САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Шидуков Асхад Хастинович

Выпускная квалификационная работа

СОТРУДНИЧЕСТВО НАТО И ЕВРОПЕЙСКОГО СОЮЗА В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ И КИБЕРОБОРОНЫ В ЭПОХУ УСИЛЕНИЯ СОРЕВНОВАНИЙ ВЕЛИКИХ ДЕРЖАВ

NATO-EU COOPERATION IN CYBERSECURITY AND CYBER DEFENSE IN THE AGE OF INCREASED GREAT POWERS COMPETITIONS

Направление 41.04.05 - “Международные отношения”,

Основная образовательная программа

магистратуры “Международные отношения (на английском языке)”

Научный руководитель:
Кандидат политических наук
Доцент кафедры американских исследований
Богуславская Юлия Константиновна

Рецензент:
Заместитель директора Института стратегических исследований и прогнозов Российского университета дружбы народов
Юраков Максим Вячеславович

Санкт-Петербург

2022

Аннотация. Стремительное развитие информационно-коммуникационных технологий (ИТК) за последние 20 лет стало мощным катализатором изменений в международных отношениях, а также способом использования ИТ-технологий для достижения определенных внешнеполитических целей. В связи с активным распространением доступа к интернету среди широких масс населения планеты, всё чаще во всех сферах общественной жизни используются такие термины, как «информационная война», «кибербезопасность», «киберзащита» и «информационные технологии».

Появление киберпространства ознаменовало не только создание искусственной сферы коммуникации и цифровой торговли, но и активизацию враждебной активности в информационном пространстве, способную нанести урон национальной безопасности, социально-экономической стабильности и сплоченности сообщества. Кибератаки иностранных субъектов, включая негосударственных и государственных акторов, являются стратегическим вызовом для ЕС и НАТО. Анализ существующих областей сотрудничества в киберпространстве, а также юридической основы между ЕС и НАТО имеет важное практическое значение. Статья 5 Устава НАТО является основой коллективной безопасности в Европе, однако учитывая то, что многие инциденты в киберпространстве находятся ниже порога применения силы, киберзащита выходит за рамки классических военных компетенций НАТО. В данной связи анализ существующих инструментариев ЕС, наделенного более широкими полномочиями учредительными договорами, а также их последующий сравнительный анализ с компетенциями НАТО, представляет важное научно-практическое значение.

Ключевые слова: международная безопасность, кибербезопасность, киберзащита, НАТО, Европейский союз, контент-анализ, сравнительный анализ, Статья 5 Устава НАТО.

Abstract. Rapid growth of Information and communication technologies (ICT) over the past 20 years has become a dramatic catalyst of changes in International Relations, as well as a way of using IT technologies to achieve certain foreign policy goals. Due to the active spread of access to the Internet among global population, terms such as "information warfare", "cybersecurity", "cyber defense" and "information technology" are increasingly in use in all social spheres.

The emergence of cyberspace marked not only the creation of a man-made sphere of communication and digital trade but also the intensification of hostile activity in the digital space, which could engender national security, socio-economic stability, and community cohesion. Cyber-attacks by foreign actors, including nonstate and state actors, are a strategic challenge for the EU and NATO. An analysis of existing areas of cooperation in cyberspace, as well as the legal framework between the EU and NATO, is of important practical significance. Article 5 of the Washington Treaty is the cornerstone of the collective security in Europe but given that many incidents in cyberspace are below the threshold of the use of force, cyber defense falls outside NATO's classic military competencies. In this regard, the analysis of existing EU tools, endowed with broader powers by the founding treaties, and their subsequent comparative analysis with NATO competencies is of scientific and practical significance.

Key words: International Security, Cybersecurity, Cyber defense, NATO, EU, Content Analysis, Comparative Analysis, Article 5 of the North Atlantic Treaty.

Contents

List of Abbreviations

List of Abbreviations

CBM - Confidence-Building Measures

CCD-COE - The Cooperative Cyber Defense Centre of Excellence

CERT - Computer Emergency Response Team

CFSP - The Common Foreign and Security Policy

CRRT - Cyber Rapid Response Team

CSDP - The Common Security and Defense Policy

CSRA - Cyber Defense Strategic Research Agenda

CyCLONe - Cyber Crises Liaison Organisation Network

CYOC - Cyber Operations Centre

EDA - The European Defense Agency

ENISA - European Union Agency for Cybersecurity

ESCD - Emerging Security Challenges Division

EU – The European Union

EU INTCEN - European Union Intelligence and Situation Centre

ICT - Information and Communication Technologies

NATO - The North Atlantic Treaty Organization

NCIA - NATO Communications and Information Agency

NCIRC - NATO Computer Incident Response Capability

NCISS - The NATO Communications and Information Systems School

NICP - NATO-Industry Cyber Partnership

OSCE - The Organization for Security and Cooperation in Europe

TEU - The Treaty on European Union

Introduction

The relevance of the study is determined by the Information revolution and its impact on social, economic, and technological development in a post-industrial society. At the impressive speed the development and interconnectedness of Information and Communication technologies (ICTs) are spreading around the globe, and internet is one of the most salient examples. According to Datareporter, 5 billion people around the world use the internet today – equivalent to 63 percent of the world's total population[1]. As a result, the economic and political incentives to exploit the network for malicious purposes have also increased, and cybersecurity has reached head-of-state-level attention.

In the past two decades, cyberspace has emerged as a priority security issue on international diplomatic agendas. It is often presented as the field that will revolutionize the conduct of politics both at the national level and within the international system. Cyberspace per se, unlike many other traditional domains of International Relations, is created by human beings. Thus, actors of International Relations elaborate this space in their own image depending on their understanding of cyberspace, the rules that could be applied in this domain, and the limitations states impose in cyberspace.

Not only states, as actors of International Relations, attempt to navigate in the domain which lacks rigid international rules, but also international organizations. Analysis of the EU-NATO cooperation within the field of cyberspace has important scientific and practical significance. The North Atlantic Treaty Organization (NATO) and the European Union (EU) are different in their raison d'être, their essence, and their membership. Any direct bilateral agenda is difficult to imagine. Thus, the analysis of the cooperation between the European Union and NATO in cyberspace 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. 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[2]. Today, NATO and EU Member States face a more diverse, complex and rapidly evolving security environment than at any time since the end of the Cold War.

[1] Digital Around the World. (2022, April). DataReportal – Global Digital Insights. URL: https://datareportal.com/global-digital-overview#:%7E:text=A%20total%20of%205%20billion,12%20months%20to%20April%20202 (Accessed 12.05.2022).

