**2.** **Literature Review**

**2.1 NATO, the EU,**

**2.2 EU-NATO Cooperation in Traditional Domains of Security and Defense**

**2.3 Cyberspace**

**2.3.1 Securitization of Cyberspace**

**2.3.2 Cyberspace and International Relations**

**2.3.3 Gap in Critical Engagement**

**2.4 EU-NATO Cooperation in Cyberspace**

**2.5 Academic Gap**

**3. Methodology**

**3.1 Discourse**

**3.2 Discourse Analysis**

**3.2.1 Why Discourse Analysis?**

**3.2.2 Discourse Analysis Approaches**

**3.2.3 Discourse and Power**

**3.3 Representation and Practice within Discourse Analysis**

**3.4 Strengths and Challenges of Discourse Analysis**

**3.4.1 Reliability and Validity Within Discourse Analysis**

**3.5 Expert Interview**

**3.6 Data Selection**

**3.7 Overview of Data**

**3.8 Coding Procedure**

**3.9 Textual Mechanisms Used for Interpreting Discourses**

**3.9.1 Presupposition and the Creation of Background Knowledge**

**3.9.2 Predicate Analysis and the Creation of Subjects**

**3.9.3 Intertextuality**

**4 Background**

**4.1** **NATO Cyber Defense Policy**

**4.1.1 Cyber-attacks and Article 5 – blurry but consistent position of NATO**

**4.1.2 NATO's Expanding Role in Cybersecurity**

**4.2 EU Cyber Security Policy**

**4.2.1 Lack of EU competence in cybersecurity regulation**

**4.2.2 A late but effective awareness**

**4.2.3 Towards a European cyber sovereignty?**

**5. Theoretical Framework**

**5.1 Critical Theory of International Relations and Global Cybersecurity**

**5.2 Background of the Critical theory of International Relations**

**5.3 Critical Theory’s vision of Cybersecurity**

**6. Analysis**

**6.1 EU-NATO Cooperation**

**6.2 EU–NATO Cybersecurity and Defense Cooperation**

**6.2.1 Comparative analysis of NATO and EU’s approaches to cybersecurity**

**6.2.3 Opportunities to Deepen NATO-EU Cooperation in Cyberspace**

**7. Findings and Conclusions**

**7.1 Findings**

**Introduction**

It has to be stated that the North Atlantic Treaty Organization (NATO) and the European Union (EU) are organizations with completely different purposes. The analysis of the cooperation between the European Union and NATO in the field of cybersecurity and cyber defense is very unusual, almost unique insofar as cyberspace is still quite marginal within the field of International Relations, but that notwithstanding cyber incidents have become more complex, more disruptive, and in many cases more political. In the past decade, cyber incidents as well as cyberattacks such as on Estonia in 2007, Georgia 2008, Ukraine 2014, 2015, 2021, 2022, the foreign electoral intervention in the United States and the EU as well as cyber incident as Win32/Stuxnet, WannaCry, and NotPetyam rendered it clearer that cyberattacks have become way more disruptive, political and targeted. According to many polls, cyber incidents are one of the most prominent threats in the international agenda. Following the TechTarget report, cyber-attacks cost US$114 billion each year[[1]](#footnote-1). Yet scholars have struggled to seriously tackle the implications of this framework.

**Methodology** is one of the most crucial parts of the thesis. There were 4 methods applied in this thesis: comparative analysis, qualitative content analysis, quantitative content analysis and discourse analysis.

One of the main methods used in this thesis is comparative analysis. The comparative analysis is a mean of generating or refuting theories and hypotheses that uses comparisons based on procedures analogous to those of the scientific method. Therefore, what it seeks is to test the validity of arguments using science and the study of similarities and differences. Usually applies statistical techniques with data analysis based on covariation or diversity interpretation. The goal is to establish correlations between two or more cases and be able to draw scientific conclusions. A comparative analysis of the approaches, competences, capabilities as well as means of action available to the European Union and the North Atlantic Treaty Organization performed in Chapter 6 was therefore necessary to clarify and define prosperities for the possible articulation of the two evolved over time systems.

Comparative analysis is also performed in Chapter 5 in order to make a comparison of critical theory with traditional theories of International Relations. This Master Dissertation implies Critical Security Studies (CSS) to analyze cyberspace and the impact it has on the relations between the European Union and NATO.

The second method used in this Master Dissertation is the qualitative content analysis. This method has been used in Chapters 4 and 6. According to Hsieh and Shannon, qualitative content analysis is a research method for subjective interpretation of the content of text data through a process of systematic coding classification and identification of themes or patterns[[2]](#footnote-2). Content analyses that we performed to determine the presence of words such as ‘cyber’, ‘cybersecurity’, ‘cyberthreat’, ‘cyber incident’ as well as ‘cyberattack’, themes, or concepts within some given qualitative data permitted to determine NATO and the US’s perception of a threat and actor in the cyber field. The qualitative content analysis findings are visualized in Appendix C.

Quantitative content analysis allowed the author to conduct the comparative analysis. Quantitative content analysis has been performed with Data Mining. Data mining aided the author in revealing core content topic areas in large data sets, and in visualizing how these concepts evolve, migrate, converge or diverge over time. The search was conducted using the following search terms ‘APT’, ‘Adware’, Botnets’, ‘Malware’, ‘DDoS’, ‘Espionage’, ‘Cybercrime’, ‘Phishing’, ‘Zero-days’, ‘Man-in-the Middle’, Ransomware’, ‘Disinformation’, ‘False flag’, ‘Terrorism’, ‘Spyware’ as well as ‘Election meddling’. We used QDA Miner Lite, Free Qualitative Data Analysis Software, which does not require the knowledge of R 3.1.1 or Python programming languages to run the analysis.

The author tested Hypothesis I and II by performing quantitative content analysis. As a result of the study, the author was able to identify a direct correlation between cyberattacks on Estonia, Georgia, Ukraine as well as cyber incidents such as WannaCry, and NotPetyam, and the dramatic increase of ‘cyber’ mentions in the official NATO and EU documents.

Author performed discourse analysis in Chapters 4 and 5. Discourse analysis is a multidisciplinary qualitative and quantitative approach to the study of discourse. Through the analysis of the content of a written or oral discourse, and its context, the student can collect useful information a research. This analysis allows the researchers to highlight key elements of a speech, or to reveal points of comparison or divergence between several speeches or interviews. In relations to this study, discourse analysis permits to test the EU-NATO discourses with regards to cybersecurity and cyber defense. The ‘socially reproduced’ understanding and conceptualization of are EU and NATO are of special importance inasmuch as these are one of the main and crucial international entities in establishing international laws and norms which is highlighted in Chapter 6.

**Literature and sources analysis.** This thesis is based on the analyses of primary and secondary sources. The primary sources are the official EU and NATO documents from 2002 up to 2021 and NATO and EU News Conferences, Speeches and Keynote Speeches. Secondary sources include the analytical studies, such as Europol’s Internet Organized Crime Threat Assessment (IOCTA) and FireEye Mandiant Special Report (FireEye), and monographs, scientific articles, collections of scientific conferences as well as domestic and foreign media materials.

We begin the literature review by examining the EU-NATO cooperation in traditional domains. We then overview how cyber is conceptualized in the field of international relations. We link security critical theory to global cybersecurity and appraise the utility of critical theory in International cyber politics. Third, we analyze the current EU-NATO cooperation in the cyber defense and cybersecurity to find out the existing academic gaps.

Many researchers analyzed the North Atlantic Treaty Organization (NATO) and the European Union (EU). NATO is a military cooperation organization of countries from Europe and North America. NATO was founded in 1949 by twelve countries, including the Netherlands. France, Italy and Great Britain also participated from the beginning, as did the United States and Canada. Over time, more and more countries have joined. The newest member states are North Macedonia (2020) and Montenegro (2017). According to the latest news, Finland and Sweden have started talking about joining NATO amid a special operation of the Russian Federation in the Ukraine. The North Atlantic Alliance, for its part, said it would be happy to do so[[3]](#footnote-3).

The European Union (EU), in its turn, is a partnership in which member states pooled their sovereignty in certain areas and created a normative and legal framework for further economic, social, legal and political iteration. The EU was the latest stage in the process of eurobuilding, launched after World War II, initially by six Western European countries (France, Italy, West Germany and the Benelux countries) to promote peace, security and economic development. Today, the EU consists of 27 member states, including most of the former communist countries of Central and Eastern Europe.

The members of the European Union have a single currency, which unites the 19 member states of the integration association. It is assumed that all members, except Sweden, will introduce the euro when they meet the criteria outlined in Article 140 of the Treaty on the Functioning of the European Union and a special protocol to it. Moreover, 22 EU countries are part of the Schengen area, which allows travel without passport checks within the Union. The states of the Union have a common trade, agricultural and foreign policy. The principle of "common foreign and security policy" was enshrined in the Maastricht Treaty in 1992. Decisions in the field of common foreign and defense policy are mostly taken unanimously.

Most of researchers downplay the role of the Union in comparison to NATO, or even perceive it as non-important partner, when it comes to security. But we have to make a distinction among defense and security providers. According to Thierry Tardy, a Senior Analyst at the EUISS, we need to understand security as a set of policies that are designed to defend and assure the protection of territories and civilians from armed attacks. Security, on its turn, is a set of policies aimed to tackle threats[[4]](#footnote-4). More simply, defense should be regarded as the action of defending, of protecting from attack and direct danger whereas security is designed to not to get threatened or attacked. As we will see in this dissertation, and as it is described by some researchers such as Poptchev Peter, NATO’s cyberpolicy aims to protect its Member States as well as their networks and all other layers which could be potentially targeted. The EU, on the contrary, wants to strengthen cyber resilience and develop common cyber security capabilities to make any kind of cyber incidents impossible to forward on its Member States[[5]](#footnote-5). Thus, we can truly affirm that the European Union is a security provider. That is why the European Union is perceived, according to Ian Manners, Senior Lecturer at the Department of Political Science of Lund University, as a civilian power. That is why the EU stresses upon the idea that the security on the European peninsula can be only guaranteed when the security and global development are ensured[[6]](#footnote-6). However, there are some authors, for instance Simon Duke, that states that the European Union can be longer seen as civilian power inasmuch as it will no longer be able to adequately defend its interests around the globe [[7]](#footnote-7). This notion has become even more relevant today amid a special operation of the Russian Federation in the Ukraine. Ian Manners in his work “The Normative Ethics of the European Union” argues that the Union represents a ‘normative power’ since it acts to extend its norms in international system.

**2.2 EU-NATO Cooperation in the field of Security and Defense**

The most important and essential goal of this dissertation is to identify the cooperation between the North Atlantic Organization and the European Union, but to do so, it is rather important to explore the cooperation between aforementioned entities in the field of Security and Defense.

We need to highlight that to study the cooperation between the European Union and NATO in cyber, it is quite important to explore questions and discussions going on in the field of Security and Defense. Jolyon Howorth, a former Visiting Professor of Political Science and International Affairs at Yale University from 2002 to 2018, proposed a new term which is “Euro-Atlantic security dilemma” to render understanding of this notion [[8]](#footnote-8). Jolyon Howorth as well as other researchers of the EU-NATO defense and security cooperation primarily focus on two research objects: the EU strategic autonomy and the challenges that NATO and the EU might be facing. The most prominent and known research papers on the EU strategic autonomy can be attributed to Vincenzo Camporini, Jolyon Howorth and Barry R. Posen. Barry R. Posen in “European Union Security and Defense Policy: Response to Unipolarity?” affirms that since 1999 the EU intentionally moves in the direction to develop its own means and capacities to conduct on its own a series of complex political military operations outside the Union’s frontiers. In this very publication, Barry R. Posen stresses upon the idea that NATO is no longer needed inasmuch as there is no longer a threat from the communist regimes and that is the main reason for Europe to be autonomous. The author states that the US uses the NATO to concentrate global power within its borders to influence the global political environment.

As for the challenges EU-NATO could be facing, “Euro-Atlantic security dilemma” of Jolyon Howorth illustrates the internal debate on the security and defense building on the European peninsula. Thus, a Franco-British engine have been the most important ones when it comes to the construction of European security and development of defense capabilities. The main challenge in this process of agreement on the ultimate goals of such a process. In most of the cases, the French side is interested in promotion of free and anonymous European projects whereas London fears that fear that a strong Europe will ultimately raise isolationist movements in the USA[[9]](#footnote-9). Thus, the goals of Paris and London might look similar, but in fact they are successful only for short-term. The next challenge is the ambiguous position of the United States towards stronger and anonymous Europe. The first position is their approval: the US approves the desire of certain European states, EU members, of the construction of independent security entities. On the other hand, this could, according to certain researchers, for instance Adam Posen, the President of the Peterson Institute for International Economics since January 2013, challenge the prime role of the USA on the global area[[10]](#footnote-10).

## 2.3 EU-NATO Cooperation in Cyberspace

The analysis of the existing EU-NATO cooperation in cyberspace literature revealed that it is very limited, fragmented and lucks theoretical framework. In most of the cases, the research papers provide technical information which lacks a theoretical analysis.

Lété Bruno and Piret Perni analyze the Union and NATO approaches to cybersecurity and cyberdefense. According to the authors, two entities comprehend the cyber incidents, cyber-attacks, cybersecurity and cyberdefense as critical and strategic issues that could potentially damage or even destroy the defense and security means of organizations. Both organization stress upon the fact that cyber should be one of the priorities for individual Member States of the aforementioned organizations.

It has to be noted that the academic literature illustrates the changes the European understanding of cybersecurity has undergone. According to Gonçalo Carriço, threats in cyberspace generated by the globalization, changed the European approach which used to fully rely on soft power[[11]](#footnote-11). The analysis of the Cyber Diplomacy Toolbox demonstrates that the EU’s approach is currently based on punishment and incorporates hard power tools. Same changes happened within NATO structures. Cyberdefense has been acknowledged at NATO and, according to Karl-Heinz Kamp, a cyberattack on a Member State can potentially invoke article 5 of the Washington treaty[[12]](#footnote-12).

The understanding of cyberspace at NATO and the European Union is also analyzed in the academic literature, but that notwithstanding the knowledge remains fragmented. It is clear that two entities do not comprehend cyberspace in the same manner. For the European Union hackers and cyber criminals are the main actors, whereas NATO sees individual states and state-sponsored groups as the most important actor. According to Siim Alatalu, all the cyberattacks (Ukraine, Estonia, Georgia), which largely contributed to the development of this topic at NATO, were attributed to the Russian Federation. According to the author Russia is the main reason of NATO to perceive states as primary actors[[13]](#footnote-13). It has to be noted that it is not possible to justify if Russia truly conducted those attacks on Estonia, Georgia and Ukraine. In addition, it should be said that this approach has been getting more central role in NATO’s actor’s perception in cyberspace insofar as its Member States have been targeted by the state-sponsored groups (the USA, France, Germany as well as Australia)[[14]](#footnote-14).

The European Union stresses upon the idea of hackers and cyber criminals to be the most dangerous actors in cyberspace. According to Europol’s European Cybercrime Centre (EC3), hackers and cyber criminals cause the Member States most harm[[15]](#footnote-15).

In conclusion, we would like to highlight once again the evident academic gap in the literature on the cooperation between NATO and the European Union in the field of cybersecurity and cyberspace. It is not currently clear how cyberspace is perceived by both member states and organizations like NATO and the EU.

**4. Background**

First and foremost, the cyber threat environment is intensifying dramatically. In the last decade, cyber incidents have become more complex, more disruptive, and in many cases more political. In the past decade, cyber incidents as well as cyberattacks such as on Estonia in 2007, Georgia 2008, Ukraine 2014, 2015, 2021, 2022, the interference in the American and European elections as well as cyber incident as WannaCry, and NotPetyam rendered it clearer that cyberattacks have become way more disruptive, political and targeted[[16]](#footnote-16).

Cyberspace is a new reality that is difficult to comprehend because of its intangible and highly technical nature, and also because of its great semantic vagueness in the literature. Indeed, there is no objective and consensual definition of cyberspace; on the contrary, there are multiple definitions depending on the disciplines, the actors and the countries. However, it can be argued that cyberspace is both the Internet and the space it generates: an intangible space in which deterritorialized exchanges between citizens of all nations take place at an instantaneous speed that abolishes any notion of distance.

There is sometimes a multi-layered representation, which makes it possible to render the entanglement of the different dimensions of cyberspace but also of the issues that are linked to it.

The first layer is physical and forms the basis of the Internet, a global network of interconnected networks of which cyberspace is the product. It is composed of cables, nodes, computers, servers and commutators that are physical assets, localized and subject to the constraints of physical and political geography. It was designed with openness and maximum information flow in mind, without any built-in security, which explains the ease with which data can be sucked in unencrypted via cables and routers.

The second layer is logical and applicative. It includes the services (applications, software, interfaces, programs) that enable the transmission of data between two points on the network, to make the information travel, in small separate packets, from its sender to its recipient. Here again, certain aspects can be geolocated (software used, company providing it, paths taken, data storage, etc.). However, the logical architecture is based on a common foundation, an essential harmonization that allows all computers in the world to understand and exchange data with each another, the Internet Protocol (TCP/IP).

The third layer is cognitive and semantic, it is the world of the users of the logical layer, the world of information, social networks, discussions and exchanges in real time in the world. It is the most intangible layer, the most difficult to geolocalize, and yet not necessarily the least relevant when it comes to determining in which language the majority of content accessed by this or that part of the planet is, who are the «friendliest» countries on Facebook, where disinformation campaigns or cabals against a movement, a state or an institution start.

