: what's a name?** *Uluslararası İlişkiler*. *8*(32). Retrieved from:https://dergipark.org.tr/tr/download/article-file/540175

Gordon, S.; Ford, R. (2002). **Cyberterrorism?** *Computers & security*. *21*(7). DOI: https://doi.org/10.1016/S0167-4048(02)01116-1

Griset, P. L.; Mahan, S. (2003). **Terrorism in perspective**. *National Criminal Justice Reference Services* – U. S. Department of Justice – Office of Justice Programs. Retrieved from:https://www.ojp.gov/ncjrs/virtual-library/abstracts/terrorism-perspective

Gross, M. J. (2011, march, 02). **A declaration of cyber-war**. *Vanity Fair*. Retrieved from:https://www.vanityfair.com/news/2011/03/stuxnet-201104

Gross, M. L.; Canetti, D.; Vashdi, D. R. (2016). **The psychological effects of cyber terrorism**. *The bulletin of the atomic scientists*. *72*(5). DOI: https://doi.org/ 10.1080/00963402.2016.1216502

Gunneriusson, H.; Ottis, R. (2013). **Cyberspace from the hybrid threat perspective**. *Journal of information warfare*. *12*(3). Retrieved from:https://www.jstor.org/stable/26486843

Hansen, L.; Nissenbaum, H. (2009). **Digital disaster, cyber security and the Copenhagen school**. *International studies quarterly*. *53*(4). Retrieved from:http://www.jstor.org/stable/27735139

Hartelius, J. (2008). **Narcoterrorism**. Stockholm: Swedish Carnegie Institute & Langenskiöld Publishing Company. Retrieved from:https://ciaotest.cc.columbia.edu/pbei/ewi/0001610/f_0001610_823.pdf

Hoffman, F. G. (2007). **Conflict in the 21st century: the rise of hybrid wars**. Arlington: Potomac Institute for Policy Studies.

Hybrid CoE (2022). **Hybrid threats as a concept**. *Hybrid CoE*. Retrieved from:https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Hybrid CoE (2022). **Establishment**. *Hybrid CoE*. Retrieved from:https://www.hybridcoe.fi/establishment/

Jackson, R.; Jarvis, L.; Gunning, J.; Breen-Smith, M. (2011). **Terrorism: a critical introduction**. New York: Red Globe Press

Jarvis, L.; Nouri, L. Whiting, A. (2014). **Understanding, locating and constructing cyberterrorism**. In: Chen, T. M.; Macdonald, S. (Eds), *Cyberterrorism – understanding, assessment, and response*. New York: Springer Science + Business Media. DOI: DOI 10.1007/978-1-4939-0962-9

Joubert, V. (2012). **Five years after Estonia's cyber-attack: lessons learned for NATO?** Research Division. *NATO Defense College*. *76*. Rome: Imprimerie Deltamedia Group. ISSN 2076-0957. Retrieved from:https://www.files.ethz.ch/isn/143191/rp_76.pdf

Kaplan, A. (1978). **The psychodynamics of terrorism**. *Studies in conflict and terrorism*. *1*(3-4). DOI: https://doi.org/ 10.1080/10576107808435411

Lachow, I. (2014). **The stuxnet enigma: inplications for the future of cybersecurity**. *Georgetown journal of international affairs*. ISSN 1526-0054. Retrieved from:https://issuu.com/gjia/docs/gj124_cyber_issue

Laqueur, W. (1987). **The age of terrorism**. Boston: Little Brown & Company.

Malcolm, J. (2004). **Testimony of deputy of assistant attorney general John G. Malcolm on Cyberterrorism before senate judiciary committee, subcommittee on terrorism, technology and homeland security**. Retrieved from:https://www.judiciary.senate.gov/imo/media/doc/malcolm_testimony_02_24_04.pdf

Mattis, J. N.; Hoffman, F. (2005). **Future warfare: the rise of hybrid wars**. *U.S. Naval Institute*. *131*(11). Annapolis: Naval Institute Press. Retrieved from:https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars

Missiroli, A. (2021). **Geopolitics and strategies in cyberspace: actors, actions, structures and responses**. *Hybrid CoE Paper*. *7*. Retrieved from:https://www.hybridcoe.fi/wp-content/uploads/2021/06/20210622_Hybrid_CoE_Paper_7_Geopolitics_and_strategies_in_cyberspace_WEB.pdf

Nakashima, E. (2012, setembro, 21). **Iran blamed for cyber-attacks on U. S. banks and companies**. *The Washington Post*. Retrieved from:https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyber-attacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html

NATO (2013). **NATO glossary of terms and definitions (English and French)**. *AAP-06 Edition 2013*. Retrieved from:https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/aap6.pdf

NATO (2014). **Wales summit declaration**. *Heads of state and government participating of the north atlantic council in Wales*. Retrieved from:https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO (2016). **Warsaw summit communiqué**. Heads of state and government participating in the meeting of the north atlantic council in Warsaw. Retrieved from:https://www.nato.int/cps/ic/natohq/official_texts_133169.htm

NATO (2018). **Brussels summit declaration**. Heads of state and government participating in the meeting of north atlantic council in Brussels. Retrieved from:https://www.nato.int/cps/en/natohq/official_texts_156624.htm#21

NATO (2022). **Nato's reponse to hybrid threats**. *North Atlantic Treaty Organization*. Retrieved from:https://www.nato.int/cps/en/natohq/topics_156338.htm

Naughton, J. (2016). **The evolution of internet from military experiment to general purpose technology**. *Journal of cyber policy*. *1*(1). DOI: https://doi.org/10.1080/23738871.2016.1157619