[2] Kerner, S. M. (2022, March 15). 34 Cybersecurity Statistics to Lose Sleep Over in 2022. WhatIs.Com. URL: https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020 (Accessed 12.05.2022).

The analysis of EU-NATO cybersecurity and cyber defense are of special interest inasmuch as at NATO cyber is declared as a domain of operations and a large-scale cyberattack on a Member State could potentially invoke Article 5 of the Washington Treaty. Similarly, to the North Atlantic Treaty Organization, a damaging cyberattack on the EU Member State may trigger a common response from all EU Members: the solidarity clause (Article 222 TFEU) could be invoked on the grounds of "a particularly serious cyber incident or attack"[1].

The comparative analysis of the legal framework, as well as the available tools to address threats in cyberspace in NATO and the EU, is of great scientific and practical importance. The aforesaid circumstances predetermined the relevance of the chosen topic of the study.

Practical significance of the study. Certain provisions of the study represent the basis for analytical forecasting of the further development of the “cyber” in the EU-NATO relations. Some of the results gained in this work can be used in the educational process, in the development and leading courses on International relations, world politics and regional studies.

The scientific novelty of the research lies in the inter-institutional analysis of the interaction between the European Union and The North Atlantic Treaty Organization with regards to cybersecurity and defense. For the first time a comparative analysis of legal, resilience, information, education and training capacities of two aforementioned international organizations have been conducted. On this basis the previous fragmented and non-comprehensive knowledge has been visualized which demonstrated how the harmonization of the EU cybersecurity policy and the NATO cyber defense policy could not only complement one another but strengthen each other and ensure security for all parties engaged.

The research question guiding this thesis is the following, ‘What is the current state of progress and shortcomings in cyberspace cooperation between NATO and the European Union with regard to cybersecurity and defense?’.

The object of the study is the European Union and The North Atlantic Treaty Organization’s cyber policies.

The subject of the study is the NATO-EU cooperation in cybersecurity and cyber defense in the age of increased great powers competitions.

The aim of the work is to identify the features of the EU-NATO cooperation in cyberspace with regards to cybersecurity and defense from a critical theoretical framework that ensures that the technological impact of cyberspace on this political relationship is not overlooked in order to

[1] Reflection paper on the future of European defence. (2017). URL: https://ec.europa.eu/info/publications/reflection-paper-future-european-defence_en (Accessed 09.03.2022).

determine how two international organizations could complement one another.

The objectives of the research are:

1. Analyze the existing EU-NATO Cooperation in Cyberspace;
2. Identify NATO Cyber Defence Policy;
3. Determine EU Cyber Security Policy;
4. Compare EU-NATO Cyber Strategies: their similarities and differences;
5. Determine Perspectives for EU-NATO cooperation.

Literature and sources analysis. This thesis is based on the analysis of primary and secondary sources. The primary sources are the official EU and NATO documents from 2004 up to 2020 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[1]. There are many prominent foreign researchers who study NATO such as Thierry Tardy, Chloe Berger, Silvia Maria Colombo, Andrea Gilli, as well as Russian prominent researchers Mikhail Viktorovich Volkov, Yulia Konstantinovna Boguslavskaya, Evgenia Viktorovna Israelyan, and the others[2].

[1] Berlinger, J. C. (2022, May 16). Finland and Sweden want to join NATO. Here's how it works and what comes next. CNN. URL: https://edition.cnn.com/2022/05/14/europe/sweden-finland-nato-next-steps-intl/index.html (Accessed 19.05.2022).

[2] Boguslavskaya, Y. K. (2013). NATO in U.S. Global Politics: American Concepts of Transformation. URL: https://www.dissercat.com/content/nato-v-globalnoi-politike-ssha-amerikanskie-kontseptsii-transformatsii; Evgenia Viktorovna Israelyan, E. (2010). CANADA - NATO: EVOLUTION OF APPROACHES. The United States and Canada:

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.

Most of researchers downplay the role of the Union in comparison to NATO, or even perceive it as non-important and non-essential 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[1]. 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[2]. 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 civilianpower. 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[3]. However, there are some authors, for instance Simon Duke, that states that the European Union can be longer seen as civilianpower inasmuch as it will no longer be able to adequately defend its interests around the globe [4]. 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

Economics, Politics, and Culture; Colombo, S. (2018). Challenging the State from Above, Empowering It from Within. IEMed Mediterranean. URL: https://www.iemed.org/publication/challenging-the-state-from-above-empowering-it-from-within/; Tardy, T., & Lindstrom, G. (Eds.). (2019). The scope of EU-NATO cooperation. In NATO and the EU: The essential partners (pp. 5–14). NATO Defense College. URL: http://www.jstor.org/stable/resrep19964.6.

[1] Tardy, T. (2018). Does European defence really matter? Fortunes and misfortunes of the Common Security and Defence Policy. European Security, 27(2), 119–137. URL: https://doi.org/10.1080/09662839.2018.1454434

[2] Poptchev, Peter. "NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages." Information & Security: An International Journal 45 (2020): 35-55.

[3] 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. URL: http://www.jstor.org/stable/25144714. (Accessed 16 May 2022).

[4] Duke, S. (2016). Europe's Harder Edges: Security and Defence. Europe as a Stronger Global Actor, 171–203. URL: https://doi.org/10.1057/978-1-349-94945-8_8.

Ethics of the European Union" argues that the Union represents a 'normative power' since it acts to extend its norms in international system.

Author then overview the cooperation between the EU and NATO 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 [1]. 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[2]. Thus, the

[1] Howorth, J. The Euro-Atlantic Security Dilemma: France, Britain, and the ESDP/ Howorth // Journal of Transatlantic Studies, 3(1). – 2005. -P. 39–54.

[2] Howorth, Jolyon. Jolyon Howorth: Great Britain and Europe: From Resistance to Rancor / Howorth, Jolyon // Politique étrangère, vol. i, no. 2. – 2010. – P. 259-271.

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[1].

Finally, it has to be stated that 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[2]. 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[3].

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,

[1] Adam Posen (2013). The Euro at Five: Ready for a Global, 01(01). URL: https://doi.org/10.4172/2375-4389.1000e101. (Accessed 02.03.2022).
[2] Carriço, G. Strengthening the EU's Resilience in the Virtual Domain / Gonçalo Carriço // European View, 16(2). – 2017. – P. 331-335.
[3] 2014 Wales Summit will only start the process of finding NATO's new balance. (2014). European Leadership Network. URL: https://www.europeanleadershipnetwork.org/commentary/the-2014-wales-summit-will-only-start-the-process-of-finding-natos-new-balance/ (Accessed 26.03.2022).