Cyberspace is therefore both a material reality that can be located and an intangible space of exchange that is complex to grasp. It can refer to a set of computer networks (and tablets, smartphones, etc.), human networks, data and information flows, everything that circulates through interconnected computer networks and that uses a common language. With the development of the Internet of Things, more and more devices of all types are connecting to networks and the amount of data available is dramatically expanding. Depending on who uses it and why, the term cyberspace can refer to a totally different reality or imagination in a certain conceptual blur.

The geopolitical approach therefore brings an indispensable tool to the apprehension of cyberspace, that of representations. A representation is "a construction, a set of more or less logical and coherent ideas" that has a function in geopolitical conflicts. It "describes, expresses a part of reality, in a vague or precise, distorted or exact way". It is thus fed by objective facts while keeping a deeply subjective character. Representations are therefore not neutral, they shape as they can serve the strategy of actors, in order to convince, worry, enthuse or mobilize actors (citizens, soldiers, voters...).

It has to be noted that cyberspace is not a territory in the geographical sense of the term, namely "an area on which a human group lives and which it considers to be its collective property", or for States a portion of terrestrial space delimited by its borders and over which its authority and jurisdiction are exercised. It is not truly a geographical space either. However, we find a whole terminology borrowed from the geographical territory, particularly the sea and space. We "navigate", we "surf", we use "routes", "gateways", "channels" in cyberspace. Because if cyberspace is not a territory, it is perceived and used by different actors as the representation of a territory, and for diametrically opposed reasons.

The concept of cyberspace first appeared in the writings of a science fiction novelist, William Gibson, who in 1984 described in Neuromancer a three-dimensional space of "infinite complexity", generated electronically, into which his characters enter by connecting via computer[[17]](#footnote-17). He thus offers a mental representation of the data and information stored at the heart of the computer systems of all humanity that will be appropriated by generations of Internet users.

This representation permeates the speeches and the imagination of the Net pioneers. In 1990, when the Internet was still only a club of a few million users, the Electronic Frontier Foundation (EFF) was created. A direct reference to the pioneering front that, according to historian Frederick Jackson Turner's thesis, formed American democracy, the association fights for the defense of freedoms in the digital world[[18]](#footnote-18). Its missions reflect the spirit in which the network was created, in the atmosphere of the counterculture of the 1960s and 1970s on Californian campuses, a spirit of openness, freedom of exchange and expression, and self-management that goes to the very heart of the Internet's architecture. The network is designed to escape control, decentralized, so that information can always bypass blocking. John Perry Barlow, a founding member of the EFF, even published a "declaration of independence of cyberspace" in 1996 in which he asserted that the laws and sovereignty of governments do not apply. Criticized at the time for his incredible optimism, he has since conceded that "we're all getting older and wiser". Many hacktivists, however, still take this statement literally and actively fight government interference in the regulation of cyberspace.

From the mid-2000s onwards, the term cyberspace paradoxically reappeared in the discourse of governments, as the representation of a territory that carries threats, a territory to be controlled, monitored, and conquered, a territory over which borders must be reestablished and sovereignty reasserted. The 2007 attacks against Estonia, which paralyzed the servers of public administrations, banks and other services in Estonia, raised awareness of the vulnerabilities that dependence on computer networks could entail for states. The attacks against Georgia the following year showed how cyber-attacks could support military forces in armed conflict, confirming the entry into the political and strategic realm of a concern that had until then remained essentially in the hands of experts and technicians.

Cyberspace has thus become a geopolitical issue; it is at the same time a stake in power rivalries, a theater of confrontation and a formidable weapon in geopolitical conflicts.

After having analyzed the concept of cyberspace, we are to investigate the most prominent cyber-attacks on European Union’s and NATO Member states as well as on their allies. There is no doubt that over the past years, more precisely over the past two decades, we have seen more and more cyberattacks on the United States of America. EU Member Statas also had to face same challenges as their closest allies. It needs to be said that the United States turned out to be more ready to face cyber challenges then the EU or NATO inasmuch as it could benefit from its sovereignty, whereas the EU and NATO had to take steps to develop cybersecurity policies at the national level while simultaneously pooling their sovereignty through the North Atlantic Treaty Organization (NATO) and the European Union (EU) to bolster their defenses.

Three of the most prominent examples of cyber aggression between nation-states are those on Estonia (2007), Georgia (2008), and Ukraine (2014, 2015) by Russia and its proxies.

On April 27, 2007, the first cyber-attack targeting a state structure took place in Estonia. This large-scale attack against the infrastructure of a third country was attributed to Russia by the Estonian authorities from the very beginning. The Estonian authorities, wanting to mark their independence from their Soviet past, had decided to move a Red Army monument from the center of the capital in Tallinn to the suburbs. This decision showed Estonia's rapprochement with the Western powers. The response did not wait. Russia would have temporarily hired the services of botnet owners, networks of PCs, to increase the number of computers involved in the denial-of-service attack against Estonia. This type of cyber-attack consists of saturating the target's servers with false requests to the point of making them unavailable. In this case, it is very difficult, if not impossible, to counter this type of attack.

It needs to be stated that distributed denial of service (DDoS) attacks are one of the most common forms of cyber-attack. To make these cyber-attacks successful, the hackers deliberately roll out malicious software to servers or computers and having that done, they create a network of infected machines. It could be done using different ways: spreading spam with infected attachment etc. The hacker, using those infected machines (the botnet), attacks websites and make them crash under immense traffic[[19]](#footnote-19).

According to the Asymmetric Threats Contingency Alliance (ATCA), an association of international experts based in London, it is the Russian authorities who have directly contributed to this. They would have rented millions of computers, which were used to defend Russian interests.

However, we have to note that there is no evidence for such a claim. It is probable that Moscow did not directly organize the attack that blocked all Estonian institutions, but rather allowed it to happen. It is absolutely impossible to justify that these attacks came from the territory of Russia or even to speak about a possible coordination of actions by a governmental service. To this day, the debate about the involvement of the Russian authorities is still raging in the West, although it is generally accepted that the state gave its consent to this action.

This first attack is a textbook case. It has marked the governments that have subsequently understood the stakes of the new cyberwar. It became necessary to protect themselves. States and supranational institutions, notably NATO, became aware of their lack of preparation for this type of aggression and decided to impose their sovereignty in cyberspace.

However, when cyber-attacks are aimed at large and indiscriminate targets, as was the case in Estonia, they are basic. They are only denial of service attacks or even spamming attacks, producing only minor effects. When massive DDOS attacks targeted Estonia in 2007, the country was only affected for a few days, with no lasting damage. From a technical point of view, such an attack is benign. It was only a common act of cyber piracy and not a "third world war that went unnoticed", as Jaak Aaviksoo, Estonian Minister of Defense, hastened to call it[[20]](#footnote-20). Anyone can be a cyberwarrior. With little means, a lot of can be done in cyberspace.

As a result of this and the cyber-attacks on Estonian public and private institutions in April and May 2007, the defense ministers of the NATO allies agreed in June 2007 that "urgent work" was needed in this area. As a result, NATO approved its first policy on cyber defense in January 2008. Since then, the NATO Cyber Defense Center of Excellence has been located in Tallinn. Here, it is the West that is playing on Russian perceptions, placing itself on their land borders and making them fear retaliation just by its presence. It is all a question of symbolism in interstate relations.

Since 2008, NATO has also been involved in another project: the drafting of the Tallinn Manual. Written by a group of experts mandated by NATO, it proposes a transposition of international law to cyber conflicts. Its final version was made public in 2013. Reflecting the divergent representations of Russian cyberspace between Russia and the West, an official of the Russian Ministry of Defense, Konstantin Peschanenko, said: "The issue of cybersecurity is the most topical at the moment. It is especially important to prevent the militarization of virtual space, while the Tallinn manual is a step in this direction. Its approach to the issue is far from perfect. And the assessments made in it seem to be one-sided"[[21]](#footnote-21). According to the Russians, it is the Atlanticists who are instrumentalizing cyberspace.

However, the Russian state is increasingly accused of interference. In the summer of 2008, "the conflict between Russia and Georgia demonstrated that cyberattacks have the potential to become a major component of conventional warfare," according to NATO. This first governmental cyberattack, attributed to Russia, has indeed allowed states to realize the new challenges linked to the Internet. A Tallinn 2.0 Manual was even written in 2017, covering operations not necessarily involving violence or occurring in peacetime. This is the category into which most of the cyberattacks that states experience on a daily basis fall. States want to respond. As a new battlefield, cyberspace is increasingly standardized and analyzed. It has become a strategic issue in its own right since 2007.

To go beyond passive self-defense, States are likely to seek strong international support, particularly within the European Union: On May 24, 2007, the Parliament of the European Union adopted a resolution strongly condemning the siege of the Estonian embassy in Moscow, the cyberattack against Estonia and the refusal of the Russian authorities to cooperate with Estonia. The resolution also "considers the attacks against one of the smallest EU member states as a test for the solidarity of the European Union" and calls for "a study on how such attacks and threats can be addressed at the European level. Nevertheless, the European Parliament refrained from commenting on the fact that this attack was facilitated by anonymity in cyberspace[[22]](#footnote-22).

Even today, the example of Estonia is emblematic of this community of hackers defending Russian interests against material acts deemed to be in contradiction with the Russian nation. However, more than ten years after this cyberattack, it is still difficult to discern the level of involvement of the authorities. The important technical difficulty of attributing disruptions within cyberspace is the primary reason for this.

By analyzing the most significant and prominent cyber-attacks on the EU and NATO, as well as their allies, we can identify and analyze the risks that are associated with cyber-attacks.

Cyberspace reveals a world of opportunities, but also of threats. In terms of security and defense, it constitutes a new area of military operations, joining the traditional physical areas (land, sea and aerospace). This consideration as a military operational domain is due to the growing importance of technological advances in politics and security and the increase in cyberattacks and disinformation campaigns that have taken place in recent years, whose main objectives have been the destabilization of political regimes and the theft of data and information. Behind these attacks are state and non-state actors, who take advantage of the lack of physical borders, the difficulty of attributing cyberattacks, and the lack of governance and competence over cyberspace to advance their political, ideological and economic interests. These circumstances show that, although it is a space common to all, the sovereignty of cyberspace depends on the ability of different actors to access it.

Hybrid threats are multidimensional challenges resulting from the convergence of different elements. In other words, a state or non-state actor that uses a mix of conventional and unconventional weapons to conduct an attack is conducting hybrid warfare. With the emergence of cyberspace, the concepts of hybrid threat and cybersecurity have become closely related, as these threats, which primarily take the form of cyber-attacks and disinformation campaigns, are a constant in cybersecurity challenges. In the case of cyber-attacks, these are often aimed at interfering in elections, stealing data or spying.

The very complex nature of these threats shows that we are facing a growing problem. We are in a digital world, which has created a new order - the network order - that requires us to design new states and new borders. Social networks, which often serve as a channel of communication and recruitment for terrorist groups such as ISIS (recognized as a terrorist organization and banned in Russia), are an example. The problem is the lack of physical borders and the resulting lack of jurisdiction, which is an advantage for cyber attackers or, in this case, terrorists seeking to spread messages, and an additional difficulty for institutions tasked with providing cybersecurity. This is why it is important to strike a balance between privacy and cybersecurity.

Another very relevant example today is the economic cyber espionage campaigns against laboratories in different countries around the world that are working on a vaccine for COVID-19, where the goal is to steal technology equipment that will save time and research.

The other major threat to cybersecurity is disinformation campaigns, which are intentionally spread. Disinformation badly undermines human rights and many elements of good quality democracy; but counter-disinformation measures can also have a prejudicial impact on human rights and democracy[[23]](#footnote-23). Disinformation moves emotions and personal beliefs more than objective information. In this context, cyberspace plays a key role, as it gives disinformation a high transmission speed and increases its reach. In recent years, the problem of disinformation has become more complex due to digitization. Behind these campaigns lies an intention to destabilize politics, often using conspiracy theories that distort the reality of what is happening around us.

One example of misinformation is the false letter that NATO Secretary General Jens Stoltenberg allegedly sent to the Lithuanian Minister of Defense a few years ago, announcing that the Alliance was withdrawing its troops from the country because of the pandemic. This letter was sent by e-mail to various Lithuanian media and was aimed at discrediting NATO and destabilizing the situation in the Baltic country. In this regard, Paz Esteban, director of the National Intelligence Center, emphasized at the aforementioned seminar that "democratic states are the most vulnerable to disinformation because they do not censor the content that circulates on the Internet and do not control the media"[[24]](#footnote-24).

This means that the media have the task of denying false information and the duty to use their influential role in public opinion. This is a shared responsibility: of the media, national authorities (as well as international organizations) and the citizens themselves. On the one hand, the authorities must raise public awareness of the risks of Internet use and must cooperate in international bodies with other member states to address these challenges. On the other hand, the individual must demand the necessary security from the media that give him access to the networks and have a critical attitude towards what he reads on the Internet, especially if the source is of dubious origin.

Thus, cyber-attacks can cause electrical blackouts, failure of military equipment, and breaches of national security secrets. They can result in the theft of valuable, sensitive data like medical records. They can disrupt phone and computer networks or paralyze systems, making data unavailable, and that is why the development of cybersecurity in NATO and EU operations has distorted the growth of cybersecurity as a major policy concern for the US and other governments. The digital revolution has also changed the fundamental conditions under which governments operate, requiring greater cross-border interdependence and connectivity. European countries have responded to the need for greater coordination and cooperation with new initiatives at national level and under the aegis of NATO and the EU. However, the relationship between national capabilities and sovereignty and the mandates of these two international organizations remains unresolved. NATO and EU efforts to integrate cyber security into existing activities have so far proved insufficient to fully address the growing cyber threats.

**4.1** **NATO Cyber Defense Policy**

It needs to be stated that cybersecurity at NATO has several quite unique features that make this topic relevant. First of all, it is an interesting topic inasmuch as until very now, scholars have extensively studied North Atlantic Treaty Organization in terms of its deterrence doctrine, its campaigns in Yugoslavia and Libya, its enlargement, etc. Cyber is a recent topic and, as a result, it has not yet been studied much even though there are some very good academic contributions such the works of Rasmussen 2001, Coker 2013, Kempf 2014, Pomarède 2014 as well as the other very prominent researchers. It should be noted that this is a topic that has only recently arrived on the political agenda of NATO, one of the international organizations that has elevated cybersecurity to a priority (see Resolution 387). Until now, NATO has focused on the defense of its own information and communication systems through the principles of prevention and resilience, which means, respectively, that NATO seeks to manage risk proactively and prepares to respond in the event of an attack. What stands out most when looking at NATO's cyber defense is the strategic ambiguity as well as the complexity of governance. It is from 2007 onwards that things accelerate politically and militarily with regard to cyber.

Etymologically, "cyber" means to govern, to direct. It is therefore very relevant to look at this topic in the context of political science research. However, it is a technical and complex topic. First, cyberspace is not easily defined. We owe this term to the American and Canadian author William Gibson who, in 1984, coined the term in Neuromancer, a dystopian fiction. Alix Desforges tries to give a definition of cyberspace: "If the Internet is easily definable and identifiable, cyberspace appears more encompassing and more virtual. It evokes both a virtual, dematerialized, borderless, anonymous 'world' of freedoms, sharing, and communication, but also a dangerous and nebulous 'space' in which socially repressed behavior can be expressed without repression"[[25]](#footnote-25). Typically, two visions clash about this virtual and dematerialized universe that is cyberspace: "Some see it as the promise of increased democracy, economic progress, and a pacified world, but it also heralds the advent of widespread surveillance, an ultimate Big Brother, and an absolute tool for crowd control and manipulation - a representation reawakened by the publication of Edward Snowden's documents as to the NSA's intelligence practices". We will focus on highlighting the characteristics of cyberspace in order to show how this space, which is originally exclusively technical, has become a social, political, military and strategic space.

First, cyberspace is composed of several layers: the physical layer encompasses all physical infrastructure, such as computers, undersea and land cables. This layer can be mapped fairly easily, but it is very difficult to reach the physical layer through a cyber-attack. Next, we find the logical or software layer, which represents all the technologies that allow information to be transported or stored. Finally, the semantic or cognitive layer is the most difficult to grasp because it concerns information, ideas, exchanges. Cyberspace is universal: "Every point on the globe reaches any other"[[26]](#footnote-26). This also implies that networks are interconnected with each other, and that it is difficult to distinguish between national and international networks. In this sense, it is possible to argue that to some extent cyberspace knows no borders, or at least not the borders between nation-states as we know them. As we shall see, borders do exist in cyberspace, and they tend to be reinforced. The theme of territorialization and borders necessarily leads to talk about sovereignty, and more precisely digital sovereignty. According to Kempf, cyberspace represents an opportunity for States to be more autonomous: "cyberdefense belongs, along with nuclear power and intelligence, to the heart of State sovereignty" (Kempf: 138). We want to show that cyber has in fact been militarized with a view to being an integral part of this sovereignty, but that in no way is cyber security inherent to state defense.