Ottis, R. (2008). **Analysis of the 2007 cyber-attack against Estonia from the information warfare perspective**. *Proceedings of the 7th conference of information warfare and security, Playmouth, 2008*. Retrieved from:https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/

Pereira, J. (2018). **As ameaças híbridas – uma abordagem conceptual no quadro da OTAN e da EU**. [Cedis Working Papern. 60. Direito, Segurança e Democracia]. Retrieved from:https://www.academia.edu/en/37668852/As_amea%C3%A7as_h%C3%ADbridas_uma_abordagem_conceptual_no_quadro_da_OTAN_e_da_UE

Pollit, M. M. (1997). **Cyberterrorism – fact or fancy?** *Proceedings of the 20th national information system security conference, Baltimore, 1997.*

Primoratz, I. (1990). **What is terrorism**. *Journal of applied philosophy*. *7*(2). DOI: https://doi.org/10.1111/j.1468-5930.1990.tb00261.x

*Resolution 1566 (2004). **Adopted by Security Council at its 5053rd meeting on 8 october 2004***. Retrieved from:https://digitallibrary.un.org/record/532676?ln=en#record-files-collapse-header

Ruby, C. (2002). **The definition of terrorism**. DOI: https://doi.org/10.1111/j.1530-2415.2002.00021.x

Ruus, K. (2008). **Cyber war I: Estonia attacked from Russia**. *The european institute*. *9*(1-2). Retrieved from:https://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia

Sanger, D. E. (2012, junho,1). **Obama order sped up wave of cyber-attacks against Iran**. *The New York Times*. Retrieved from:https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyber-attacks-against-iran.html

Schmidt, A. (2013). **The Estonian cyber-attacks**. In: Healey, J.; Grindal, K. (Eds), *A fierce domain: conflict in cyberspace, 1986 to 2012*. Arlington: Cyber Conflict Studies Association. Retrieved from:http://netdefences.com/wp-content/uploads/SchmidtA-2013-Estonian-Cyber-attacks.pdf

Sen, A. K. (2015). **Iran's growing cyber capabilities in a post Stuxnet era**. *Atlantic Council*. Retrieved from:https://www.atlanticcouncil.org/blogs/new-atlanticist/iran-s-growing-cyber-capabilities-in-a-post-stuxnet-era/#:~:text=Iran%20has%20vastly%20ramped%20up,the%20Atlantic%20Council%20April%208.

Shachtman, N. (2009). **Kremlin kids: we launched the Estonian cyber war**. *Wired*. Retrieved from:https://www.wired.com/2009/03/pro-kremlin-gro/

Soesanto, S. (2020). **Why it exists, why it doesn't, and why it will**. *Real Instituto Elcano*. Retrieved from:https://www.realinstitutoelcano.org/en/analyses/cyber-terrorism-why-it-exists-why-it-doesnt-and-why-it-will/

Soo Hoo, K.; Goodman, S. Greenberg, L. (2008). **Information technology and the terrorism threat**. *Survival Global Politics and Strategy*. *39*(3). DOI: https://doi.org/10.1080/00396339708442930

Thachuck, K. (2007). **Transnational threats: smuggling and trafficking in arms, drugs and human life**. London: Praeger.

Tikk, E.; Kasha K.; Vihul, L. (2010). **International cyber incidents: legal considerations**. *Cooperative cyber defence centre of excellence*. Retrieved from:https://ccdcoe.org/library/publications/global-cyber-security-thinking-about-the-niche-for-nato/

Tóth, D. (2015). **The history and types of terrorism**. *University Ostroh Academy – Law Series*. *1*(1). Retrieved from:https://www.academia.edu/20390252/The_history_and_types_of_terrorism

UNODC. (2018). **Counter-terrorism**. *United Nations office on drugs and crime*. Module 4. Retrieved from:https://www.unodc.org/e4j/en/terrorism/module-4/key-issues/defining-terrorism.html

UNODC. (2019). **Hactivism, terrorism, espionage, desinformations campaigns and warfare in cyberspace**. *United Nations office on drugs and crime*. Module 14. Retrieved from:https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/hacktivism.html

U. S. Department of State. (2001). **Patterns of global terrorism (2000)**. *Secretary for civilian security, democracy and human rights* – Bureau of counterterrorism and countering violence extremism. Retrieved from:https://2009-2017.state.gov/j/ct/rls/crt/2000/index.htm

U. S. Department of Transportation (2000). **2000 annual assessement of motor vehicle crashes**. *National center for statistics and analysis (U.S.)*. Retrieved from:https://rosap.ntl.bts.gov/view/dot/4835

Waever, O.; Buzan, B.; Kelstrup, M.; Lemaitre, P. (1993). **Identity, migration and the new security agenda in Europe**. London: Palgrave Macmillan

Waever, O. (1995). **Securitization and desecuritization**. New York: Columbia University Press

Weimann, G. (2004). **Cyberterrorism – how real is the threat**. *United States Institute of Peace* – Special report. Retrieved from:https://www.usip.org/sites/default/files/sr119.pdf

Wellman, C. (1979). **On terrorism itself**. *Journal of Value Inquiry*. *13*(4). DOI: https://doi.org/ 10.1007/bf00135860

Williams, M. C. (2003). **Words, images, enemies: securitization and international politics**. *International Studies Quarterly*. *47*(4). Retrieved from:http://www.jstor.org/stable/3693634

Zetter, K. (2011). **How digital detectives deciphered Stuxnet, the most menacing malware in history**. *Wired*. Retrieved from:https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

Zalman, A. (2012). **A guide to different types of terrorism**. Retrieved from:http://terrorism.about.com/od/whatisterroris1/tp/DefiningTerrorism.htm