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[1]. 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)[2].

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[3].

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.

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 3 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 3 in order to make a comparison of critical

[1] 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. URL: http://www.jstor.org/stable/resrep21140.13. (Accessed 16 May 2022).

[2] Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA. (2021). Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. URL: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a (Accessed 16 May 2022).

[3] Internet Organized Crime Threat Assessment (IOCTA). (2019). URL: https://www.europol.europa.eu/publications-events/main-reports/iocta-report (Accessed 16 May 2022).

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 2 and 3. 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[1]. Content analysis 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 B.

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 2 and 3. 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

[1] Hsieh, H. F., & Shannon, S. E. Three Approaches to Qualitative Content Analysis. Qualitative Health Research / Sarah E. Shannon, Hsiu-Fang Hsieh // Qual Health Res, 15(9). – 2005. -P.1277–1288.

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 3.

Based on the theoretical framework above, one would expect the following **hypotheses** to hold true:

1. The use of the term "cyber" in official NATO documents increased dramatically in the 2004-2018 time period.
2. The geopolitical situation in 2007-2009 as well as in 2014 is the reason for the increased presence of the term "cyber" in NATO's official documentation.
3. The EU and NATO share similar approaches when it comes to the applicability of international law in cyberspace, confidence-building measures, relations with private sector and international entities. Thus, these elements are avenues for developing a common or complementary approach to cyber defense and cybersecurity.

The structure of the thesis consists of an introduction, 3 chapters, including 9 paragraphs, a conclusion, a bibliography and 5 appendices. In Chapter 1 the author uses Critical Theory, with a sub-section of Critical Security Studies, in order to analyze cyberspace and the impact the complexities within this domain have on the pre-existing relationship between the EU and NATO. Chapter 2 is focused on is the qualitative and quantitative content analysis of the EU and NATO's approaches to cybersecurity and cyber defense. The author examines NATO Cyber Defence and EU Cybersecurity policies in order to determine two international entities' perception of the main actors, threats and risks in cyber environment, and identify advantages and limitations of the existing Cyber Policies. In Chapter 3 the author analyses the existing EU-NATO cyber cooperation in order to test the current state of progress and shortcomings in cybersecurity and defense cooperation. The author also uses data collected with qualitative and quantitative content analysis and performs a comparative analysis and determines potential perspectives for EU-NATO cyber cooperation.

Chapter I. Theoretical Framework: 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.

1.1 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, but critical theory has also 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[1].

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[2]. 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[3]. 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"[4]. 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"[5].

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

[1] Sallach, D. L. (1974). Class Domination and Ideological Hegemony. The Sociological Quarterly, 15(1), 38–50. http://www.jstor.org/stable/4105619.
[2] Herz, J. H. (1950). Idealist Internationalism and the Security Dilemma. World Politics, 2(2), 157–180. https://doi.org/10.2307/2009187.
[3] Zaslavskaya N. (2017). 'Theories of International Relations', in Russia and the World. (ed.). Lexington Books: Maryland. pp. 35-37.
[4] 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.
[5] Ibid.

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"[1]. 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

[1] 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.

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'[1].

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.

1.2 Critical theory and Security Studies

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[2].

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

[1] 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.
[2] 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.

assumptions go against human interests. Moreover, this realistic 'ideology', pretending to be a theory of knowledge, largely lacks methodology[1].

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[2].

To link Critical security studies and Arms control, we are, according to critical theory, to ask ourselves some important questions. What is the definition of this term? Where does it come from? What is it for? Why is it necessary? What is it intended to promote? And how states should do it?

With the proliferation of Information and Communication Technologies (ICTs), Internet has become one of the greatest equalizers. Interest in cybersecurity has never been greater among International Relations scholars. Nowadays the Internet provides us with the possibility to communicate with one another across the globe. It also provides with a medium for ideological, cultural, and informational exchange. Such previously unimaginable level of interconnectedness benefits not only civilians, but also businesses and governments. But that notwithstanding, for all goods, the widespread of the Internet represents series of great threats. From the financial loss of businesses through cyber threats, the leak of classified government data happed due to cyber-attacks may pose huge challenge to national and economic security of nations. The cyber and hybrid threats are increasingly seen as a strategic challenge.

In the past decade, cyber incidents as well as cyberattacks such as, for example, on Estonia in 2007, Georgia 2008, Ukraine 2014, 2015, 2021, 2022, the alleged interference in the American

[1] Wyn Jones, R. (1999). Security, strategy and critical theory. Colorado: Lynne Rienner Publications.
[2] Booth, Ken. (1991). "Security and Emancipation", Review of International Studies, Vol. 17, No. 4 (Oct., 1991), pp. 313-326.

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[1]. The aforementioned examples might serve as important cases of critical junctures with regards to cyber defence as well as cybersecurity.

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[2]. 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.

These examples serve as illustrations of critical junctures regarding NATO, the EU and the cyberdomain. The attacks on Estonia, Georgia, and Ukraine, were effectively attacks on a NATO member country, an aspiring NATO member country, and a dithering aspirant country. Conjointly, the attacks did, to varying degrees, have a confrontational impact on NATO. Therefore, it would be expected for the data analysis to show a spike in associations to "cyber"the periods of 2007-2008, and 2014 in Chapter 3.

[1] 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.

[2] Christou, G. (2016). Cybersecurity in the Global Ecosystem. In: Cybersecurity in the European Union. New Security Challenges Series. Palgrave Macmillan, London. https://doi.org/10.1057/9781137400529_3.

Chapter II. Understanding the European Union and the North Atlantic Treaty Organization's approach to cybersecurity and cyber defense

First and foremost, it has to be said that the cyber threat environment is intensifying dramatically. In the last two decades, cyber incidents, as well as cyber-attacks, 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 alleged 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[1].

This topic is of special interest inasmuch as cyber-attacks became an integral part of warfare. Since the beginning of the Special military operation in Ukraine, announced by the Russian President Vladimir Putin on the 24th of February 2022, Russia has been hacked at an unprecedented scale and become a target for cyber-terrorist like never before. The volunteer group of hackers knocks Russian websites on the daily basis and makes them inaccessible: government departments, food delivery, Russian banks, and payments services have all targeted to disrupt life in Russia. Interestingly enough, cyberwar has been declared on Russia by a hacker group 'Anonymous'[2].