Next, we need to provide a brief portrait of the different actors. We believe that the typology proposed by Dorothy Denning is the most appropriate for capturing the difference in nature and intention between actors. The expert proposes 6 categories:

- First, we find what Denning calls "insiders", who are individuals who have access to documents or procedures. According to Denning, this accounts for 80% of cybersecurity incidents. Without giving a statistic, Hunker (2013) states that the cyber-attack to be most wary of is from the inside;

- Second, hackers are individuals who try to break into or gain access to systems, as opposed to insiders. This category is very vague and can be applied to the following categories;

- Then come the spies, whether they act for economic or political reasons, their goal is to steal data while remaining invisible;

- Denning then distinguishes criminals who act with the sole purpose of obtaining money, whether by ransom, selling information or stealing credit card data;

- Terrorists fall into this category because they use cyberspace to support their physical operations on the ground. This case, which we will study in detail, shows the limit of such a categorization since in most cases, terrorists use cyberspace to finance their operations (we could therefore classify them as "criminals") and to recruit;

- Finally, the nation-states, which Denning considers to be the ones to be most wary of, since some of them, about twenty, including Russia, China and North Korea, would have cyberwarfare capabilities[[27]](#footnote-27).

Moreover, there are different cyber-attacks. Hunker identifies 2 types: passive attacks that seek to copy or steal data without disrupting the system, the network or even without being noticed (cybercrime such as bank data theft, cyber espionage). On the other hand, there are the so-called disruptive attacks whose goal is to disrupt networks and systems, or even block them for the purpose of vindication (vandalism, revenge, ransomware, hacktivism)[[28]](#footnote-28). Nations such as North Korea and China are very active in espionage and in developing disruptive tools.

Finally, the most important characteristic in the study of cybersecurity is the opacity that results in the difficulty of attributing attacks. In other words, it is technically difficult to identify one's attacker. NATO recognizes this as a problem in developing its strategy: "The most worrisome aspect of cyberspace is that the attacker has the advantage over the defender. Attackers only need one weak link to penetrate the network, while defenders have to guard against all vulnerabilities. These attacks, moreover, move at the speed of light, leaving little or no time to react" (Annual Commission Report 2011 - Information and National Security, §31). In this sense, this characteristic gives the advantage to the attacker, that surely has legal consequences but above all strategic consequences because it generates a sense of uncertainty and in fine, the political decision will carry a risk, because all the elements of the attack cannot be known.

However, as Amoore and de Goede state: "Paradoxically, however, this recognition of incalculability does not lead to an abandonment of calculative techniques in favor of, for example, a political-philosophical recognition of the fragility of modern life"[[29]](#footnote-29). Indeed, we will see that NATO, inspired by the United States, shows a desire to master uncertainty by trying to manage these potential dangers, which we will call risks. Based on poststructuralist authors, we will show that risk management is a way of governing.

We asked ourselves what strategy NATO has in place to combat cyber-attacks. This question led us to analyze how NATO, in a context of globalization, perceives threats and builds its cyber defense doctrine accordingly. Taking part in a vast reflection on the link between technologies and security, our research is intended to be an academic contribution to the discipline of international relations. The relevance of this topic is primarily due to the current context and the growing importance of cyber in international relations. We believe that cyber allows us to redistribute the cards in terms of strategy, particularly military, but also on an international scale. It is possible to see the study of cyber as a way to highlight the vulnerability of great powers. For example, cyber allows us to understand North Korea, a technically hermetic state, as an actor that could have the upper hand over highly connected states. Cyber thus allows us to question to some extent what we understand about international relations. There are very few publications in this discipline that understand cyber as a risk. We believe that studying cyber as a risk allows us to move away from the technical and micro aspects of this subject in favor of a more global understanding. In other words, our research allows us to focus on the political issues that have invested cyber. To do so, it gives a consistent place to doctrinal and strategic elements by conducting a discursive study.

**4.1.1** **Cyber-attacks and Article 5 – blurry but consistent position of NATO**

NATO adopts a purely defensive strategy in the cyber context and tries above all to protect its own networks and data. The notion of deterrence remains fundamental in NATO's cyber strategy and is in line with the Alliance's collective defense vocation. Vincent Joubert, a research fellow at the Foundation for Strategic Research (FRS), in an Alliance research note, points out the need to develop "a robust defense system with improved security standards, focusing on prevention, resilience and non-redundancy. To this deterrence by denial must be added deterrence by punishment, based on a capacity to respond very severely to any form of cyber-attack. The role of the United States in this process of deterrence is explicit, with national texts stating that any form of hostile act in cyberspace could lead to collective retaliation, under Articles 4 and 5 of the NATO Treaty. The pursuit of these two types of deterrence maintains a form of deliberate ambiguity in NATO's strategy. However, this equivocal interpretation of articles 4 and 5 can be perceived as a conscious and assumed will to leave any form of potential aggressor in a state of uncertainty about the possible consequences of an attack against the interests and cyber capabilities of the alliance, but also as a lack of political will and a chronic inability to assume the possibility of a collective response. Therefore, this obvious ambiguity could lead a potential adversary to prefer, within its repertoire of action, a cyber-type of attack rather than a conventional approach.

Some experts suggest transposing the MC 14/3 strategic concept, initially intended for nuclear risk, to the cyber field, allowing for retaliation "either at the level chosen by the aggressor, or - given the stakes of the conflict and the presumed intentions of the adversary - to proceed with a deliberate escalation (symmetrical or asymmetrical), or to inflict major damage on the aggressor from the outset"[[30]](#footnote-30). Here again, a simplistic transposition of a strategic concept to the cybernetic framework does not allow for an absolutely coherent response. Indeed, the current methodological vagueness remains persistent in the definition of the threshold, which is nevertheless essential for the implementation of a proportionate response, in the absence of objective and scientific measurement tools. Lucas Kello, senior lecturer in international relations at the University of Oxford, deplores in this sense "the absence of known or agreed conversion tables that could guide the application of the principle of equivalence", which further complicates the potential response, which could be perceived as much greater than the damage caused by the targeted State, especially if it takes place in a conventional framework.

One of the major characteristics of cyberspace is the obvious difficulty of designating the enemy and reinforces the legal difficulty of a legally justified collective response. Indeed, according to Didier Danet, professor at ESM Saint-Cyr, "the combination of [Defense and Security] / attack continuum leads to a form of indistinction of the adversary (who can be an individual as well as a state power) and who is likely to attack without fear of retaliation or reprisal the armed forces as well as the vital interests or the population of a country, however well protected it may be". Although the author of the cited article was keen to qualify this hypothesis, the designation of the enemy in cyberspace poses a major problem, particularly in the applicability of Articles 4 and 5. Indeed, knowing whether an attack has been perpetrated by an activist group or a state structure requires considerable means of analysis and a margin of error exists, thus leaving a damaging imprecision, all the more so as false-flag attack capabilities can be much more easily achieved in the cyber field than in a conventional framework. On the one hand, it is extremely delicate to determine the precise origin of an attack, as "the international ramifications of botnets (networks of denial-of-service attacks) are such that any mapping of actions in cyberspace is quickly subject to methodological limitations". On the other hand, if it turns out that a majority of the attacks are localized in a particular country, the exact designation of the person responsible and/or sponsor of the attack is not obvious. It is indeed difficult to succeed absolutely in "proving the formal links between state resident and state authority in the case of cyber-attacks". Therefore, the difficulties in providing clear evidence of the guilt of a state sponsor in the field of attribution pose decisive questions for NATO in the perspective of a collective response.

**4.1.2** **NATO's Expanding Role in Cybersecurity**

The Bucharest Summit in early 2008 saw the approval of NATO's cyber defense concept, leading to the development of its cyber defense policy. One of the immediate consequences, and the Alliance's most visible response to the attack on Estonia, was the creation of the Cooperative Cyber Defense Centre of Excellence (CCD COE) on 14 May 2008 in Tallinn, Estonia, on the initiative of eight member countries. The Centre's mission is to enhance capabilities, cooperation and information sharing among NATO member and partner countries. It also contributes annually to the organization and conduct of the Cyber Coalition exercise. France became a full member of the CCD COE in June 2014. Today, the center has 18 members as well as 3 Alliance partners[[31]](#footnote-31).

The cyber defense policy and action plan were adopted in 2011, but it was at the Wales summit in September 2014 that the most significant decision was taken for the Alliance. In a strengthened version of the policy, cyber defense is recognized as part of NATO's core task of collective defense, opening the possibility of invoking Article 5 of the Washington Treaty. It would then be up to the North Atlantic Council to decide, on a case-by-case basis, whether the circumstances for such an invocation would be met following a cyber-attack.

This enhanced cyber defense policy also affirms that, for NATO, international law applies in cyberspace, but also that the Alliance's main task is the defense of its networks and that it is up to each member country to develop and improve its national cyber defense capabilities, a commitment made at the 2016 summit. Thus, through its training capabilities, but also by improving and strengthening information sharing and mutual assistance, particularly during the annual Locked Shields exercise, NATO is contributing to strengthening the overall resilience of the Alliance. The policy thus implemented also emphasizes the need for the Alliance to develop its cooperation in cyber defense, both with international organizations (UN, EU, OSCE, etc.) and with industry. This last cooperative aspect has been formalized through the NATO Industry Cyber Partnership (NICP), a partnership in which member countries commit to strengthening their ties with industry by relying on existing NATO, state and industrial structures. This partnership promotes, among other things, information-sharing activities, exercises, training and education, as well as multi-national intelligent defense projects.

At the 2016 Warsaw Summit, another historical milestone was reached with the recognition of cyberspace as an area of operations in which NATO must be able to defend itself as effectively as it does in the air, land, and sea environments. It was historic, because for the first time in its history, NATO added an operational domain to the three traditional ones. Cyber defense is thus fully integrated into the operational planning and conduct of Alliance operations and missions. The most notable consequence of this recognition was the announcement in October 2018 of the creation of the Cyber Operations Center, or CyOC. Housed at SHAPE in Mons, the center's primary purpose is to provide the information necessary for situational awareness in cyberspace. Its mission is also to coordinate the efforts of the many existing and well-established elements, both within the NATO command structure and in each member country, to execute the Alliance's cyberspace operations and missions. Because NATO does not have sufficient cyber defense assets of its own, Allies agreed that sovereign capabilities would be made available to the Alliance on a voluntary basis for the conduct of cyber operations, as is done with traditional assets in the other three domains.

Concerning the defense of its own networks, NATO relies on the NCIRC. As part of the NATO Communications and Information Agency (NCIA), it protects NATO's networks by providing centralized and permanent cyber defense support for all Alliance sites through its technical center. However, NCIRC's role is not limited to responding to cyber incidents. Its coordination center is effectively responsible for coordinating cyber defense activities within NATO and with member countries.

Since its first steps in cyber defense in 2002, NATO has developed an ambitious cyber defense policy. The physical means for its implementation exist and the most recent ones are growing. It now remains for the Alliance to acquire the legal and diplomatic arsenal that will enable it to legitimize its action in cyberspace, but also, from a military point of view, a doctrine for operations in cyberspace that will be a valuable guidance document for NATO commanders.

The legal aspect is more complex to deal with. Indeed, the goal of the Alliance is to define what would be a state of cyber warfare, which would allow it to conduct, if necessary, preventive operations in cyberspace

However, it is crucial to define the threshold beyond which a malicious act falls into armed conflict and, at the same time, how NATO can respond to acts that would then fall into the realm of cybercrime. In this sense, the Alliance is considering how it might respond to malicious acts in a systematic way, without triggering a disproportionate conflict. The Allies' goal is to develop as broad a range of responses as possible, so that they can develop measures to counter any attacks against them in a manner consistent with international law and the principles of restraint and proportionality, and thus deter further cyber-malicious acts.

NATO now has the capabilities to be resilient to cyber-attacks against it. The Alliance continues to improve these capabilities and to develop new ones. This construction must continue while dealing with the new threats of cyberspace. The Alliance's resolve is, indeed, as strong in cyberspace as it is in every environment where it has interests. NATO must now demonstrate that its resolve to deter aggression against its members remains and is finally expanding into a fourth operational area.

In conclusion, NATO's role and capabilities in the field of cyber defense remain unclear. While there is a consensus on the primarily defensive nature of the Alliance in this area, two blocks seem to be emerging in the objectives to be achieved by NATO. Indeed, the global defense of NATO's networks is an objective widely shared by all members. However, while the Baltic, Central and Eastern European countries would like to see an expanded global role for NATO, military powers such as France and Great Britain refuse to give NATO too proactive a role in protecting their networks, in the name of sovereignty and for fear of a potential erosion of their national independence. In a system based on a common decision involving all the member states, the ability to find a political consensus remains extremely problematic and hinders any form of increased integration, which can be very damaging for certain small states with necessarily limited means.

**4.2 EU Cyber Security Policy**

"Cyber crises know no borders", explains Mr. Juhan LEPASSAAR, Director of ENISA. The European Union is an open space where goods and services can circulate freely. Software and data can therefore be transmitted very easily within the EU, which means that they are more vulnerable to external attacks. A virus that appears in Poland can be found a few minutes later in Portugal without passing any protection barrier.

The European Network and Information Security Agency (ENISA) is the European cyber security agency created in 2004. The original objective of this agency is to analyze and evaluate the methods of each country in cyber defense. But beyond its advisory role, it is not able to act in the field in direct support of potential attacks.

Because in a European Union without common armed forces, cyber defense is still entirely a matter of national sovereignty. Each country therefore has its own agency and its own policy. France, for example, has a national agency for information systems security (ANSSI).

This is a weakness because the unity of the cyber world implies large-scale attacks, affecting areas that can extend to several continents. A Union that cannot protect itself from external interference during elections or that can be overwhelmed by a computer worm at any time is susceptible to attacks that can destroy its economy or paralyze its armies at certain critical moments.

In this chapter I would like to answer the following research questions: Where does the European Union stand today? What is the European position on cyber cooperation, and what could EU expect in the future?

**4.2.1 Lack of EU competence in cybersecurity regulation**

As the European Union does not have its own cyber defense, only cooperation organizations, each State is responsible for its own protection. Therefore, there is a great diversity of protection between countries. We can distinguish three cases. Western Europe, at a rather advanced stage and which has become aware of the extent of the danger. Central Europe, which relies on protection within the framework of NATO. And the very particular case of Estonia.

It has to be noted that some countries in Central Europe have a different approach. For some nations, cyber security is the business of civilian authorities (hence the idea of cyber security and not cyber defense). Cyber-attacks are criminalized and dealt with internally without any link to the military. For example, in the Czech Republic, cyber defense is the responsibility of the national security agency and the minister of the interior, while the minister of defense only deals with issues related to NATO. Slovakia places cyber defense in the hands of the minister of finance. In Hungary, cyber defense is mainly based on international cooperation (especially from NATO) and consists of small national authorities. Cyber defense issues are analyzed under the spectrum of economic and security danger more than on the issue of protection of state sovereignty. It is important to note that some countries such as the Baltic States (including Estonia mentioned earlier) and Poland still organize a more sustained defense. But the region remains reluctant to respond to immiscions in their cyber space. Of the hundred or so attacks that were recorded in this region in 2017, less than a quarter were dealt with by state authorities.

In recent years, the EU has adopted a number of policies and regulatory measures related to cybersecurity. These are mainly in the areas of the internal market and criminal justice to enhance the security of citizens, businesses and public administrations in the digital environment. However, these policies and regulations lack coherence, resulting in a multitude of redundant and contradictory obligations. A recent example of this lack of coherence is the European Commission's proposal to give law enforcement authorities cross-border access to data (electronic evidence). The analysis of this proposal revealed that the enhanced cooperation regime allowing EU Member States rapid access to supplier data would prevent Member States (MS) "from assuming responsibility for the effective protection of fundamental rights on their territory" and would lead to legal uncertainty for both service providers and individual users.

It is often argued that consistency in cybersecurity policy is difficult to achieve because of different understandings of both cybersecurity and its scope. Many definitions of "cybersecurity" are used at the EU level, as well as at the national level, by the EU institutions, stakeholders, and EU Member States. Definitions of cybersecurity vary and depend on the addressee, the context and the area of expertise in which they are used. In the field of cybersecurity in the EU, discussions can include various aspects such as cyber resilience, cybercrime, cyber defense, cyber security in the strict sense, and other general cyberspace issues.

However, policy documents and legislative measures often only address certain aspects of the cybersecurity domain and are adopted without being considered in the overall legal framework. Examples include the areas of cybercrime, network and information security measures (targeting critical service operators or providers of critical and digital infrastructure), and electronic communications, which encompass issues of privacy and data protection. The conceptualization of cybersecurity is becoming increasingly complex as the boundaries between the different domains of cybersecurity become blurred. The different meanings of the term "cybersecurity" can have advantages and disadvantages. The term has the flexibility to adapt to changing circumstances. However, a constantly evolving term can become overly inclusive or broad, thus impeding consistent regulation in this area. It also creates friction between the power of the EU and that of the member states, especially in the area of national security. Therefore, the ambiguity around the term "cybersecurity" in the EU needs to be removed in order to clarify the responsibilities of regulatory institutions.

The difficulty in creating comprehensive and coherent cybersecurity policies is further compounded by the uncertainty over the EU's competence to legislate on cybersecurity issues. The EU only has the competence conferred on it by the member states in the treaties. It can have exclusive competence, shared competence, or competence that is limited to supporting, coordinating, or complementary actions. As cybersecurity is not attached to any specific area, the EU is looking for a permissible legal justification for the adoption of cybersecurity regulatory measures in well-defined areas of competence. For example, the European Commission's proposal for Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a common high level of security of networks and information systems in the Union (NIS Directive) asserted that the multiple practices of member states with respect to cybersecurity measures hinder the protection afforded to consumers and businesses, thereby reducing "the overall level of security of networks and information systems." In other words, it suggested that additional (cyber)security measures were needed. This ambiguous use of the term "cyber security" in several EU policies and measures is not accidental. It may suggest that there is a "competence problem" that is at the heart of the relationship between the EU and its member states. Recognition of the internal, external, and defense dimensions of cybersecurity requires careful consideration of the member states' attribution of EU competence, as well as the institutions' interpretation of EU competence.