Cyberspace is a new reality that is difficult to comprehend taken into account its intangible and highly technical nature. As was already discussed cyberspace is complex to understand due to 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.

According to Frédérick Douzet, Professor at the French Institute of Geopolitics at Paris 8 University and chairwoman of the Castex Chair of Cyber Strategy, there is sometimes a multi-

[1] Dunn Cavelty, M., & Wenger, A. Cyber security meets security politics: Complex technology, fragmented politics, and networked science / Myriam Dunn Cavelty, ORCID Icon, Andreas Wenger // Contemporary Security Policy. – 2019. № 41 (1). - P. 5–32.

[2] Milmo, D. (2022, February 28). Anonymous: the hacker collective that has declared cyberwar on Russia. The Guardian. URL: https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia (Accessed 13.03.2022).

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. Since it was designed with high openness, with no build-in security, data can be pulled in unencrypted through cables and routers with ease.

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 next cyber layer is cognitive and semantic. It represents the world of the users of the logical layer, the world of information, social networks, discussions and exchanges in real time. We need to highlight that this layer is the most intangible one, the most difficult to localize, 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, a state-sponsored group or an institution started.

Therefore, taking into account the multi-layered representation of cyberspace, we can state that it is both a material reality with hard assets that could be located and an intangible space of exchange that is complex to grasp. It can refer to a set of computer networks (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. As the author previously highlighted 5 billion people around the world use the internet today – equivalent to 63 percent of the world's total population[1]. Moreover, depending on who uses the Internet and why, the term cyberspace can refer to a totally

[1] Digital Around the World. (2022, May). DataReportal – Global Digital Insights. URL: https://datareportal.com/global-digital-overview#:%7E:text=A%20total%20of%205%20billion,12%20months%20to%20April%202022 (Accessed 13.05.2022).

different reality or imagination in a certain conceptual blur.

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[1].

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[2]. 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.

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[3].

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 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. The EU Member States also had to face the

[1] Douzet, F. La géopolitique pour comprendre le cyberespace / Frédérick Douzet // Hérodote. – 2014. №. 152-153. – P. 3-12.
[2] Ibid. – P.13-15.
[3] Christou, G. Cybersecurity in the Global Ecosystem / George Christou // Cybersecurity in the European Union. New Security Challenges Series. Palgrave Macmillan, London. – 2016. № 18. – P.2016.

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 than 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 allegedly Russian and its proxies.

On April 27, 2007, the first cyber-attack targeting a European 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, wishing 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 demonstrated Estonia's rapprochement with the Western powers and its readiness to give up its Soviet past. The response did not wait. Russia would have temporarily hired the services of botnet owners, and 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) attack is 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[1].

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[2].

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

[1] Nazario, J. DDoS attack evolution / JoseNazario // Network Security. – 2008. № 7. – P. 7–10.
[2] Thomson, I., & Thomson, I. (2007, June 1). Russia “hired botnets” for Estonia cyber-war. iTnews. URL: https://www.itnews.com.au/news/russia-hired-botnets-for-estonia-cyber-war-82600 (Accessed 13.02.2022).

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 Russian Federation gave its consent to this action[1].

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[2]. Anyone can be a cyberwarrior. With little means, a lot 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"[3]. According to the Russians, it is the

[1]1.Eriksson J, Giacomello G. The Information Revolution, Security, and International Relations: (IR)relevant Theory? / Johan Eriksson, Giampiero Giacomello // International Political Science Review. – 2006. № 27(3). – P. 221-244.

[2] Joubert, V. & Samaan, J. L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE / Vincent Joubert, Jean-Loup Samaan // Hérodote. – 2014. № 152-153. – P. 261-275.

[3] Comprehensive study on cybercrime. - February 2013 / UNODC. Imprint New York: United Nations, 2013. – P. 115-

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 and not by the Russian state[1].

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

118.

[1] PROPOSITION DE RÉSOLUTION sur l'Estonie. (2007). Union européenne, 2007 - Source : Parlement européen. URL : https://www.europarl.europa.eu/doceo/document/B-6-2007-0220_FR.html (Accessed 23.04.2022)

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 were 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[1]. 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

[1] Vosoughi, S., Roy, D., Aral, S. The spread of true and false news online / Soroush Vosoughi, Deb Royand, Sinan Aral // Science (New York, N.Y.). – 2018. №59. P.1146–1151.

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"[1].

Thus, fake news as well as state-sponsored disinformation campaigns are especially problematic and dangerous for democratic systems. Therefore, it has to be stated that free mass media is the main responsible actor in democratic countries in denying false information and combatting disinformation campaigns. But not only free media has this responsibility to combat false information; citizens, national authorities and especially international organizations share this responsibility. There is a growing debate on how to face and address these issues. Dame Adjin-Tettey puts in that there are several ways on how to combat fake news. In his research paper researcher investigates the effect of media and so-called information literacy on the ability to approach state-sponsored sophisticated disinformation campaigns and fake news[2]. According to the researcher, national authorities are to raise public awareness of the risks linked to the use of Internet and must cooperate in international bodies with other member states to address these challenges. Additionally, citizens must have a critical attitude and approach towards what they listen and read on Internet, especially if the sources are of nebulous origins.

Having analyzed the most significant and prominent cyber-attacks on the EU and NATO we have identified risks associated with cyber-attacks. The example of the cyberattack on Estonia demonstrates that cyber-attacks can cause electrical blackouts, failure of military equipment, and breaches of national security secrets. For the first time declared war on the Russian Federation in cyberspace demonstrated that cyber-attacks could result in the theft of valuable, sensitive data like medical records.

---

[1] Thomas, E., Thompson, N., & Wanless, A. (2020, June 10. The Challenges of Countering Influence Operations. Carnegie Endowment for International Peace. URL: https://carnegieendowment.org/2020/06/10/challenges-of-countering-influence-operations-pub-82031 (Accessed 24.04.2022)

[2] Dame Adjin-Tettey, T. Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education / Theodora Dame Adjin-Tettey // Cogent Arts & Humanities. – 2021. - № 9(1). URL: https://doi.org/10.1080/23311983.2022.2037229 (Accessed 25.04.2022)

Cyberattacks 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, which has been analyzed in Chapter 2 and 3 of this Master Thesis.

2.1 NATO Cyber Defense Policy: actors, threats and risks perception

It needs to be stated that cybersecurity at NATO has several quite unique features that make this topic relevant for master thesis. First of all, it is an interesting topic inasmuch as until very now, scholars have extensively studied the North Atlantic Treaty Organization in terms of its deterrence doctrine, its campaigns in Yugoslavia and Libya, its enlargement, and other topics. 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 Coker and Pomarède as well as the other very prominent researchers[1]. 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

[1] Coker, C. (2013). Why NATO Should Return Home The Case for a Twenty-First Century Alliance. The RUSI Journal, 158(4), 122–138; Pomarède, J. (2014). L'(in)sécurisation par les technologies militaires et la mise en sens de la violence : Le cas de l'intervention militaire de l'OTAN au-dessus de la Libye (2011). Cultures & Conflits. – 2014. № 93. -P. 125-145.

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"[1]. 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, it needs to be said that cyberspace is composed of several layers: the physical layer encompasses all physical infrastructure, such as computers, commutators, 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"[2]. 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". We want to effectively demonstrate that cyberspace has been militarized to be an integral part of that sovereignty, but at the same time cybersecurity is by no means an integral part of national defense.

[1] Desforges, Alix. Les représentations du cyberespace : un outil géopolitique / Alix Desforges // Hérodote. – 2014. vol. 152-153, no. 1-2. - P. 67-81.

[2] Masoumifar, A. Cyberspace Sovereignty: Is Territorializing Cyberspace Opposed to Having a Globally Compatible Internet? / Ali M. Masoumifar // Journal of Cyberspace Studies. – 2022. № 6(1). – P. 1-20. URL: doi: 10.22059/jcss.2022.327215.1064 (Accessed 27.04.2022).

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:

Insiders. According to the researcher those are the individuals who have access to documents or procedures. According to Denning, this accounts for 80% of cybersecurity incidents.

The next category stands for hackers. Hackers are the individuals who try to break into or gain access to systems, with no given access or permission, as opposed to insiders.

The third category is composed of the spies. The main goal of spies, according to Denning is to steal data while remaining invisible for knowledge or resource owners.

The aforementioned researcher then overviews criminals who act with the main purpose of obtaining money. It is usually achieved by ransom, selling information or stealing credit card data at different websites or using other illicit means.

Terrorists constitute the fifth category. Normally terrorists 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 and to recruit.

The last category, number six, which the researcher identifies, includes nation-states, which are the ones to be most wary of, since some of them, about twenty, including Russia, China and North Korea, have significant cyberwarfare capabilities[1].

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)[2]. 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 if not practically

[1] 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 (Accessed 27.04.2022).
[2] Hunker, Jeffrey. Cyber war and cyber power Issues for NATO doctrine / Hunker, Jeffrey // Semantic Scholar. – 2010. – №3. – P. 158.

impossible 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"[1]. 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"[2]. 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.

Thus, the question the author raises is 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.

[1] Annual Commission Report 2011 - Information and National Security, (2011). https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120125_Annual_Report_2011_en.pdf
[2] Risk and the War on Terror / Louise Amoore, Marieke de Goede [et al.] – London: Routledge, 2008. – P. 156.

2.2 Strengths and Weaknesses of NATO's Cyberdefense Posture

The North Atlantic Treaty Organization should be seen as a defense provider insofar as NATO's cyberpolicy aims to defend and protect its Member States as well as their networks and all other layers which could be potentially targeted. The notion of deterrence remains fundamental in NATO's cyber strategy and is in line with the Alliance's collective defense policies. Vincent Joubert, a research fellow at the Foundation for Strategic Research (FRS), in an Alliance research note, indicates that the need to develop "a robust defense system with improved security standards, focusing on prevention, resilience and non-redundancy"[1]. 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. Author stress upon the role of the United States in this process of deterrence. The role of the States is truly explicit. The US national security reports texts state that any form of hostile act in cyberspace could lead to collective retaliation, under Articles 4 and 5 of the NATO Treaty.

One may notice an ambiguity in NATO's strategy: the role of the US as security provider and the NATO's purely defensive direction. We tend to believe that this is done deliberately 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.

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"[2]. 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

[1] Five years after Estonia's cyber-attacks: lessons learned for NATO? (2012). Research Division - NATO Defense College, Rome.

[2] 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.

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.[1]

One of the main characteristics of cyberspace is the great difficulty of identifying the enemy, providing evidence of an attack or interference in, for instance, allegedly Russian interference in the 2016 US presidential election. This is what significantly complicates the legal basis for a reasoned collective response.

Thus, we might conclude that, knowing whether an attack was carried out by an activist group, specific individual, hacker group, terrorist organization or a state entity requires significant means of analysis, and there is a margin of error that results in devastating inaccuracy. This is of special importance because false-flag attack capabilities can be much easier to achieve in cyberspace compared to other fields.

It should be also stated that the precise rout and origin of a specific attack is highly difficult to determine, on the one hand, because "the international implications of botnets (denial-of-service attack networks) are such that any comparison of actions in cyberspace is quickly subjected to methodological limitations. On the other hand, if it turns out that most attacks are localized to a particular country, the exact assignment of the person responsible and/or the sponsor of the attack is not known and is not obvious. Indeed, it is difficult to have absolute success in "proving formal links between a state resident and a state agency in the case of cyberattacks." This complicates the application of the 5th Article of the Washington treaty, and represents a major weakness of NATO.

Nevertheless, the organization we are studying, NATO, has made promising progress, which will be analyzed. The first NATO's cyber defense concept had been approved at The Bucharest Summit in early 2008. Author would like to emphasis the crucial role of a cyber-attack on Estonia in 2007 for this to happen. This was one of the immediate consequences and the Alliance's most noticeable response to the attack on Estonia. The Cooperative Cyber Defense Centre of Excellence (CCD COE) was created 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

[1] Lucas Kello, Cyber legalism: why it fails and what to do about it / Lucas Kello // Journal of Cybersecurity. – 2021. - Volume 7, Issue 1.

2014. Today, the center has 18 members as well as 3 Alliance partners[1].

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 this international entity. 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[2].

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[3]. 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

[1] 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.

[2] Wales Summit Declaration. (2014). NATO. https://www.nato.int/cps/en/natohq/official_texts_112964.htm (Accessed 17.11.2021).

[3] M. Storm Jensen. Five good reasons for NATO's pragmatic approach to offensive cyberspace operations / Mikkel Storm Jensen // Defence Studies. – 2022. URL: DOI: 10.1080/14702436.2022.2080661 (Accessed 02.05.2022).

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.