Combating cybersecurity threats must be recognized as an issue requiring the expertise and cooperation of relevant stakeholders in different fields such as computer science, psychology, law, education, business and policy. The EU is already taking such a multi-stakeholder approach with the initial involvement of the public and private sectors, including national governments, Internet service providers, technology and security companies, business enterprises and civil society, to combat cybersecurity threats. However, such cooperation could be strengthened.

At the EU level, a number of EU institutions, agencies, and services already focus on cybersecurity issues, such as the EC's general directorates (e.g., DG CONNECT, DG Mobility and Transport, and DG Joint Research Centre). Although efforts have already been made to establish cooperation between these DGs and various units within them, these are sometimes only informal practices, and practices already governed by formal policies have not yet fully revealed their potential. Moreover, given the ever-increasing importance and dependence of societies on ICT, the number of DGs involved in cybersecurity issues can be expected to grow continuously. EU institutions and agencies working on different aspects of cybersecurity policy are already trying to develop their cooperation through both formal and informal means, such as specialized expert networks, conferences, and multi-stakeholder meetings. However, the establishment of a more comprehensive governance structure is essential to the success of any multi-stakeholder approach. To date, efforts to establish institutional cooperation have been mostly inconsistent, incomplete and not effective enough. Therefore, future policy initiatives should make a clear distinction between the roles, competencies and objectives of the areas and actors involved. This is particularly important in deciding whether to pursue more offensive or more defensive cybersecurity strategies. Such a decision could be inspired, for example, by the debates around the use of so-called lawful access, effective encryption without backdoors or zero-day exploits (based on secret vulnerabilities). Thus, the European Union should make a serious effort to address concerns about the potential weakening of the entire IT security environment, privacy and data protection, and human rights protection in general. It would therefore be desirable to involve security experts, data protection authorities, human rights advocates and the general public in defining a better balance between law enforcement needs and the rights of citizens. The recently adopted cyber security law is a step forward, as it at least clarifies the governance structure by specifying the different roles of The European Union Agency for Cybersecurity (ENISA): it consults with the EC on cyber security issues and provides a focal point for expertise, which facilitates cooperation and coordination among the parties involved.

The 2013 and 2017 EU Cyber Security Strategies call for a comprehensive approach to cyber security protection. This also applies to national approaches to cyber security. The cooperation mechanisms extending from the EU to the member states' institutions could be further improved. Although several cooperation groups exist, such as the European Data Protection Committee or the Body of European Regulators for Electronic Communications (BEREC), some of them are severely understaffed or only partially exploit their potential for effectiveness because they have difficulty sufficiently involving all relevant actors. In some cases, entities and regulators with responsibilities in different areas of a country's cybersecurity do not have effective communication practices. For example, the exchange of expertise and information between CERTs and police authorities at the national level could still be improved. However, when addressing this issue, Member States should be encouraged to establish more consistent rules and mechanisms for information exchange, in line with EU values and citizens' fundamental rights. Although most Member States developed their first cybersecurity strategies before the adoption of the NIS Directive, it may be useful to pre-define the governance framework at the national level, setting out the roles and responsibilities of both public and private sector stakeholders. When considering the changes needed to facilitate effective cybersecurity cooperation, the highest standards of rule of law and protection of fundamental rights must be respected. This is particularly crucial in the area of law enforcement and criminal procedure, where a delicate balance must be struck between the interests of states, societies and individuals. Therefore, policymakers need to develop a clear understanding of the limits to cybersecurity cooperation imposed by judicial and legality principles and strive to maintain consistency between different legislative frameworks.

**4.2.2 A late but effective awareness**

Following the 2007 crisis in Estonia, ENISA did not have the competences to act on the ground, in direct support. In general, following this attack, the European Union did not really have any tangible action to protect its members, and relies on the active and efficient action of NATO in this matter.

An embryo of a common cyber defense policy appeared in 2016 with adoption of the NIS (Network and Information Systems Security) directive. This is the first legislative framework to be agreed upon throughout the EU. This framework, transposed in 2018, establishes an audit obligation for companies, incident notifications and elaborates security measures for companies. The objective is not so much the cyber defense of the Union as a first protection of the whole territory against malicious viruses sent from abroad that can steal information or money from companies in the EU. This directive is the starting point of a reinforced collaboration between countries, and voted unanimously, it shows a beginning of awareness. But this awareness does not mean total agreement. The dissensions between the different countries, as explained above, prevented the implementation of an effective and binding policy, with a definite effect on European defense.

Less than a year after the adoption - but before the transposition - of this directive, two computer worms hit the world: Wannacry and Notpetya. These worms are typical examples of what the NIS Directive is supposed to prevent. In May and June 2017, they affected hundreds of thousands of computers around the world. Posing as ransomware, they block access to computers and offer to return that access in exchange for a ransom. These attacks have caused billions of dollars in damage and are considered the largest cyberattacks in history. They are all the more dangerous because to this day the international community has not found anyone responsible for any of the attacks. Moreover, in 2016 and 2017 with the suspicions of Russian interference in the American and French elections, the international community became aware of the urgency to act in a more effective and coordinated manner against external intrusions into a country's cyber space.

In response to these two phenomena, starting in 2017, the European Union began to act in a coordinated manner and on an ambitious scale. This was the objective of the European summit in Tallinn on September 19, 2017. On the one hand, it proposed to create a new policy, more ambitious than the NIS Directive to protect against worms such as WannaCry. On the other hand, it created a new agency, as a continuation of ENISA to assist states directly against cyber-attacks. In addition, a recommendation of the European Commission was taken to allow Europol to act in partnership with all countries to help victims of cyber-attacks to defend themselves and limit the damage. It set up secure communication networks communication networks, permanent points of information exchange between countries. A new dynamic, the awareness at the European level, therefore, sees the light of day in 2017 and has been developing since.

First, through Permanent Structured Cooperation (PESCO). This structured cooperation is provided for by the Treaty of Lisbon to deepen cooperation in the field of security and defense of Member States. It is therefore a military approach that is taken.

Among the very first proposals for cooperation, Lithuania has put forward the establishment of a common cyber force to respond to cross-border crises: the cyber rapid response teams and mutual assistance in cyber security. This assistance includes specialized units from each participating country. These units can be mobilized jointly to reinforce the defense of a particular country in case of an attack. It now includes Lithuania, Estonia, Croatia, Romania, Spain and the Netherlands and is one of the most advanced projects within PESCO.

Following the success of this project, other proposals have been set up. They have been launched by different countries and each one includes a part of the members. These include the French initiative for the development of common and secure military radio technologies (ESSOR), the Greek initiative for the development of common defense measures (for the moment, these are mainly common firewalls), and the joint project between Spain and Portugal for the development of a cyber and innovation school to train experts in this field (EU CAIH).

Finally, still in a logic of cooperation, ENISA is setting up since 2019 the Blue Olex event to strengthen the exchange of knowledge in the EU. Organized in France in 2019 and in the Netherlands in 2020, this event aims to prepare a political discussion on cyber defense by bringing together senior officials from the 27. To this end, this year's event has enabled the establishment of CYCLONE with the idea of establishing an intermediate level between political and technical in the management of cyber crises.

The objective is to allow a global and efficient analysis in response to cyber crises between countries.

This multiplication of initiatives shows Europe's interest in cooperating in this field to preserve its sovereignty in the face of external attacks.

**4.2.3 Towards a European cyber sovereignty?**

Eventually, it is possible to envisage an autonomous EU in cyber defense. But there are many obstacles to such autonomy.

A first obstacle to this autonomy lies in the reluctance of countries to share information and sovereignty prerogatives, particularly concerning defense. Without going back over the history of the EDC and the various failed European defense initiatives, the European Union is reluctant to share its defense, including in the cyber domain.

Some more advanced countries do not want to share information that is too sensitive for fear that it will be transferred to less secure countries and eventually stolen in an attack on this EU member country but with lower security standards.

A second obstacle concerns the already strong cooperation with NATO. Some EU countries with an underdeveloped cyber defense wish to develop their national defense first, considering that the current NATO protection is sufficient. Even the most advanced countries are now relying on the organization, as we have seen with Germany, which will join the Netherlands in making its forces available to NATO and not to the European Union. NATO's cyber power and its rapid awareness, which has allowed for in-depth work for over a decade, make it a considerable force. For many, there is not much interest in leaving this protection to create another autonomous, but less strong one.

These few obstacles should not, however, make us forget the significant progress made by the European Union in cooperation. In this field, it is important to have driving countries that launch increasingly ambitious dynamics in the cyber cooperation of the Union. We can cite Poland, which remains under the NATO umbrella, but is strengthening its national forces and cooperating in many areas.Its national forces and cooperates in many areas with the EU and France. This The latter has not contributed its forces to NATO, preferring to launch many European defence projects, as Emmanuel Macron stated in his 2018 Paris appeal, calling for an autonomous European cyber power. These two driving countries are joined by the Baltic countries, with Estonia being a pioneer in this field and Lithuania wishing to develop its capabilities in full cooperation with the European Union.

Finally, the European Union has many fundamental dilemmas and disagreements about its common management of cyber defense. Between countries that consider cyber to be a civilian matter, those that rely on the NATO umbrella, and those that are afraid to share information with countries that are not sufficiently advanced in terms of security, the EU has many challenges to overcome before it can achieve an autonomous and effective defense against the giants of cyber-attacks such as China or the United States. However, the advances are present, they are multiple and sometimes confused but in a certain direction of strengthening the European cyber power.

**5. Theoretical Framework**

**5.1 Critical Theory of International Relations and Global Cybersecurity**

The purpose of this chapter is rather straightforward. It is very unusual, almost unique insofar as critical theory is still marginal within the field of International Relations, however, it already challenged traditional theories of International Relations. Thus, this needs to be explained. In this chapter, we will recount, summarize, and emphasize on basic assumptions of Critical Theory of International Relations, analyze its background, and attempt to apply some of the basic ideas of critical theory to global cybersecurity. We do this in basically three steps. We begin with the discussion of critical theory’s background and the necessity for a structural rethinking of security in International Relations. We then overview the basic ideas of critical theory of international relations and analyze the works of the biggest representatives of this theory. After that, we link security critical theory to global cybersecurity and appraise the utility of critical theory in International cyber politics. While traditional theoretical models of International Relations, such as Realism, can be rather helpful when analyzing the international relations dimension of NATO-EU cooperation, they frequently lack a critical engagement. This Master Dissertation implies Critical Security Studies (CSS) to analyze cyberspace and the impact it has on the relations between the European Union and NATO.

Even though we make a comparison of critical theory with traditional theories, we do not claim to present a detailed comparison of critical theory to traditional International Relations theories.

To achieve the aforementioned goals, we use qualitative methods of research in International Relations. We use comparative research. A structurationist approach is also used in this thesis.

**5.2 Background of the Critical theory of International Relations**

The need for a structural rethinking of security in International Relations was demonstrated by political, social, and economic circumstances which occurred as soon as the Soviet Union collapsed, and the Cold War was brought to its end. Traditional schools of thought of International Relations were state-centristic and mostly neglected transnational, supranational, and subnational factors and their role in International Relations. For example, major upheavals in International Relations such as the demise of the USSR and September 11 Terrorist attacks represent a crucial milestone and a turning point in the development of International Relations theory inasmuch as they demonstrated to the scholars and researches that state-centristic theories of IR were no longer able to take into consideration new emerging issues and thus traditional theories were no longer of practical validity. No traditional theory was able to go beyond the framework of analyzing state-system interaction and concentrate on the events within the state. This is one of the major reasons why traditional theories were unable to foresee the demise of the Soviet Union. The rise of nationalism in Eastern Europe, the collapse of the confidence in Marxism-Leninism and in communism in general, the rise of influence over the Soviet leaders by alternative security thinking, and other big factors were not taken into account by traditional theories because it went outside of the traditional paradigm. In this regard, the representatives of the Welsh School of International Relations, Richard Wyn Jones and Ken Booth proposed a new approach to security policy, which was influenced by the Frankfurt school and Gramscian's thinking. Not only had they proposed a new analytical perspective that could meet the need for decentralizing the state as a reference object of research, critical theory has proven to be a valuable tool in the service of security research to meet the growing need for a broader research framework which helped overcome the theoretical axiom that in the second half of the 20th century turned security thinking into a simple dichotomous competition.

Founded by the Frankfurt School, a group of German intellectuals associated with the Institute of Social Research at the University of Frankfurt in the 1920s-1960s (including Max Horkheimer, Theodor W. Adorno, Herbert Marcuse, and Walter Benjamin), critical theory was applied to international relations by Robert Cox in the early 1980s, and that is why R. Cox may be regarded as the father of critical theory of International Relations. But that notwithstanding some respected researches in the field of International Relations propose to divide the scholars of this theory into two large generations: ‘the first generation’ which includes German social theorists and philosophers such as Herbert Marcuse, Max Horkheimer, and Theodor W. Adorno, and ‘the second generation’ which include such philosophical schools of thought in the field of International Relations as neo-Marxism, Social constructivism, Critical Theory, feminism, neo-Gramscianism, and the others. Sensu stricto, both generations of these schools of thought of International Relations try to change the entirely descriptive type of social science to an exploratory one. Critical theory’s analytical purpose and theoretical assumptions make it different from traditional IR theories. Its ideas originate from Freudian, Marxist as well as Kantian culture and primarily focuses on the idea of human emancipation from the modern state and economic system, social practices, and repressive institutions, by supporting ideas that meet universalist principles of justice.

As we have already stated above, even though critical theory embraces a big number of different assumptions and approaches, the concept of ‘emancipation’ of Kantian and Marxist traditions are at the base of critical theory’s lineage. Kant and Marx, with their universal aspirations, become central figures for critical theory in modern times insofar as they both proposed revolutionary ideas about new ways to reshape the world. Immanuel Kant contributed to the development of the cosmopolitan and supranational political communities by his claims of the increasing interconnectedness of the world. It has to be noted that Kant initiated an approach to IR theory that went beyond the traditional framework of thinking of world politics as simply interstate politics. He anticipated modern theories of International Relations which are taking into account international terrorism, world economy, environmental issues, arms control, and social movements as central objectives of concern in the determination of domestic policy.

On the other hand, Karl Marx, historian, economist and socialist who wrote the works that formed the basis of communism. Marx’s works largely contributed to the development of the critical theory of International Relations. His critique of a capitalist economic system says that we, as participants of capitalist economic relations, understand the economy in terms of free exchange, private property rights and the rule of demand and supply, and in doing so, we start thinking about the capitalist economic system as justified and how it should be whereas this way of thinking is nothing more than an ideology. An ideology that obscures from its participants destructive labor exploitation and the creation of an unfair economic system. Marx’s critical theory of the economic system was later on developed by the representatives of the Frankfurt School of IR and especially by Adorno, Marcuse, Habermas, and Horkheimer.

Having analyzed the very base of critical theory’s lineage, we noticed that Marx and Kant focused on different research areas and postulation, but that notwithstanding there is a common defining feature of critical theory which is the need for systematic change for human emancipation and global freedom. The aforementioned need for systematic change for human emancipation and global freedom does not represent the majority of critical theory’s assumptions nor it helps to understand the contemporary sense of critical theory, and that is why recent sources of critical theory are to be further analyzed: Antonio Gramsci and his influence over Robert Cox, Jürgen Habermas, Andrew Linklater.

Antonio Gramsci is one of the most influential thinkers of the 20th century. Gramsci’s theory of hegemony proposed a new complex nature of the state, by introducing the “relationship between the dominant and dominated classes”. Hegemony, according to Antonio Gramsci, is the use of moral, intellectual, economic, political, and other forms of power by the dominant class to achieve its goals and to do so, this dominant class is to establish its worldview as universally accepted by the people. In this regard, the state is not a unipolar actor in the international arena, as it is comprehended by the realists. Moreover, Gramscianism, instead of accepting the realistic understanding of the anarchical system approach, believes that states become bound together on the international arena insofar as they accept bourgeoisie morals as well as values[[32]](#footnote-32).

The second distinction to be made between the realist approach and Gramsci’s theory is their understanding of Security dilemma. According to John H. Herz, states, concerned about their security from being attacked or dominated, strive to attain security[[33]](#footnote-33). Thus, states are trying to acquire more power to secure themselves. But these actions, on the contrary, rendering them more insecure inasmuch as the others start preparing for the worst and accumulate more power. Some scholars of international relations have claimed that security dilemma is the most crucial source of conflict. We can then, following John Herz’s work, explain the vicious circle of arm race between the Soviet Union and the United States of America which was on presumably since 1945 up to the end of the demise of the USSR in 1991, since both superpowers sought primarily to secure themselves by the accumulation of nuclear weapons. Gramscian theory of hegemony sees differently Security dilemma. As it was mentioned above, Gramsci’s theory of hegemony understanding lies within class-relation and relations between dominant and dominated. A coercive force is considered to be the primary instrument of the dominant-class inasmuch as it has the ability to keep dominated groups disorganized and convinced that moral principles that were established are universally accepted. In this regard, the main reason for the collapse of the Soviet Union may be found in the dissemination within the soviet civil society of bourgeoisie ideology, morals, and values.