We would emphasize the importance of determining the threshold beyond which a malicious action could be turned into a military conflict. Taking into account that for now it is not quite defined how, and by using which means the North Atlantic Treaty Organization could respond to a proven state-sponsored attack, it is crucial to determine the route map. In this sense, the goal of the NATO Member States is to develop as wide a range of response measures as possible so that they can develop measures to counter any attacks against them in accordance with international law and the principles of restraint and proportionality and thereby deter further cyber-malicious actions.

With NATO’s cyber capabilities been tested and analyzed, we can state that today it has strong capabilities to withstand cyber-attacks against it. The Organization continuously improves its capacities in cyber space which can be justified by more aggressive attacks taking place in cyber. The construction of strong and prominent cyber defense policy should go on which would enable NATO to defend itself and deter aggression against its Members’ networks.

In conclusion, author would like to emphasize that 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. However, we believe that these obstacles will be overcome very soon as we noted earlier, external threats and challenges strengthen NATO and consolidate its members.

2.3 EU Cyber Security Policy

In the past decades, the European Union has developed an increasingly broad, multi-sectoral set of foreign and cybersecurity policy instruments. All of these multi-sectoral cybersecurity instruments can have implications for supporting the EU's efforts to resolve crises and conflict management effort. Cybersecurity is certainly the EU's most salient problem on the political agenda. This statement can be proven by the fact that cybersecurity is a priority also reflected in the EU's next long-term budget (2021-2027). Thus, the purpose of this Subchapter is to examine the EU Cyber Security Policy, its cyber industry, defense capacities, and cyber research and infrastructure.

Mr. Juhan, Director of The European Union Agency for Cybersecurity (ENISA), states that " Cyber crises know no borders"[1]. 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 applied by every EU Member State in cyber defense. But beyond its advisory role, it is not able to act in the field in direct support of potential attacks.

[1] The 9th Annual European Cyber Security Conference. (2022, March 31). EU Cyber Security 2021. URL: https://eucybersecurity.com/ (Accessed 05.03.2022).

Since the EU does not have a common army, 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). Author would lie to emphasize the cyber security policy of Estonia. As it was discussed earlier, Estonia was the first EU state to be attacked in cyberspace. Estonia has been at the forefront of cybersecurity internationally. The NATO Cooperative Cyber Defense Centre of Excellence (CCD CoE) and the EU Agency for large-scale IT systems (EU-LISA) are both based in Tallinn[1].

The fact that cyber defense is still entirely a matter of national within the European Union represents a risk insofar as large-scale cyberattacks would potentially affect 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 subchapter we 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? To answer these questions, author needs to analyze the legal ground of EU competence in cybersecurity regulation.

As it was discussed above, the Union is not responsible for cyber policy of its nation states. 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, which was highlighted before several times. Author pays special attention to Estonia since this country played a key role in the EU-NATO cyber policy design[2].

It has to be noted that some countries in Central Europe have a different approach. Andrea Simandi puts in that "Every CEE country thinks that they are very special and very different, but once you engage in deeper conversations to understand their concrete requirements and concerns, they are not that different…but for all cyber threats are for real and require promising measures to face with". Thus, 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

[1] ŠTrucl, D. (2021). Tallinn 2021 Comparative study on the cyber defence of NATO Member States. NATO CCDCOE. https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf.

[2] How Estonia became a global heavyweight in cyber security. Invest in Estonia (February 11, 2022). URL: https://investinestonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/ (Accessed 04.02.2022).

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[1]. 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[2].

In recent years, the European Union 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 believed that EU Member States have difficulties in achieving consistency in cyberspace and more precisely in cybersecurity due to varying from country to country understanding of cybersecurity, its actors, threats, risks linked to this topic and its scope. Cyber perception varies and depends on the addressee, the context and the area of knowledge in which they are used. In the field of cybersecurity in the Union, discussions may include various aspects such as cyber resilience, cybercrime, cyber defense, cybersecurity 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, and electronic communications, which encompass issues of privacy and data protection. The

[1] The Cybersecurity Challenge in Central and Eastern Europe. (2018). CMS. URL: https://cms.law/en/media/local/cms-cmno/files/publications/publications/the-cybersecurity-challenge-and-central-and-eastern-europe (Accessed 04.02.2022).

[2] European Court of Auditors. (2019). Challenges to effective EU cybersecurity policy. URL: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf (Accessed 02.05.2022).

conceptualization of cybersecurity is becoming increasingly complex as the boundaries between the different domains of cybersecurity become blurred.

Author stresses upon the advantages and disadvantages of cybersecurity meanings within the European Union. The term has the flexibility to adapt in 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[1]. 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

[1] REPORT on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, Directive (EU) 2016/1148 (COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)). (2021). https://www.europarl.europa.eu/doceo/document/A-9-2021-0313_EN.html (Accessed 05.05.2922).

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 (DG) (e.g., DG CONNECT, DG Mobility and Transport, and DG Joint Research Centre)[1]. 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.

[1] Cybersécurité européenne : comment construire une société numérique plus sûre ? (2019). Corporate. URL: https://www.orange.com/fr/cybersecurite/cybersecurite-europeenne-comment-construire-une-societe-numerique-plus-sure (Accessed 04.04.2022).

It is worth noting that the 2013, 2017 and 2020 EU Cyber Security Strategies call for a more structured and comprehensive approach to cyber security protection. This also applies to national approaches to cyber security. According to the EU Cybersecurity Strategy, cooperation mechanisms within the EU must be improved. There is an acute shortage of personnel or an inability to fully exploit the potential for effectiveness, which is due to the difficulty of involving all necessary actors. The European Data Protection Committee or the Body of European Regulators for Electronic Communications (BEREC) is an effective instrument but faces similar problems. A further obstacle is the lack of effective communication in the regulatory authorities. For example, the exchange of expertise and information between CERTs and police agencies at the national level can still be improved. However, when addressing this issue, member states should be encouraged to establish more consistent rules and mechanisms for information sharing in accordance with EU values and citizens' fundamental rights. Although most member states developed their first cybersecurity strategies before the NIS Directive, it may be useful to define a governance structure at the national level in advance, defining the roles and responsibilities of both public and private sector stakeholders. When considering the changes necessary to facilitate effective cybersecurity cooperation, the highest standards of rule of law and protection of fundamental rights must be upheld. This is especially important in the area of law enforcement and criminal procedure, where a delicate balance must be struck between the interests of states, societies and individuals. Policymakers therefore need to develop a clear understanding of the limits of cybersecurity cooperation imposed by principles of justice and the rule of law and strive to ensure consistency between different legislative frameworks.

2.4 The EU as a Coherent Cybersecurity Actor

Back in 2007, during the cyber-attacks on Estonia, The European Union Agency for Cybersecurity (ENISA), which currently actively contributes to the EU cyber policy, did not have the competences to act on the ground. In general, following this attack, the European Union did not really have any tangible action to protect its members, and relied on the active and efficient actions of NATO in this matter. It has to be stated that NATO did not have many capacities to face cyber-attacks as well as cyber incidents.

In this Subchapter author examines the European Union as a cybersecurity actor. It has to be noted that a coherent common European cyber defense policy firstly appeared back in 2016 with adoption of the Network and Information Systems Security (NIS) directive. This is the first

legislative framework to be agreed upon throughout the European Union. This framework, transposed in 2018, establishes an audit obligation for companies, incident notifications and elaborates security measures for companies. The objective of NIS is the cyber defense of the Union as a first protection of the whole territory against cyber incidents such as malicious viruses sent from foreign states that could potentially steal information or resources such as capital from companies in the EU. The NIS Directive defines that Is the European approach to Critical infrastructure. Critical infrastructure, following the NIS, includes not only digital environment including digital financial services, but also operational environments which, in its turn, include energy distribution, electricity generators as well as water supply. This directive is the starting point of a reinforced collaboration between EU Member States and voted unanimously. The unanimous adoption of this Directive in 2018 demonstrates the beginning of the common coherent awareness. Nevertheless, this awareness does not mean total agreement. The disagreement between the different countries (especially dissention between Central European Countries and Western Europeans), as explained in Subchapter 2.3 EU Cyber Security Policy, prevented the implementation of an effective and binding policy, with a definite effect on European defense.

Interestingly enough one year after the Network and Information Systems Security (NIS) directive adoption in the European Union, two major cyber incidents (computer worms such as Notpetya and Wannacry) hit the world. The NIS Directive's adoption is supposed to prevent those two computer viruses from entering the EU cyberspace. According to Directive on security of network and information systems (NIS Directive), the Council of Europe imposed sanctions on six individuals and three organizations. Russian, Chinese and North Korean residents, upon which he sanctions have been imposed, were restricted from entering the EU. Sanctions also includes asset freeze[1].

Notpetya and Wannacry have caused billions of dollars in damage and are considered the largest cyberattacks in history. But that notwithstanding, there are more destructive and dangerous incidents which may occur in cyberspace. For instance, 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 interference into a country's cyber space.

Similarly to NATO's cyber defense evolvement in response to growing cyber activities within

[1] Anna Zygierewicz. (2020, November). Directive on security of network and information systems (NIS Directive). European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/654198/EPRS_BRI(2020)654198_EN.pdf (Accessed 07.05.2022).

this domain, the EU's cyber security policy became more coherent due to the external threats. Thus, the European summit's objective in Tallinn on September 19, 2017 was to elaborate a policy which would enable it to act in a more coordinated way. On of the main result of this Summit was that the European Parliament's recommendation was taken into account and since 2017 Europol can 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, 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[1]. The Memorandum of Understanding, signed in 4th of March in Croatia, legally enables counter cyber operations across jurisdictions of Lithuania, Estonia, Croatia, Romania, Spain and the Netherlands. It forms so-called Cyber Rapid Response Team (CRRT). Memorandum of Understanding also defines legal status, procedures and mechanisms of CRRT operations. CRRT is formed by military experts and civilians. The main goal of Cyber Rapid Response Team is to neutralize harmful cyber incidents through internet or physically[2].

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).

[1] Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT) | PESCO. (2018). Permanent Structured Cooperation (PESCO). URL: https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/ (Accessed 07.04.2022).

[2] Kristi Raik. Not Yet Fit for the World: Piecemeal Buildup of EU Military, Cyber and Intelligence Assets / Kristi Raik // European Union. URL: https://www.iai.it/sites/default/files/joint_rp_4.pdf (Accessed 07.04.2022).

Finally, ENISA sets 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 EU Member States. This is a successful direction for further strengthening the EU's cybersecurity policy inasmuch as The Cyber Crises Liaison Organization Network (CyCLONe) was launched during Blue OLEx 2020. CyCLONe is a cooperation network for EU Member States' national authorities in charge of cyber crisis management to collaborate and develop timely information sharing and situational awareness based on tools and support provided by ENISA, which serves as the CyCLONe Secretariat[1].

Having analyzed cybersecurity capacities of the European Union, author raises the following question: "Is it possible for the EU to be autonomous?". There are several obstacles for this kind of "independence".

The first well-known obstacle for the Union to be autonomous if cybersecurity lies in reluctance of countries to share information and sovereignty prerogatives, particularly concerning defense. To prove this statement author appeals to the example of The European Defense Community which is one of biggest failures of the Union. The European Defense Community provided for 14 French divisions, West Germany and Italy were to contribute 12 each, and the Benelux countries were to contribute five divisions together. Articles 2 and 5 of the Paris Treaty stipulated that the grouping to be created would operate "within the framework of NATO and in close cooperation with it". At the same time, the Paris Treaty envisaged the creation of common military units and a common military budget. Thus, the establishment of the European Defense Community (EDC) was designed to minimize the threat of war between European countries.

The Pleven plan was never implemented: the attempt to create the EDF was in sharp contradiction to the decisions of the 1945 Crimean and Potsdam Conferences, which prohibited the rebuilding of the German national army. Despite all the contradictions regarding the EOC, on May 27, 1952, the foreign ministers of six European states (France, West Germany, the Benelux countries, and Italy) signed the Treaty of Paris, providing for the creation of a European defense community. This treaty was ratified by the West German Bundestag and the national parliaments of the Benelux countries, but the French National Assembly rejected the initiative. Thus, the development of politico-military integration in the 1950s was complicated by the fear of a German

[1] EU runs exercise to test response to large cyber incidents. (2021). Portal Publishing Ltd. URL: https://www.continuitycentral.com/index.php/news/technology/6737-eu-runs-exercise-to-test-response-to-large-cyber-incidents (Accessed 08.04.2022).

resurgence[1]. There are other failures of the European defense initiatives.

The second obstacle lies within NATO's cyber cooperation. It is well known that some EU Member States such as CEE countries relies mostly on NATO. 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 obstacles should not make us downplay the role of the Union in comparison to NATO, or even perceive it as non-important and non-essential organization when it comes to cybersecurity.