The next prominent scholar who largely contributed to the development of critical theory is Robert Cox that was influenced by Antonio Gramsci. Robert Cox, according to some scholars, may be regarded as the father of critical theory[[34]](#footnote-34). According to Robert Cox, critical theory differs dramatically from traditional theories insofar as it is anti-status-quoist since it «allows for a normative choice in favor of a social and political order different from the prevailing order”[[35]](#footnote-35). His famous formula – “a theory is always for someone and for some purpose” recalls that all theories have a perspective, which itself "derives from a position in time and space, especially social and political"[[36]](#footnote-36).

Robert Cox presents critical theory as opposed to problem-solving theory, corresponding to what Horkheimer called "traditional theory", which "takes the world as it finds it". Dominant theories such as the neorealism of Waltz or the Liberal neo-institutionalism of Keohane are, for Cox, typical cases of problem-solving theories. Critical theory, on the contrary, "wonders how this order was born. [It] does not take institutions and social and power relations for granted, but challenges them." This theory is "critical" in that it challenges the dominant order, questions "where it comes from" and it is also normative in that it is based on "a normative choice in favor of a social and political order different from the dominant order, but it limits the range of choices to the alternative orders that constitute achievable transformations of the existing world". It is thus, unlike problem-solving theory, historical not just because it analyzes the past, but it is concerned with a continuing process of historical change since social, economic, or political orders are not fixed in space and time. Because critical theory of International Relations deals with a continuing process of historical change, it is more adjusted to grips with the changing reality to better comprehend the world it has to deal with, understand, and explain rather than problem-solving theory.

The other major distinction to be made here between critical theory and problem-solving theory is the understanding of the possibilities of state’ changes. Problem-solving theory does not call into question states in terms of the possibilities of fundamental changes since they occur within a limited framework, whereas critical theory goes beyond it and it searches for its origins and the developmental possibilities of fundamental change.

Cox took the Gramsci's theory of hegemony and applied it to the World order, rather than to International relations inasmuch as the latter is a very state-centristic term. Rather than mere domination, hegemony is a subtle balance between coercion and consent: dominated states do not suffer their subordination as a constraint, on the contrary, it seems to them natural, therefore acceptable, and they even participate in it because they feel that it is in their interest. In this sense, hegemony is «the recruitment of other people in the exercise of your power by convincing them, cajoling them, and forcing them to believe that they want what you want." It is not just inter-state but is expressed "in universal norms, institutions, and mechanisms which lay down general rules of behavior for states and for those forces of civil society that act across national boundaries – rules which support the dominant mode of production"[[37]](#footnote-37). For example, Cox explains, the periods 1845-1875 and 1945-1965 were hegemonic, around the United Kingdom and the United States respectively.

As was aforementioned, Robert Cox analyzed world order, rather than International Relations. In doing so, he challenges the state-centristic realism’s study of interstate relations which does not take into consideration social forces. This is, according to Cox, a misleading way of analyzing International Relations. Instead of focusing on interstate relations, Robert Cox proposes to focus on the state form and how it can be changed under the influence of civil society and other macro forces. Productive forces, ideas, and institutions are crucial in the analysis of ‘world order’ or ‘global politics’ or ‘global political economy’[[38]](#footnote-38).

Having analyzed literature on critical theory of International Relations, we can distinguish major assumptions of critical theory of IR:

1. States are not the only actors of World Politics According to Robert Cox, social constructs are the principal actors of World Politics;
2. The major purpose of theory is to provide understanding and practical knowledge for further emancipation. Theory should be able to be altered to grips with the changing reality for better understanding of the world it deals with;
3. States and the system in which they operate are not unchangeable since they are not fixed in time and space;
4. The appropriate methodology is that which focus is on relations between social structures and states.

**5.3 Critical Theory’s vision of Cybersecurity**

The Aberystwyth School (sometimes The Welsh School) of security studies or Critical Security Studies (CSS) is based on the works of Richard Wyn Jones and Ken Booth. It has to be noted that both of them were influenced by Gramsci’s theory and Frankfurt School. As all of them have their roots in Marxism, they are all oriented towards the elaboration of a theory that would be aimed at the systemic transformation for human emancipation and the creation of a free global community. Emancipation, according to critical theory, implies liberty but of an egalitarian character. It requires the integration of reciprocal rights[[39]](#footnote-39).

Critical security studies are opposed to the traditional security studies which have dominated the subject for half a century. Traditional security thinking is rather status quo oriented and it is of state-centristic nature. For Richard Wyn Jones and Ken Booth traditional approaches, such as the realistic approach, can never lead to true security as they focus on ‘power’ and ‘order’ and emphasize the need of strong states and military power. Traditional theories focus more on military force, not on security itself. Ken Booth considers realism to be an ‘unrealistic’ ideology that is too narrow, and its assumptions go against human interests. Moreover, this realistic ‘ideology’, pretending to be a theory of knowledge, largely lacks methodology[[40]](#footnote-40).

Unlike traditional theories which consider states as the central security actor and the principal security provider, CSS claims that states are the ones that render humankind insecure since way more people were killed by their own governments rather than by foreign armies or foreign governments. Security, according to Booth, can be achieved only when it is understood as emancipation. ‘Emancipation’ and ‘security’ are of the same meaning in CSS. In order to achieve it, we are to conceptualize the term ‘security’ and understand why people and groups feel insecure and suffer from it. Apparently, Ken Booth claims, biological motivations for security are universal, that is the necessity to have shelter, food, to feel secure physically, etc. Thus, the core elements of ‘security’ are universal biological motivations. In order to achieve global security, people should create security communities, made up of free communities and cosmopolitan states. Global governance which is composed of emancipated governments will be able to transcend the Security dilemma, which is the most crucial source of conflict. Emancipation, not power or order, produces true security, inasmuch as it enables people to go beyond barriers between ‘us’ and ‘them’. In perusing emancipation, real security can be attained[[41]](#footnote-41).

Therefore, having analyzed the Critical Security Studies, we may conclude that there are three core ideas that underpin CSS. The first core idea is that security is a derivative concept; that is, security reflects deeper assumptions about the nature of politics and the role of conflict in political life. It connotes that human’s understanding of security comes from the way one’s thinks about the world and the politics. The ideas intentionally disseminated in the human’s society by specific actors will always influence the way we think, perceive, and understand threats. It ultimately influences the way we define security itself.

The second idea of CSS consists of the argument that the security agenda must be broadened. Military force, according to Barry Buzan, should not be considered as the only potential threat. Five different sectors such as the environment, the economic, the political, the military and the societal should also be analyzed. “Military security concerns the two-level interplay of the armed offensive and defensive capabilities of states, and states' perceptions of each other's intentions. Political security concerns the organizational stability of states, systems of government, and the ideologies that give them legitimacy. Economic security concerns access to the resources, finance and markets necessary to sustain acceptable levels of welfare and state power. Societal security concerns the ability of societies to reproduce their traditional patterns of language, culture, association, and religious and national identity and custom within acceptable conditions for evolution. Environmental security concerns the maintenance of the local and the planetary biosphere as the essential support system on which all other human enterprises depend. These five sectors do not operate in isolation from each other. Each defines a focal point within the security problematique, and a way of ordering priorities, but all are woven together in a strong web of linkage”[[42]](#footnote-42).

**6. Analysis**

**6.1 EU-NATO Cooperation**

The analysis of the relationship between the European Union and the North Atlantic Treaty Organization requires a chronological approach to understand the nature and extent of the relationship developed between the two institutions. The historical context in which they were created largely determines the purpose of this cooperation. This cooperation has developed not only in time but also and above all in space with the various enlargements that have occurred since their respective creation. Thus, in the aftermath of the Second World War, Europe was deeply divided by the ideological and political opposition of the Cold War. Faced with the urgency of economic reconstruction, the countries of Western Europe, following the commitments they had made during the war, proceeded to reduce their military strength, while the Soviet Union decided to preserve the full power of its armed forces. Stunned and worried by this Soviet decision, the European allies and their North American partners began negotiations which later led to the creation of organizations for military cooperation. A succession of unprecedented political events between 1947 and 1949 accelerated matters. These included direct and indirect threats to the sovereignty of several European countries, including Norway, Greece, and Turkey, the June 1948 military coup in Czechoslovakia, and the blockade of Berlin in April of the same year. Faced with this series of political events, Belgium, France, Luxembourg, the Netherlands, and the United Kingdom signed on 17 March 1948 a treaty on economic, social, and cultural cooperation and, above all, on collective self-defense, which established a system of automatic mutual assistance in the event of armed aggression in Europe. Denmark, Iceland, Italy, Norway, and Portugal are invited by the signatory powers to join the "Brussels Treaty". Shortly after the signing of the Brussels Treaty, Canadians, Americans, and British begin talks in Washington on a collective defense treaty for the North Atlantic area. The negotiations between the three parties led to the signing of the "Washington Treaty" on April 4, 1949, which established a common security system based on a partnership between the twelve signatory states. The treaty reaffirms the natural right of independent states to individual or collective self-defense per Article 51 of the UN Charter. Member countries agree to consider an armed attack on one of them, in Europe or North America, as an attack on all of them. Only fourteen months after the signing of the Washington Treaty, the West feared the expansionist aims of the Soviet Union following the outbreak of the Korean War. The signatories of the Washington Treaty decided to set up a permanent military structure to better implement their common defense commitments. This led to the creation of the North Atlantic Treaty Organisation or NATO with an administrative General Secretariat. German reunification in 1990, the disappearance of the Warsaw Pact, and the collapse of the Soviet Union in 1991 raised questions about the desirability of maintaining a military alliance. Opinions are divided on the issue. First of all, in Europe, a strategic American presence is desired by the Germans, who see it as a means of reassuring their neighbors about the consequences of German reunification for their security. The less powerful European states see the American presence as a guarantee against the domination of one or more major European partners. On the American side, they advocate a revision of the missions assigned to NATO by giving it a broader geographical scope and assigning it a general European security function beyond territorial defense. This is precisely the program implemented by NATO since 1990.

This is precisely the program that NATO has been implementing since 1990. This raises the question of continued North American involvement in European security and the institutional preservation of NATO. Is a European defense policy conceivable in the framework of cooperation with NATO? I will attempt to answer this question by analyzing the political and military framework for cooperation between the European Union and NATO, and by clarifying the role of the European Defence Agency.

We need to start off with the cooperation frameworks between the European Union and NATO: political and military cooperation.

The European Union and NATO have developed a close partnership over the years, resulting in political and military cooperation. The issue of relations between the two institutions has been dominated by fears of overlap and divergence between them. The US Secretary of State then used the "3Ds" to better illustrate this concern that characterizes the relationship between the European Union and NATO, namely: the risk of decoupling of actions carried out by NATO and the European Union, the risk of duplication of military capabilities and discrimination against non-EU NATO members such as Turkey, Albania and Croatia.

The Political Framework of NATO-EU cooperation: Four (4) major political events have played an important role in defining and strengthening a policy of cooperation between the two institutions, namely: the Prague Summit, the European Security and Defiance Policy, the so-called "Berlin Plus" arrangements and the Brussels European Council of 2003. We will analyze the European Security and Defiance Policy to better understand the political framework of cooperation.

A joint EU-NATO declaration was adopted in 2002. This declaration paves the way for closer political and military cooperation between the two partners. It sets out the political principles of this cooperation and guarantees the European Union access to NATO logistical and planning assets for its own military operations. The European Security and Defense Policy aims to add to the range of EU instruments already available for crisis management and conflict prevention, the capacity to conduct EU-led crisis management operations including military operations without NATO participation. ESDP supports the European Union's foreign and security policy. While preserving their respective autonomy, the European Union and NATO are developing a partnership based on consultation, dialogue, cooperation and transparency in crisis management and preservation. The ESDP provides for the strengthening of the strategic partnership between NATO and the European Union, in a spirit of complementarity and with respect for the decision-making autonomy of the Union and the Alliance. The text also provides for EU support to the UN and the African Union in peacekeeping. France made the European Security and Defence Policy a priority of its Presidency in the second quarter of 2008, submitting to its European partners a comprehensive programme based on a coherent approach, namely: a shared analysis of threats and risks through the updating of the European Security Strategy, a collective commitment through an increase in European defence capabilities, recognition of the strategic and economic need to restructure the defence industrial and technological base, the strengthening of partnerships with NATO and the UN, and finally, the increased responsibility of the European Union in the face of global threats3. In the framework of its security and defence policy, the European Union is demonstrating its responsibilities in the fight against terrorism, the proliferation of weapons of mass destruction, maritime piracy, drug trafficking and organised crime. The European Union and NATO thus contribute to the definition of a global approach to crisis management through the implementation of a common security and defence policy in the framework of a strategic and privileged partnership.

As mention above the European Union and NATO have a relationship in the military field. This translates into operations conducted by one or the other organisation with logistical and material support from the other. Thus, within the framework of the European Security and Defence Policy, the Union has launched for the first time, a naval air operation off the coast of Somalia. Other operations will see the two institutions intervene side by side. The analysis of KFOR in the former Yugoslavia perfectly demonstrates all levels of military cooperation between NATO and the EU.

Following numerous violations of human rights, international humanitarian law and international security, NATO decided to intervene in the former Yugoslavia in order to guarantee peace and security throughout the European continent. The aim was to bring peace between Albanians and Serbs. As in other missions, NATO and the European Union are working as a military partner to bring peace to the former Yugoslavia through the KFOR (Kosovo Force) mission. This force has been led by NATO since 1999, while the European Union has been providing civilian assets to the UN Mission in Kosovo for several years. It has also taken over the component of the UN mission. Through this mission entitled "Rule of Law", the European Union contributes to the promotion of democracy and the construction of a rule of law based on the respect of international legal values. EULEX-KOSOVO is the largest civilian mission ever launched under the European Security and Defence Policy (ESDP), with the aim of supporting the Kosovar authorities, particularly in the police, justice and customs sectors, in a rapid return to the rule of law. On the ground, close cooperation between the two institutions has developed, with NATO and EU experts often working in the same team. As in other missions, the Kosovo mission was a good example of EU-NATO cooperation in the military field. The legitimacy of the operation was challenged by the UN Security Council, which alone has responsibility for peacekeeping in the world under Chapter VII of the UN Charter. NATO justified itself by invoking Resolutions 1160 and 1199 of 1998[[43]](#footnote-43).

Charles Goerens, Luxembourg Minister of Defence from 1999 to 2004 and former member of the Western European Union (WEU) Assembly, which he chaired from 1987 to 1990, explained in an interview, he explained that "in his view, European security cannot be conceived without the North Atlantic Treaty Organisation (NATO)[[44]](#footnote-44). Despite the political will of the Heads of State and Government to free Europe from American tutelage in security and defence matters, it is clear that the European Union remains heavily dependent on NATO in defence and security matters. As a result, European security policy and European defence identity are in contrast in the cooperation between the two institutions. However, over the years, Defence Europe has continued to develop to the point where Europe can take charge of its own defence policy, notably through the "Berlin Plus" agreements which allow the European Union to use NATO assets and capabilities for operations without North American participation. It is also important to mention France's unique position within NATO, because this French position is proof of the existence of differences of opinion and conflicts of interest that can mark the relationship between NATO member countries. While participating in its activities, France decided to withdraw unilaterally from the Atlantic Organisation in 1966, for political (détente), strategic (refusal to join the deterrent force) and military reasons (desire to control the involvement of its forces in NATO's military operations). However, this decision did not prevent the development of military cooperation between France and the integrated structure of NATO. It participates in all of NATO`s political consultation bodies but does not participate in the Defense Planning Committee[[45]](#footnote-45). Finally, the military intervention of the coalition in Libya, which NATO commands, reflects the political will of European and North American actors to promote democracy and respect for human rights through joint military operations.

**6.2 EU–NATO Cybersecurity and Defense Cooperation**

The European Peninsula has a very particular institutional landscape in terms of collective security and defense (Please see Appendix A). It includes the North Atlantic Treaty Organization (NATO), an organization that is specialized in collective security and defense since its creation in 1949, but also the European Union (EU), which, on the other hand, has seen its competences in this area gradually built up, particularly since the Nice (2001) and Lisbon (2011) treaties.

While war is still a "state affair", there is a "rooting of alliances" and, more broadly, of collective security structures. Hume, from the mid-18th century, argues that each state acts to achieve a direct objective (individual security) but also to fulfil an indirect objective, the international balance of power[[46]](#footnote-46). Therefore, alliances can be useful in building a balance of power, or at least in balancing threats. Indeed, the sense of an alliance for a state is to become part of, and contribute to, a collective security system that gives it greater power.

There is no doubt that these very same theories and strategies could be applied in cyberspace. Since cyber threats are reterritorialized, nebulous, opaque, relatively instantaneous and difficult to attribute, the integration of an inter-state cooperation or alliance can be particularly relevant to consolidate power relations.

It is quite clear from this extract that the articulation of the competences of the EU and its Member States with NATO, the 'transatlantic security architecture', is also a key issue. NATO, a transatlantic military alliance that today includes 21 EU Member States, is a key player in European security (Please see Appendix B). The latter is important because, in the event of a proven aggression, it involves the United States and Canada in the defense of Europe in its broadest sense, just as it involves, reciprocally, the commitment of its European members in the defense of the two North American countries.

Collective cyber defense appears relevant in view of the potential for cyber conflict and the resulting cyber threats. It seems particularly appropriate on a regional scale. It could be based on pre-existing and solid networks of trust, which are very important in cyberspace, where the concept of a state's strategic neighborhood is called into question. The value of a collective cyber defense for the EU no longer needs to be demonstrated, but the question now is to define the precise modalities: what collective cyber defense for Europe?

Both the EU and NATO are institutionalizing cyber issues. Both organizations have adapted their structures and administrations to these emerging issues. Each of these two entities has established a policy based both on decisions and regulations and on specialized agencies[[47]](#footnote-47). NATO as well as the European Union seek to achieve the same objective, which is twofold: on the one hand, to strengthen the security of the networks and information systems of their institutions; on the other hand, to improve the security or strengthen the capacities of the Member States.

However, as they have not developed their policies jointly, "there is some confusion about the roles of NATO and the EU in the field of cyberspace, particularly in the military sphere. It is very difficult to see elements of subsidiarity or complementarity in each other's work emerging. Yet there is no doubt that the security of the European Union and NATO are indeed very interconnected.

In needs to be stated that cybersecurity is a new opportunity for NATO and the European Union to cooperate and strengthen their cooperation. The cooperation among NATO and EU in the aforementioned field is currently critical inasmuch as this field has no international regulatory structures and the cyberattacks are getting more complex, more disruptive, and in many cases more political.

In 2016 the Technical Agreement on Cybersafe was signed between the NATO Computer Response Center (NCIRC) and the EU Computer Emergency Response Team (CERT). According to this agreement, the cooperation between the European Union and NATO has to get strengthened through the exchange of information, joint training, research and exercises. The Technical Agreement on Cybersafe indeed creates legal basis to facilitate information-sharing to improve cyber incident prevention, detection and response together at the European Union and NATO.

We need to highlight that the most prominent steps towards cyber cooperation were made with the help of two signed joint statements, one of which was adopted in 2016 and the other in 2018. In the joint declaration of 2016 adopted by the President of the Council of Europe, the President of the European Commission and the Secretary General of NATO, the EU and NATO called the expansion of cooperation "in the field of cybersecurity and defense including in the context of our missions and operations, exercises and training as “urgent needs” and cooperation in this area as a strategic priority (NATO and the European Union, 2016). Technological innovation by strengthening cooperation between the EU, NATO and the excellent NATO Joint Security Center for the Study of cybersecurity innovations (NATO, 2016). Wendel Rupp argues that if the EU follows the decisions of NATO, this can continue, that is, it must continue to develop its capabilities to complement the capabilities of the Alliance or risk falling behind. In 2017, a common set of new implantation proposals was added to the Joint Declaration to promote the exchange of best practices between cyberbullying and crisis management and response officers in addition to operational aspects of cybersecurity, including threat analysis and malicious information, with the aim of improving joint understanding of the field and finding potential synergies. The criticality of the EU-NATO cooperation in cyberspace has been reaffirmed by the 2018 NATO & European Union Joint Declaration.

**6.2.1 Comparative analysis of NATO and EU’s approaches to cybersecurity**

A comparison analysis of the approaches, competences, capabilities as well as means of action available to these two international entities is therefore necessary to clarify and define prosperities for the possible articulation of the two systems.

We have performed content analyses to determine the presence of words such as ‘cyber’, ‘cybersecurity’, ‘cyberthreat’, ‘cyber incident’ as well as ‘cyberattack’ in official document of both international organizations to determine the EU and NATO’s change of cyber perception and identified the reasons behind this dramatic change. Data mining has been also used in this Chapter to transform fragmented text into a structured format to identify meaningful patterns and new insights which was done using QDA Miner Lite.

First, we are to analyze the North Atlantic Treaty Organization’s approach and how it defines the “cyber”.

NATO's defense competences were defined by the Washington Treaty (or North Atlantic Treaty, the Washington Treaty), the founding treaty signed on 14 April 1949. While NATO remains an institution of collective security, as expressed in its first three articles, the Atlantic Alliance more specifically and above all provides for collective defense in the event of armed aggression, as stated in its Article 5, a true mutual assistance clause. The States Parties undertake above all to take all necessary measures to prevent and combat aggression[[48]](#footnote-48).

The States Parties undertake above all to avoid conflicts and to settle international disputes by existing peaceful means (Articles 1 and 2 of the Washington Treaty). They develop, individually and collectively, the necessary capabilities to deter threats and resist aggression (Article 3). Finally, the mutual assistance clause (Article 5) offers two operative provisions defining NATO's competences: On the one hand, the idea that "an armed attack against one or more of [the parties] occurring in Europe or North America will be considered as an attack against all parties"; on the other hand, that each state "will assist the party or parties so attacked by taking forthwith, individually and in agreement with the other parties, such action as it deems necessary, including the use of armed force" (Article 5, the Washington Treaty).

There is no doubt that NATO's handling of the cyber threat has emerged and evolved as a result of major cyber incidents that have impacted the Alliance and its members. It was following the cyber-attacks during the 1999 Kosovo war, in which the Alliance was engaged, that NATO decided to address this threat. An internal audit was first conducted by SACEUR (Supreme Allied Commander Europe). Then the heads of state made commitments at the Prague summit in November 2002 to "strengthen [their] capabilities to defend against cyber-attacks". However, at that stage, the subject was only dealt with from a purely technical angle. It was not until the 2007 cyber-attack against Estonia (a NATO member) that the cyber threat became part of the political agenda. This attack raised the question of the inviolability of Article 5 of the Washington Treaty in the event of cyber-attacks, and, if so, the response to be adopted (computer counterattack or conventional response). It was not until the following year that the first NATO Cyber Defense Policy was adopted by the North Atlantic Council, a sign that cyber had become a major concern for the organization and its member states. Such a significant emerging threat, that since the Warsaw Summit in July 2016, cyberspace has been recognized as "an area of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea" (§ 70 of the Summit Communiqué). NATO explicitly states that the mutual assistance clause can be invoked in the event of a cyber-attack against one of the states. Cyber defense is therefore part of the NATO defense strategy.

With that being said, we can articulate that cyber defense takes a prominent place in NATO’s official document and is thus an integral part of NATO's core competence in collective defense and Communiqué) and NATO’s News Conferences, Speeches and Keynote Speeches in Chapter 4, rigorously proves the Hypothesis 1 and 2.

Content analyses that we performed to determine the presence of words such as ‘cyber’, ‘cybersecurity’, ‘cyberthreat’, ‘cyber incident’ as well as ‘cyberattack’, themes, or concepts within some given qualitative data permitted to determine NATO’s perception of a threat and actor in the cyber field. NATO sees individual states and state-sponsored groups as one of the most active actors. Cyberattacks on Ukraine, Estonia, Georgia largely contributed to the development of this topic at NATO and its individual states perception as primary actors. In addition, it should be said that this approach has been getting more central role in NATO’s actor’s perception in cyberspace during 2002 up to 2021 insofar as its Member States have been targeted by the state-sponsored groups (the USA, France, Germany as well as Australia)[[49]](#footnote-49).

We have justified the aforementioned statement using a coding process of key words and associations of official NATO documents and researchers’ papers on this topic. The search was conducted using the following search terms ‘APT’, ‘Adware’, Botnets’, ‘Malware’, ‘DDoS’, ‘Espionage’, ‘Cybercrime’, ‘Phishing’, ‘Zero-days’, ‘Man-in-the Middle’, Ransomware’, ‘Disinformation’, ‘False flag’, ‘Terrorism’, ‘Spyware’ as well as ‘Election meddling’. We used QDA Miner Lite, Free Qualitative Data Analysis Software, which does not require the knowledge of R 3.1.1 or Python programming languages to run the analysis. The data and the findings are visualized in Appendix C.

Unlike NATO, the EU's cyber defense capabilities have not evolved as a result of cyber incidents directed against it, but rather in anticipation of this emerging threat. The EU has thus gradually developed a posture of resilience and coordinated response.

First of all, in terms of defense generally, the Common Security and Defense Policy (CSDP), defined in Article 42 of the Treaty on European Union (TEU), allows the EU to have civilian and military means at its disposal in the resolution of crises and conflicts between countries. An integral part of the Common Foreign and Security Policy (CFSP), CSDP is today more akin to a form of collective defense. It can only constitute a genuine "common defense" once a common policy has been unanimously adopted by the European Council (Article 42(2) TEU). Indeed, the CSDP is "based on the capabilities provided by the Member States" (Article 42(1) TEU) and still relies essentially on national budgets to finance expenditure on operations (despite the Athena funding mechanism). Finally, decision-making remains intergovernmental, with the unanimity rule prevailing for Council decisions (Article 42 § 4 TEU).

A mutual defense clause nevertheless offers the possibility of collective defense since the Treaty of Lisbon (Article 47 § 7 TEU). Similar to the second operative provision of Article 5 of the Washington Treaty, it states that "in the event of a Member State being the object of armed aggression on its territory, the other Member States [of the European Union] shall render aid and assistance by all the means in their power".

Although the European Union has gradually become aware of the emergence of the cyber risk since the 1990s, it was not until February 2013 that it declared itself competent in cyber defense. It is through the European Union's Cybersecurity Strategy: Open, Safe and Secure Cyberspace, published jointly by the Commission and the High Representative for Foreign Affairs and Security Policy, that the Union has self-assigned its competence in the field of cyber defense in the light of the CSDP. Precisely, it is priority three (out of five) that gives it this attribution and defines its contours:

«2.3 Developing a cyber defense policy and capabilities as part of the Common Security and Defense Policy (CSDP).

Cyber security efforts in the EU also have a cyber defense dimension. To increase the resilience of communication and information systems safeguarding Member States' national defense and security interests, the development of cyber defense capabilities must focus on detection, response and recovery from sophisticated cyber threats.

As these threats are multifaceted, synergies between civilian and military approaches to the protection of critical cyber infrastructure need to be developed. These efforts need to be supported by R&D and close cooperation between public authorities, the private sector and academia in the EU"[[50]](#footnote-50).

This Cyber Strategy, revised in 2017, is then mainly aimed at resilience as a whole, and not necessarily the removal of the threat through operational action against a potential aggressor. Led by the EEAS, it was developed in close consultation with DG CNECT (Communication Networks, Content and Technology), but also DG GROW (Internal Market, Industry, Entrepreneurship and SMEs) and DG HOME (Migration and Home Affairs). This strategy is complemented by the Network and Information System Security (NIS) Directive of 6 July 2016, which determines the standards to which businesses must subscribe to strengthen civil cyber security within the EU. The strategy as a whole therefore focuses more on the internal security of the Union.

The overall strategy thus focuses more on the internal security of the Union, a concern that is less about internal security than about economic imperatives[[51]](#footnote-51). Cyber defense at the EU level is therefore still in its infancy, despite the Commission's clear recognition of the importance of cyber defense cooperation in the Reflection Paper on the Future of European Defense (2017).

Moreover, this strategy does not explicitly refer to the mutual assistance clause (47(7) TEU) but only to the solidarity clause (Article 222 TFEU), which can be invoked on the grounds of "a particularly serious cyber incident or attack"[[52]](#footnote-52). It is interesting to note, however, that the Commission's strategy does not explicitly refer to the solidarity clause. On the other hand, it is interesting to note that in its 2018 "cyber defense resolution", the European Parliament affirmed the applicability of both clauses. It thus outlines a collective cyber defense strategy for the EU.

Having compared the legal ground for the EU and NATO cybersecurity and cyber defense capacities, we are to compare the means used at NATO and the European Union that could complement each other. First, we are to compare the resilience capabilities: threat analysis and monitoring, system security and response capabilities.

Since the Warsaw Summit in July 2016, NATO member states have committed to improving their cyber defenses in order to ensure a high level of collective resilience for the whole Alliance. Beyond the individual efforts of member states, NATO has specific cyber defense capabilities:

* At NATO HQ, the Emerging Security Challenges Division is the strategic analysis body that ensures a coordinated approach to emerging defense and security risks. Cyber concerns are among other inter-national security challenges such as terrorism, proliferation of weapons of mass destruction or energy insecurity24.
* The NATO Communications and Information Agency (NCIA) supports NATO operations, connects information and communications systems, and defends NATO networks.
* The NATO Computer Incident Response Capability (NCIRC), located at Supreme Headquarters Allied Powers Europe (SHAPE), ensures the protection of NATO networks. With approximately 200 experts, the NCIRC continually works to prevent and, if necessary, respond to cyber incidents. This capability also has a role in analyzing future challenges.
* Finally, the establishment of a Cyber Operations Centre (CYOC) was decided in 2018 by the Heads of State at the Brussels Summit. This Centre, integrated into NATO's enhanced command structure, should be fully operational by 2023. It will provide the Alliance with real cyber response capabilities alongside the conventional capabilities (land, air, sea) made available by the Member States. Similarly, in the context of its missions and operations, NATO will be able to benefit from national IT capabilities[[53]](#footnote-53).

At the EU level, a set of institutional means also exists to ensure resilience in cyberspace. While parallels can be drawn with NATO agencies, the institutional set-up is based on a different conception: it is primarily built around cyber security, not specifically cyber defense. The 2013 Cyber Strategy makes resilience and cyber security the cornerstones of European action. Thus, in all three aspects mentioned above, there is a need to understand cyber defense capabilities as part of the broader cyber security structures:

* The role of analysis and strategic intelligence at the EU level is firstly carried out by the EU Intelligence Analysis Centre (INTCEN) in Brussels, Belgium, which was established in 2011. This structure has a threefold role: "to provide the High Representative, the EEAS and the Member States with intelligence analysis, early warning and awareness of specific geographic situations ". The European Institute for Security Studies (EUISS) in Paris, France, an autonomous think tank under the CSDP, also contributes to open-source analysis and risk forecasting in the cyber domain. Many of its publications focus on European cyber defense.
* ENISA, Heraklion, Greece, is the European Network and Information Security Agency. It provides recommendations and supports the development and implementation of cyber policies.
* The Union's response capacity has been ensured since 2012 by a permanent Computer Emergency Response Team (CERT-EU). It cooperates with Member States' response capacities and the private sector to respond to cyber incidents of all kinds.

However, the EU does not have a specific cyber operational response capability alongside conventional capability, as does NATO's CyOC. In the absence of such a capability, the EU Military Staff (EUMS) can provide military and operational expertise. The EUMS is the integrated military structure of the EU. It is attached to the EEAS and is fully multinational and joint. Two of its divisions provide expertise in cyber defence. Firstly, the Policy and Planning Division (CON/CAP) is responsible for doctrines, strategic planning concepts and capability development plans. Secondly, the Command and Information Systems Division (CIS) provides expertise on communications and information systems at both strategic and operational levels. However, there is no single center to steer planning and operational control in the cyber domain. It is therefore up to the existing planning structures to integrate cyber operational control into their operations. The five headquarters in the Member States are responsible for executive operations, while the Military Planning and Conduct Capability (MPCC) is responsible for non-executive operations. The current division between the MPCC and the five headquarters could make it difficult to deploy coherent cyber operational responses alongside conventional forces.

Next, we are to analyze how the technical factor is ensured at NATO and the European Union.

There is no doubt that cyber defense can only be effective and credible if it has information capabilities that ensure a high level of resilience. Both the Union and the Alliance have an added value in enhancing capabilities to achieve standardization and interoperability in this area.

Today, the EU's vulnerabilities result in particular from the fragmentation of national strategies and capabilities[[54]](#footnote-54). Inter-institutional cooperation is vital to ensure effective mechanisms, as well as the emergence of a strategic cyber defense culture. Military priorities in the field of cyberspace must be shared within the Union. The European Defense Agency (EDA) is the driving force at EU level for supporting the development of Member States' capabilities. It thus contributes to coordination and joint action through the development of joint and standardized military capabilities. In particular, the EDA is defining a Cyber Defense Strategic Research Agenda (CSRA) in order to target and pool the research and technology efforts needed to achieve a resilient European cyber defense.

The EU has a particular advantage in this area, as research and development is one of its shared competences[[55]](#footnote-55). Thus, beyond the EDA, European research and development programmes can also influence the European defense technological and industrial base and drive capability development in the field of cyber security and technological innovation. A joint Communication to the European Parliament and the Council recognizes that "the high level of resilience required for cyber defense requires a specific targeting of research and technology efforts"[[56]](#footnote-56).

NATO does not have as broad a remit as the EU and therefore has fewer means to influence the development of its members' capabilities. However, the Alliance remains active in this area, notably through the defense planning process. This process aims to ensure that NATO has the right set of capabilities to guarantee the security of its member states. NATO thus sets targets for the implementation of national capabilities. It thus pushes certain states to develop their capabilities to a sufficient level and strengthens the resilience of the Alliance. NATO has also established so-called 'smart defense' initiatives, which aim to pool the efforts of willing nations to develop and maintain capabilities that would otherwise be too costly to develop and maintain alone. Various projects in the field of cyber defense have been carried out, such as the Malware Information Sharing Platform (MISP) or the Multinational Cyber Defense Capability Development Project (MNCD2).

Third, we have to analyze the human factor at NATO and the Union’s levels., their education and training capacities.

In addition to the technical issue, defense is also a people issue. In both cyber security and cyber defense, the education and training dimension is therefore essential to ensure optimal preparation for potential threats and to deploy an effective response.

In this regard, various NATO branches are conducting cyber education, training and exercises to enhance the human capabilities of its members:

* The Cooperative Cyber Defense Centre of Excellence (CCD-COE) in Tallinn, Estonia, is a cyber defense research and training organization. It was established outside the NATO system and is therefore not part of the command structure. However, since October 2008, the CCD has been accredited by NATO as a Centre of Excellence (COE) and an international military organization. Since January 2018, the CCD-COE is more specifically responsible for the coordination of cyber defense education and training for all NATO agencies. As such, CCD-COE is de facto grafted into Allied Command Transformation (ACT).

NATO, and a variety of other actors, continue to be very attentive to the expertise and advice of the CCD-COE. This center is the source of the two Tallinn Manuals, documents that are influent in international opinion and in particular within the Alliance itself but are not official Alliance policy.

* Under the aegis of the NATO Communications and Information Agency (NCIA), an NCIA Academy opened in Oeiras (Portugal) in September 2019 to train civilians and military personnel in cyber defense, including the defense of information system and network connections. The NATO Communications and Information Systems School (NCISS), which was previously located in Latina, Italy, has been integrated into this Academy.
* A NATO Cyberpolygon in Tartu, Estonia, allows experts to train and develop their capabilities in realistic exercises. The Cyber Coalition exercise, one of NATO's largest cyber exercises, is facilitated by this facility every year.
* The NATO School in Oberammergau, Germany, conducts cyber-related training in operations, strategy, policy, doctrine and procedure.
* Finally, the NATO Defense College in Rome offers strategic thinking on military-political issues, including cyber defense issues.

At EU level, the European Defense Agency (EDA) also offers national and European cyber defense education and training modules. The main objective of these modules is to ensure the integration of cyber defense into the operational planning process. Furthermore, in the spirit of training, the EDA conducts dialogues and coordination actions between Member States and other international partners. The EDA thus also contributes to the enhancement of the EU's expertise in this field. In this way, these exchanges strengthen the Union's cyber defense by deterring "by denial" potential belligerent adversaries. The European Security and Defense College also plays an important role in terms of training in cyber issues but is aimed at a wider audience. The educational content of the College includes training elements on all aspects of cyber, but also on other issues such as hybrid threats that may involve cyber issues in wider military activities.

Regarding realistic exercises and preparations for cyber-attacks, ENISA is active in this field; it mainly deploys cyber security exercises, such as the "Blue OLEx" exercise organized in France in 2019. However, the European Union Military Staff (EUMS) should be looked to for cyber defense capacity building exercises. The EUMS also conducts close consultations and coordination activities with NATO and other international organizations in this context.

In conclusion, we need to analyze diplomatic capabilities: combining soft and hard power at both organizations.

On 19 June 2017, the Council of the European Union adopted the Cyber Diplomacy Toolbox (CDT). The CDT is intended to be a joint diplomatic response to malicious cyber activities. For Van der Meer, this 'toolbox' was designed as an important deterrent by identifying the potential consequences of a joint diplomatic response; a 'collective soft power' initiative that balances and complements the development of defensive and offensive capabilities of EU Member States or within NATO[[57]](#footnote-57). Furthermore, since 17 May 2019, the European Council has been able to impose "targeted restrictive measures to deter and counter cyber-attacks with significant effects which constitute an external threat to the Union or its Member States"[[58]](#footnote-58). The sanctions regime is in effect defensive against attacks and attempted cyber-attacks.

Furthermore, the EDA is contributing to the emergence of a European discourse on cyber at the international level. Having a strategic culture at the European level would not only help to strengthen cyber defense internally, but also to consolidate it externally. This European discourse is a second important element in the aforementioned deterrence by denial. To this end, the EU E-Strategy calls on the EDA to lead "dialogue and coordination between civilian and military actors in the EU", but also with international partners other than NATO.

**6.2.3 Opportunities to Deepen NATO-EU Cooperation in Cyberspace**

Thus, having analyzed the most critical fields of cyber defense at NATO and the EU, we can see in which room the articulation of the NATO and EU means is possible.

The analysis of the competences and means of the EU and NATO shows the progressive construction of their cyber defense architectures. Nevertheless, many duplications and grey areas can be quickly identified and may lead to uncertainties. An awareness of the importance of coordination between the two institutions is therefore necessary and is gradually gaining ground. The objective is therefore to seek complementarity or at least closer coordination between the two. This would promote the emergence of a stronger and more resilient collective cyber defense in Europe. This would include being able to clarify the respective perimeters of action of the EU and NATO, specifically for the member countries of both systems. For example, in the event that one of these states suffers a cyber-attack on the scale of an armed attack, the political choice between recourse to Article 5 of the Washington Treaty or Article 42.7 TEU could be made easier.

Like defense more generally, the Union's cyber defense cannot be conceived without taking into account that of the Alliance. The 2018 "cyber defiance" resolution also recalls the importance of the "transatlantic security architecture framework" in this context.

Cybersecurity and cyber defense together constitute one of the seven areas of enhanced cooperation between NATO and the EU since the Joint Declaration on Strengthening Practical Cooperation, signed in Warsaw in July 2016. A few months earlier, in February, a technical agreement between the two institutions was also signed to strengthen their cooperation on cyber defense. Specifically, as we have stated previously, this agreement between the NATO Computer Incident Response Capability (NCIRC) and CERT-EU aimed to strengthen protection against cyber-attacks by sharing best practices, among other things. There is therefore enhanced coordination between the two institutions in this area, resulting in the exchange of information, best practices, joint training and exercises, with the ultimate goal of interoperability of capabilities. These elements were in fact reiterated in the most recent joint declaration on cooperation between the EU and NATO signed last year, on 10 July 2018.

However, this coordination remains limited. As J. Joubert and J.-L. Samaan have expressed it, it is difficult to identify the elements of complementarity or subsidiarity between the two[[59]](#footnote-59). The cyblization of collective defense in Europe is essentially limited to exercises and training, and capability means are still lacking. Moreover, despite the desire to establish chains of command and response systems across institutions, these are struggling to be put in place, both at the EU and NATO levels[[60]](#footnote-60). Both organizations are experiencing the same difficulty that intergovernmentalism can cause. National sovereignty can then appear to be an obstacle to the development of a common cyber defense with mutual capabilities. While NATO is beginning to develop its cyber defense capabilities alongside its conventional capabilities, this is only a nascent development. For the EU, as more broadly in the project of a "Europe of defense", the institution has not managed to develop its own conventional capabilities because of divergent national political will. The Common Security and Defense Policy (CSDP) remains an intergovernmental policy. The CSDP remains an intergovernmental policy for which unanimity is the rule[[61]](#footnote-61).

While much effort has been made to adapt Europe's collective security and defense structures to the emerging threats of cyberspace, there are still several shortcomings in the regional architecture: the complexity of overlapping structures, the duplication of certain activities and the lack of clear subsidiarity between NATO and the EU, the difficulty of developing capabilities and the lack of interoperability, the lack of definition of clear doctrines, etc. Collective cyber defense is still under construction.

Yet, the EU and NATO have much in common in areas broader than operational exercises, the pursuit of interoperability, or capacity building. In terms of confidence-building measures, references, the applicability of international law, relations with the private sector or with other international partners, the EU and NATO share very similar approaches. These elements constitute potential avenues of reflection towards the development of common or complementary synergies.

First, European cyber defense must promote cooperation and exchange in order to reduce the risk of conflict. Confidence-building measures (CBMs) are particularly effective tools for this purpose. This is particularly true in cyberspace, which is characterized by a certain opacity. The Organization for Security and Co-operation in Europe (OSCE), for example, through its Decision No. 1202 (2016) has established an elaborate confidence building measures (CBM) framework aimed at reducing interstate conflicts arising from the use of information and communication technologies (ICT). It would be relevant for NATO and the EU to build on these cyberspace specific CBMs. Beyond the implementation of an elaborate CBM framework within the members of their institutions, cooperation on CBMs, first between the EU and NATO, and then possibly with other regional organizations in Europe (such as the OSCE) and beyond, would strengthen the effectiveness of European cyber defense.

Secondly, it is important for European cyber defense to maintain close links with the private sector, especially industry, a key player in cyberspace. Indeed, insofar as the majority of networks are owned and managed by private actors, it is difficult to conceive of a cyber defense that does not rely on a set of capabilities, civil and military, public and private. A complementarity between the European Union and the private sector is essential. Complementarity between NATO and the EU can also be developed in this respect, especially at the industrial level. For D. Fiott, it is the European defense industrial and technological base that holds the key to European interoperability and the harmonization of cyber defense capabilities[[62]](#footnote-62). Elements of industrial policy (supporting investment, supporting R&D, facilitating access to the market or to financing, encouraging the emergence of a specialized workforce) are therefore tools that should not be neglected in the implementation of an effective cyber defense policy.

The EU, as described above, has particularly powerful means at its disposal in this respect thanks to its extended competences. The "NATO-Industry Cyber Partnership" (NCIP), set up in 2014, could then be brought closer to the EU's activities in this field, especially those in the context of "Horizon 2020"/"Horizon Europe". Cooperation with the EDA and its CSRA or the European Investment Bank, which can provide funding for certain cybersecurity/cyberdefence projects, could also be beneficial. This rapprochement would aim to harmonize certain efforts to accelerate progress and innovation. Furthermore, beyond the industrial aspect, the EU and NATO can also work together with the private sector at the operational level to promote information sharing (between the private sector and government, but also within the private sector), as well as the adoption of common standards based on identified best practices. Indeed, on this last point, the standardization of security practices and means of response allows for a more robust cybersecurity - and therefore also by extension a cyberdefence. This standardization should be generalized to all actors involved.

Moreover, European cyber defense also has a role to play in international discussions and negotiations on international law applicable to cyberspace. Indeed, while there have been many discussions on the applicability of law in cyberspace, notably within the framework of the United Nations through its Group of Governmental Experts (UNGGE), there is no commonly adopted position at the international level and much remains to be done. The EU and NATO both recognize the applicability of law in cyberspace, and the European Union has a role to play. Both the EU and NATO recognize the applicability of international law in cyberspace. Closer coordination between the two bodies on possible norms and law enforcement measures in cyberspace would therefore already be an important step forward for the European region. Furthermore, in the international discussions on this issue, the EU can be a major influencer and play a considerable role in the negotiations as a very active observer member of the UN, with a coordinating force for the positions of its member states. The EU could defend, together with its member states, the values it promotes for an "open, safe and secure" cyberspace, as indicated in the title of its cybersecurity doctrine, the applicability of international law in cyberspace being one of its cornerstones. While recognizing that the founding treaty does not give NATO competence to defend positions on behalf of its member states in the same way as the EU since the Lisbon Treaty, the EU's diplomatic influence will be all the more important in the negotiations if NATO and EU member states are able to agree on the rules applied in Europe beforehand.

Finally, NATO and the EU must also work closely with third states. Effective cyber defense requires an increased dialogue with third states to help minimize the risk of conflict. Confidence-building measures should therefore also be implemented with states outside the Union and the Alliance (e.g. states that are particularly active in cyberspace). In addition, more advanced strategic partnerships can also be envisaged. The close relationship that the United States and Canada share with Europe could be the basis for an enhanced partnership between these regions. Australia, for example, has a cooperation program with the EU (August 2017) as well as with NATO (August 2019), both of which include several cyber-related aspects, including countering cyber threats of all kinds. A coordinated EU/NATO approach with certain partners in the field of cyber defense could have many benefits.

Thus, a collective cyber defense for Europe must be comprehensive in its approach. Extending its action beyond operational considerations is the best way to ensure robustness of defenses in the cyber space. A coordinated approach within this framework, with in particular a clear articulation of the two collective cyber defense systems, will reinforce the objectives sought and will represent a strong balance of power.

To conclude, cyberspace thus represents a new field for collective action in Europe. A collective cyber defense allows the entire region and its member states to arm themselves more effectively against the cyber threat. NATO and the EU are working on the construction of this, but it is not yet complete. These two institutions, because of their composition and the fact that they share a majority of members in common, have a very similar area of action in Europe, which gives rise to certain overlaps and doubloons of activities. In order for their actions to be as effective as possible, they should both operate in a complementary manner with clear elements of subsidiarity with each other. In the absence of complementarity, a coordinated approach remains a minimum to maintain the credibility of collective cyber defense in Europe. The joint membership of 22 states should be an important force in this process of rapprochement and coordination.

Finally, this cyber defense, whatever its form, must be global in its approach. Without limiting itself to operational responses or capability elements, it must contribute more generally to international peace and security by promoting confidence-building measures with all international actors (States, organizations, companies), by participating in discussions on the applicability of international law to cyberspace and by pursuing joint synergies with the private sector. The dual nature of cyberspace means that civilian cyberspace regulations are also binding for military applications. The EU, with a regulatory capacity far superior to that of NATO, thus plays a decisive role in cyber defense, even if its primary concern is cyber security.

Today, NATO member states seem to have more tools to respond at an operational level to belligerent cyber-attacks, especially with the start of the Integrated Cyber Operations Center under the enhanced command structure. Yet the real opportunity lies with the EU, which operates across the entire cyber security-cyber defense spectrum. As a diplomatic power with significant European soft power, it must now strengthen its skills and resources in this area, specifically in cyber defense, while the viability of the Alliance is being questioned by the American president, Donald Trump. Moreover, with the imminent exit of the United Kingdom from the Union, the main blocking factor in the development of a European defense policy, a new dynamic towards a common policy (or at least elements of common defense) seems possible. In this particular context, the EU has more than ever the opportunity to develop its own strategic culture, allowing it to assert its strategic autonomy and build a European hard power in cyberspace.

**References:**

1. Booth, K. (1991). Security and Emancipation. Review of International Studies, 17(4).
2. Buzan, B. (1991). New Patterns of Global Security in the Twenty-First Century. International Affairs (Royal Institute of International Affairs 1944-), 67(3), 431–451. JSTOR. https://doi.org/10.2307/2621945.
3. Christopher Grundy, What is the Difference Between a Realist and a Gramscian Understanding of Hegemony? [Electronic resource]. – International Relations. URL: https://www.e-ir.info/2012/06/08/what-is-the-difference-between-a-realist-and-a-gramscian-understanding-of-hegemony/.
4. Cox, R.W. (1981). Social Forces, States and World Orders: Beyond International Relations Theory. Millennium: Journal of International Studies 10(2).
5. Cox, Robert W. “Gramsci, Hegemony and International Relations : An Essay in Method.” Millennium 12, no. 2 (June 1983): 162–75. https://doi.org/10.1177/03058298830120020701.
6. Herz, John H. "Idealist Internationalism and the Security Dilemma." World Politics 2, no. 2 (1950): 157-80. Accessed October 25, 2021. doi:10.2307/2009187.
7. Krause, Keith. "Critical Theory And Security Studies: The Research Programme of 'Critical Security Studies'." Cooperation and Conflict 33, no. 3 (1998): 298-333. Accessed October 24, 2021. http://www.jstor.org/stable/45083929.
8. Leysens A. (2008) The Legacy of Coxian Critical Theory. In: The Critical Theory of Robert W. Cox. International Political Economy Series. Palgrave Macmillan, London. https://doi.org/10.1057/9780230584457\_6.
9. Marcos Farias Ferreira, Introducing Critical Theory in International Relations [Electronic resource]. – International Relations. URL: https://www.e-ir.info/2018/02/18/introducing-critical-theory-in-international-relations/.
10. Matt Davies, IR Theory: Problem-Solving Theory Versus Critical Theory? [Electronic resource]. – International Relations. URL: https://www.e-ir.info/2014/09/19/ir-theory-problem-solving-theory-versus-critical-theory/.
11. Moolakkattu JS. Robert W. Cox and Critical Theory of International Relations. International Studies. 2009;46(4):439-456. doi:10.1177/002088171004600404.
12. Nunes, João. "Reclaiming the Political: Emancipation and Critique in Security Studies." Security Dialogue 43, no. 4 (2012): 345-61. Accessed October 25, 2021. http://www.jstor.org/stable/26301921.
13. Sallach, David L. "Class Domination and Ideological Hegemony." The Sociological Quarterly 15, no. 1 (1974): 38-50. Accessed October 25, 2021. http://www.jstor.org/stable/4105619.
14. Wyn Jones, R. (1999). Security, strategy and critical theory. Colorado: Lynne Rienner Publications.
15. Zaslavskaya N. (2017). ‘Theories of International Relations’, in Russia and the World. (ed.). Lexington Books: Maryland. pp. 35-37.

Appendix

Appendix I: The European Peninsula and Russia

Map

Description automatically generated

The European Peninsula and Russia, a map by the Geopolitical Futures portal 27[[63]](#footnote-63)

Appendix B

Map

Description automatically generated

A map showing European membership of the EU and NATO. Great Britain is no longer the case

Appendix C

Map

Description automatically generated

***Приложение 1.***

**Государства-члены Европейского Союза[[64]](#footnote-64)**



***Приложение 5.***

**Сводный индекс инновационного развития стран ЕС[[65]](#footnote-65)**



Appendix C

Timeline

Description automatically generated with low confidence

## The Increasing Prominence of Cyber(Security) as perceived by NATO

This section ensues a discussion based on the findings of the quantitative content analysis.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Year** | **Cyber** | | **New Threats** | | **Stability**  **Security in Region** | | **Terrorism** | | **Proliferation WMD** | | **Biological,Nuclear, Chemical Weapons** | | **Russia** | | **Article 5** | | |
| 2002 | 2 | | 1 | | 3 | | 19 | | 8 | | 2 | | 46 | | 2 | | |
| 2003 | 1 | | 0 | | 0 | | 1 | | 0 | | 1 | | 3 | | 0 | | |
| 2004 | 1 | | 3 | | 2 | | 36 | | 17 | | 7 | | 16 | | 0 | | |
| 2005 | | 1 | | 0 | | 0 | | 4 | | 0 | | 0 | | 21 | | 0 |
| 2006 | | 2 | | 0 | | 2 | | 13 | | 9 | | 2 | | 14 | | 0 |
| 2007 | | 6 | | 2 | | 0 | | 3 | | 1 | | 1 | | 1 | | 0 |
| 2008 | | 9 | | 0 | | 1 | | 12 | | 16 | | 8 | | 22 | | 1 |
| 2009 | | 7 | | 0 | | 0 | | 1 | | 0 | | 0 | | 0 | | 0 |
| 2010 | | 20 | | 0 | | 3 | | 8 | | 16 | | 8 | | 19 | | 2 |
| 2011 | | 3 | | 1 | | 0 | | 1 | | 0 | | 1 | | 4 | | 0 |
| 2012 | | 15 | | 0 | | 2 | | 14 | | 15 | | 9 | | 35 | | 1 |
| 2013 | | 2 | | 0 | | 2 | | 2 | | 0 | | 2 | | 0 | | 0 |
| 2014 | | 20 | | 0 | | 2 | | 13 | | 13 | | 14 | | 46 | | 3 |
| 2015 | | 9 | | 0 | | 0 | | 0 | | 0 | | 0 | | 8 | | 1 |
| 2016 | | 2 | | 0 | | 1 | | 3 | | 0 | | 0 | | 42 | | 1 |
| 2017 | | 7 | | 0 | | 2 | |  | |  | |  | |  | |  |
| Total | | 100 | | 7 | | 18 | | 130 | | 95 | | 55 | | 277 | | 11 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2005 | 1 | 0 | 0 | 4 | 0 | 0 | 21 | 0 |
| 2006 | 2 | 0 | 2 | 13 | 9 | 2 | 14 | 0 |
| 2007 | 6 | 2 | 0 | 3 | 1 | 1 | 1 | 0 |
| 2008 | 9 | 0 | 1 | 12 | 16 | 8 | 22 | 1 |
| 2009 | 7 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 2010 | 20 | 0 | 3 | 8 | 16 | 8 | 19 | 2 |
| 2011 | 3 | 1 | 0 | 1 | 0 | 1 | 4 | 0 |
| 2012 | 15 | 0 | 2 | 14 | 15 | 9 | 35 | 1 |
| 2013 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 0 |
| 2014 | 20 | 0 | 2 | 13 | 13 | 14 | 46 | 3 |
| 2015 | 9 | 0 | 0 | 0 | 0 | 0 | 8 | 1 |
| 2016 | 2 | 0 | 1 | 3 | 0 | 0 | 42 | 1 |
| Total | 100 | 7 | 18 | 130 | 95 | 55 | 277 | 11 |

**Table 1: Word Frequency**

1. Kerner, S. M. (2022, March 15). 34 Cybersecurity Statistics to Lose Sleep Over in 2022. WhatIs.Com. https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020 [↑](#footnote-ref-1)
2. Hsieh, H. F., & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. Qualitative Health Research, 15(9), 1277–1288. https://doi.org/10.1177/1049732305276687 [↑](#footnote-ref-2)
3. Berlinger, J. C. (2022, May 16). Finland and Sweden want to join NATO. Here’s how it works and what comes next. CNN. https://edition.cnn.com/2022/05/14/europe/sweden-finland-nato-next-steps-intl/index.html [↑](#footnote-ref-3)
4. Tardy, T. (2018). Does European defence really matter? Fortunes and misfortunes of the Common Security and Defence Policy. European Security, 27(2), 119–137. https://doi.org/10.1080/09662839.2018.1454434 [↑](#footnote-ref-4)
5. Poptchev, Peter. "NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages." Information & Security: An International Journal 45 (2020): 35-55. [↑](#footnote-ref-5)
6. Manners, Ian. “The Normative Ethics of the European Union.” International Affairs (Royal Institute of International Affairs 1944-), vol. 84, no. 1, 2008, pp. 45–60, http://www.jstor.org/stable/25144714. Accessed 16 May 2022. [↑](#footnote-ref-6)
7. Duke, S. (2016). Europe’s Harder Edges: Security and Defence. Europe as a Stronger Global Actor, 171–203. https://doi.org/10.1057/978-1-349-94945-8\_8 [↑](#footnote-ref-7)
8. Howorth, J. (2005). The Euro-Atlantic Security Dilemma: France, Britain, and the ESDP. Journal of Transatlantic Studies, 3(1), 39–54. https://doi.org/10.1080/14794010508656816 [↑](#footnote-ref-8)
9. Howorth, Jolyon. "Jolyon Howorth: Great Britain and Europe: From Resistance to Rancor", Politique étrangère, vol. i, no. 2, 2010, pp. 259-271. [↑](#footnote-ref-9)
10. Adam Posen (2013). The Euro at Five: Ready for a Global, 01(01). https://doi.org/10.4172/2375-4389.1000e101 [↑](#footnote-ref-10)
11. Carriço, G. (2017). Strengthening the EU’s Resilience in the Virtual Domain. European View, 16(2), 331. https://doi.org/10.1007/s12290-017-0465-3 [↑](#footnote-ref-11)
12. 2014 Wales Summit will only start the process of finding NATO’s new balance. (2014). European Leadership Network. https://www.europeanleadershipnetwork.org/commentary/the-2014-wales-summit-will-only-start-the-process-of-finding-natos-new-balance/ [↑](#footnote-ref-12)
13. Alatalu, Siim, et al. “NATO’s Responses to Cyberattacks.” HACKS, LEAKS AND DISRUPTIONS: RUSSIAN CYBER STRATEGIES, edited by Nicu Popescu and Stanislav Secrieru, European Union Institute for Security Studies (EUISS), 2018, pp. 95–102, http://www.jstor.org/stable/resrep21140.13. Accessed 16 May 2022. [↑](#footnote-ref-13)
14. Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA. (2021). Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. https://www.cisa.gov/uscert/ncas/alerts/aa22-110a [↑](#footnote-ref-14)
15. Internet Organized Crime Threat Assessment (IOCTA). (2019). https://www.europol.europa.eu/publications-events/main-reports/iocta-report [↑](#footnote-ref-15)
16. Dunn Cavelty, M., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, 41(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855 [↑](#footnote-ref-16)
17. Douzet, F. (2014). La géopolitique pour comprendre le cyberespace. Hérodote, 152-153, 3-21. https://doi.org/10.3917/her.152.0003 [↑](#footnote-ref-17)
18. Turner, Frederick Jackson, 1861-1932. (1894). The significance of the frontier in American history. Madison: State Historical Society of Wisconsin. [↑](#footnote-ref-18)
19. Nazario, J. (2008). DDoS attack evolution. Network Security, 2008(7), 7–10. https://doi.org/10.1016/s1353-4858(08)70086-2 [↑](#footnote-ref-19)
20. Joubert, V. & Samaan, J. (2014). L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE. Hérodote, 152-153, 261-275. https://doi.org/10.3917/her.152.0261 [↑](#footnote-ref-20)
21. Comprehensive Study on Cybercrime. (2013). https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ\_Sessions/CCPCJ\_22/\_E-CN15-2013-CRP05/Comprehensive\_study\_on\_cybercrime.pdf [↑](#footnote-ref-21)
22. PROPOSITION DE RÉSOLUTION sur l’Estonie. (2007). Union européenne, 2007 - Source: Parlement européen. https://www.europarl.europa.eu/doceo/document/B-6-2007-0220\_FR.html [↑](#footnote-ref-22)
23. Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. Science (New York, N.Y.), 359(6380), 1146–1151. https://doi.org/10.1126/science.aap9559 [↑](#footnote-ref-23)
24. Thomas, E., Thompson, N., & Wanless, A. (2020, June 10). The Challenges of Countering Influence Operations. Carnegie Endowment for International Peace. https://carnegieendowment.org/2020/06/10/challenges-of-countering-influence-operations-pub-82031 [↑](#footnote-ref-24)
25. Desforges, Alix. « Les représentations du cyberespace : un outil géopolitique », Hérodote, vol. 152-153, no. 1-2, 2014, pp. 67-81. [↑](#footnote-ref-25)
26. Masoumifar, A. (2022). Cyberspace Sovereignty: Is Territorializing Cyberspace Opposed to Having a Globally Compatible Internet?. Journal of Cyberspace Studies, 6(1), 1-20. doi: 10.22059/jcss.2022.327215.1064 [↑](#footnote-ref-26)
27. Dorothy Denning, "Levels of Cyberterror Capability: Terrorists and the Internet," http://www.cs.georgetown.edu/~denning/infosec/Denning-Cyberterror-SRI.ppt, presentation, and Zack Phillips, "Homeland Tech Shop Wants to Jump-Start Cybersecurity Ideas," CQ Homeland Security, September 14, 2004 at http://homeland.cq.com/hs/display.do?docid=1330150&sourcetype=31&binderName=news-all. [↑](#footnote-ref-27)
28. Hunker, Jeffrey. Cyber war and cyber power Issues for NATO doctrine / Hunker, Jeffrey // Semantic Scholar. – 2010. – №3. – P. 158. [↑](#footnote-ref-28)
29. Amoore, L., de Goede, M. Risk and the War on Terror. – London: Routledge, 2008. – Р. 156. [↑](#footnote-ref-29)
30. Officially entitled “The Overall Strategic Concept for the Defense of the North Atlantic Area”, MC 14/3 has been better known as “flexible response,” which describes the essence of the strategy. [↑](#footnote-ref-30)
31. Member countries (18): Belgium, Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Netherlands, Poland, Portugal, Slovakia, Spain, Turkey, United Kingdom, United States.

    Partner countries (3): Austria, Finland, Sweden. [↑](#footnote-ref-31)
32. Sallach, D. L. (1974). Class Domination and Ideological Hegemony. The Sociological Quarterly, 15(1), 38–50. http://www.jstor.org/stable/4105619 [↑](#footnote-ref-32)
33. Herz, J. H. (1950). Idealist Internationalism and the Security Dilemma. World Politics, 2(2), 157–180. https://doi.org/10.2307/2009187 [↑](#footnote-ref-33)
34. Zaslavskaya N. (2017). ‘Theories of International Relations’, in Russia and the World. (ed.). Lexington Books: Maryland. pp. 35-37. [↑](#footnote-ref-34)
35. Cox, Robert W. “Social Forces, States and World Orders: Beyond International Relations Theory.” Millennium 10, no. 2 (June 1981): 126–55. https://doi.org/10.1177/03058298810100020501. [↑](#footnote-ref-35)
36. Cox, Robert W. “Social Forces, States and World Orders: Beyond International Relations Theory.” Millennium 10, no. 2 (June 1981): 126–55. https://doi.org/10.1177/03058298810100020501. [↑](#footnote-ref-36)
37. Cox, Robert W. “Gramsci, Hegemony and International Relations: An Essay in Method.” Millennium 12, no. 2 (June 1983): 162–75. https://doi.org/10.1177/03058298830120020701. [↑](#footnote-ref-37)
38. Cox, Robert W. “Gramsci, Hegemony and International Relations: An Essay in Method.” Millennium 12, no. 2 (June 1983): 162–75. https://doi.org/10.1177/03058298830120020701. [↑](#footnote-ref-38)
39. Krause, Keith. "Critical Theory And Security Studies: The Research Programme of 'Critical Security Studies'." Cooperation and Conflict 33, no. 3 (1998): 298-333. Accessed December 7, 2020. http://www.jstor.org/stable/45083929. [↑](#footnote-ref-39)
40. Welch, D. A. (2000). [Review of Security, Strategy, and Critical Theory, by R. W. Jones]. The American Political Science Review, 94(2), 522–524. https://doi.org/10.2307/2586105. [↑](#footnote-ref-40)
41. Booth, Ken. (1991). “Security and Emancipation”, Review of International Studies, Vol. 17, No. 4 (Oct., 1991), pp. 313-326. [↑](#footnote-ref-41)
42. Buzan, B. (1991). New Patterns of Global Security in the Twenty-First Century. International Affairs (Royal Institute of International Affairs 1944-), 67(3), 431–451. JSTOR. https://doi.org/10.2307/2621945 [↑](#footnote-ref-42)
43. Resolution 1160 of 1998, imposes an arms embargo on the former Yugoslavia Resolution 1190 of 1998, requires the withdrawal of troops from Kosovo [↑](#footnote-ref-43)
44. Charles Goerens, former President of the Western European Union [↑](#footnote-ref-44)
45. Competent body for the command of the integrated military structure [↑](#footnote-ref-45)
46. Seth, C., & von Kulessa, R. (Eds.) 2017. 58. The Balance of Power and Future Peace. In The Idea of Europe: Enlightenment Perspectives. Open Book Publishers. Tiré de http://books.openedition.org/obp/4346 [↑](#footnote-ref-46)
47. Joubert, Vincent, et Jean-Loup Samaan. « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE », Hérodote, vol. 152-153, no. 1-2, 2014, pp. 261-275. [↑](#footnote-ref-47)
48. B. Tertrais. Article 5 of the Washington Treaty: Its Origins, Meaning and Future / B. Tertrais // Research Division, NATO Defense College. – 2016. – P.12. [↑](#footnote-ref-48)
49. Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA). URL: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a. [↑](#footnote-ref-49)
50. European Parliament resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606(RSP)),. (2013). https://www.europarl.europa.eu/doceo/document/TA-7-2013-0376\_EN.html. [↑](#footnote-ref-50)
51. D. Deschaux-Dutard. Cybersécurité et cyberdéfense : Éléments d’introduction du point de vue de la science politique / D. Deschaux-Dutard // Cyber, Nano : Nouvelles technologies et nouveaux enjeux sécuritaires, Cours dans le cadre du master Sécurité internationale et défense de la faculté de droit de Grenoble. – 2017. – P.232. [↑](#footnote-ref-51)
52. Reflection paper on the future of European defence. (2017). https://ec.europa.eu/info/publications/reflection-paper-future-european-defence\_en [↑](#footnote-ref-52)
53. Cyberdéfense de l’OTAN. (2018). https://www.nato.int/nato\_static\_fl2014/assets/pdf/pdf\_2018\_02/20180213\_1802-factsheet-cyber-defence-fr.pdf [↑](#footnote-ref-53)
54. E. Nagyfejo, Transatlantic collaboration in response to cybercrime: how does strategic culture affect EU-US collaboration in the fight against cyber crime?, thèse doctorale, Université de Warwick, déposée septembre 2016 ; Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense (2018/2004(INI)), Strasbourg, 13 juin 2018. [↑](#footnote-ref-54)
55. Klamert, Marcus. "Article 4 TFEU." In the EU Treaties and the Charter of Fundamental Rights: A Commentary. Oxford University Press, 2019. Oxford Scholarship Online, 2021. doi: 10.1093/oso/9780198759393.003.75. [↑](#footnote-ref-55)
56. Joint Communication to The European Parliament and The Council. (2019). https://data.consilium.europa.eu/doc/document/ST-12211-2017-INIT/en/pdf [↑](#footnote-ref-56)
57. . Van der Meer, (2017). EU Creates a Diplomatic Toolbox to Deter Cyberattacks. Council of Foreign Affairs. https://www.cfr.org/blog/eu-creates-diplomatic-toolbox-deter-cyberattacks [↑](#footnote-ref-57)
58. Consolidated text: Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02019D0797-20210519 [↑](#footnote-ref-58)
59. J. Joubert & J.-L. Samaan, « L’intergouvernementalité dans le cyberespace : étude comparée des initiatives de l’OTAN et de l’UE », op. cit., p. 275. [↑](#footnote-ref-59)
60. Fiott, D. (2017). The cybridisation of EU defence. Issue Alert, 24. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert%2024%20Cybridisation%20of%20defence.pdf [↑](#footnote-ref-60)
61. Consolidated version of the Treaty on European Union - TITLE V: GENERAL PROVISIONS ON THE UNION'S EXTERNAL ACTION AND SPECIFIC PROVISIONS ON THE COMMON FOREIGN AND SECURITY POLICY - Chapter 2: Specific provisions on the common foreign and security policy - Section 2: Provisions on the common security and defence policy - Article 42 (ex Article 17 TEU), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12008M042 [↑](#footnote-ref-61)
62. Fiott, D. (2017). The cybridisation of EU defence. Issue Alert, 24. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert%2024%20Cybridisation%20of%20defence.pdf [↑](#footnote-ref-62)
63. The European Peninsula and Russia, a map by the Geopolitical Futures... | Download Scientific Diagram (researchgate.net) [↑](#footnote-ref-63)
64. Map of the EU 2020 [Электронный ресурс] // Map of Europe. – Режим доступа: https://mapofeurope.com/eu-map-2020/ [↑](#footnote-ref-64)
65. Составлено автором на основе данных официального сайта Европейского парламента (2019 Innovation Scoreboards: The innovation performance of the EU and its regions is increasing [Электронный ресурс] / European Parlaiment. – Режим доступа : https://ec.europa.eu/regional\_policy/en/newsroom/news/2019/06/17-06-2019-2019-innovation-scoreboards-the-innovation-performance-of-the-eu-and-its-regions-is-increasing) [↑](#footnote-ref-65)