In conclusion, the central aim of this Chapter was to analyze and provide a deeper understanding of the European Union and the North Atlantic Treaty Organization's evolving ecosystem for cybersecurity. In the past decades, the European Union has developed an increasingly broad, multi-sectoral set of foreign and cybersecurity policy instruments. All of these multi-sectoral cybersecurity instruments can have implications for supporting the EU's efforts to resolve crises and conflict management effort. Its adaptive and flexible type of resilience drives the EU's approach to cybersecurity. Thus, the EU's role in cyber cannot be downplayed: the advances are present, they are multiple and sometimes confused but in a certain direction of strengthening the European cyber power. As for NATO' inclusion of "cyber" in its collective defense strategy, it is directly connected with the number of references of "cyber" it uses in its legal documentation. Content analysis demonstrates that cyber attacks such as on Georgia, Ukraine and Estonia were the biggest catalysis for "cyber" to become one of the operational domains to the three traditional ones. A significant increase of the use of the "cyber" terms demonstrates its growing significance within NATO. However, despite the consensus in NATO about the importance of cyberdefense, two blocs seem to emerge in the goals to be achieved by NATO. Indeed, the global defense of NATO networks is a goal shared by all members. But while the Baltic, Central and Eastern European states would like to see an expanded global role for NATO, military powers such as France and Britain refuse to give NATO too active a role in defending their networks, in the name of sovereignty and for fear of the potential erosion of their national independence. In a system based on a common solution involving all member states, the ability to find political consensus remains highly problematic and unclear.

[1] Shidukov A. Evropeiskii soiuz problemy i perspektivy [European Union: Problems and Prospects]. Bachelor thesis, Pyatigorsk University, Pyatigorsk, 2020.

Chapter III. NATO-EU cooperation in cybersecurity and cyber defense

3.1 EU-NATO Cooperation and Strategic Autonomy

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 international entities. 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. The author begins with the analysis of NATO as an international entity.

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 these Soviet military activities, the European allies with the United States and Canada began negotiations which later led to the creation of organizations for military cooperation[1].

Political and military events which took place between 1947 and 1949 accelerated the formation of the military organization. It has to be stated that such unprecedented events as military coup in Czechoslovakia in 1948, the blockage of Berlin in 1949, sovereignty threats to Greece and Norway are one of the crucial ones. 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.

NATO parties agreed to consider an armed attack on one of them, in Europe or North America,

[1] Henrikso, A. The Creation of The North Atlantic Alliance 1948–1952 / Allan K. Henrikson // U.S. Naval War College Press. – 1980. № 33(4). – P. 4–17.

as an attack on all of them., which was stated in Article 5 of Washington Treaty. 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 Organization 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 were 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 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.

As for the European Union (EU), it 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.

The modern European Union is a complex structural formation encompassing two European communities and two spheres of activity - common foreign and security policy, and common internal affairs and justice policy. At the same time, the Union as a whole is a single organization. Its

organizational unity is ensured both by the single composition of its member states and by the single system of governing institutions and bodies[1].

We need to start off our analysis 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[2].

When it comes to the political field of EU-NATO cooperation, we need to keep in mind that namely four crucial political events 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.

Thus, a joint EU-NATO declaration was adopted in 2002. This declaration paves the way for closer political and military cooperation between the two international organizations. 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. The European Security and Defense Policy (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

[1] 1. Shidukov A. Evropeiskii soiuz problemy i perspektivy [European Union: Problems and Prospects]. Bachelor thesis, Pyatigorsk University, Pyatigorsk, 2020.
[2] Howorth, J. NATO and ESDP: Institutional Complexities and Political Realities / Jolyon Howorth // Politique étrangère. – 2009. – P. 95-106.

in peacekeeping. France made the European Security and Defense Policy a priority of its Presidency in the second quarter of 2008, submitting to its European partners a comprehensive program 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 defense capabilities, recognition of the strategic and economic need to restructure the defense 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 threats. In the framework of its security and defense 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 organized 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 defense 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 organization with logistical and material support from the other. Thus, within the framework of the European Security and Defense 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[1].

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 were 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 contributed to the spread 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 Defense 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

[1] Christou, G. Conclusions: Towards Effective Security as Resilience in the European Union? / George Christou // Cybersecurity in the European Union. New Security Challenges Series. Palgrave Macmillan, London. – 2016. № 105. – P. 171-189.

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[1].

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, "in his view, European security cannot be conceived without the North Atlantic Treaty Organization (NATO)"[2]. Despite the political will of the Heads of State and Government to emancipate Europe from American patronage in security and defense matters, it is clear that the European Union remains heavily dependent on NATO in defense and security matters. As a result, European security policy and European defense identity are in contrast in the cooperation between the two institutions.

However, over the years, the European Union elaborated a policy in the way so it could take charge of its own defense policy, notably through the "Berlin Plus" agreements which allow the European Union to use NATO assets and capabilities for operations without the participation of United States. Moreover, the "Berlin Plus" agreements establish 'NATO-EY Capability Group', sets procedures for monitoring, return and release of NATO assets, and finally establishes NATO-EU consultation arrangements in the context of EU-led operations making use of NATO assets and capabilities[3].

Author aims to emphasize a special role that France plays in security and defense within NATO which proves the existence of difference points of view and conflicts of interests within NATO. It is very interesting case inasmuch as France once withdrawn from the North Atlantic Treaty Organization (NATO) in 1966 due to political and military reasons. It is believed that Special military operation launched by the Russian President Vladimir Putin on 24th of February united NATO as never before. But the talks bout the NATO's unnecessarily for the European Union and inability to adapt to modern conditions are still there. It is worth mentioning the recent statement of the French far-right former presidential candidate Marine Le Pen. On April 13, 2022 Le Pen called for a closer cooperation and ties with the Russian Federation[4].

[1] Resolution 1160 of 1998, imposes an arms embargo on the former Yugoslavia Resolution 1190 of 1998, requires the withdrawal of troops from Kosovo

[2] Charles Goerens, former President of the Western European Union

[3] Varwick, J. (2019). The European Union and NATO: Partnership or Rivalry? Worldsecuritynetwork. URL: https://www.worldsecuritynetwork.com/Other/Varwick-Prof.-Dr.-Johannes/The-European-Union-and-NATO-Partnership-or-Rivalry (Accessed 13.05.2022).

[4] Le Pen wants France out of NATO integrated command, backs NATO-Russia links (2022). France 24. URL: https://www.france24.com/en/france/20220413-le-pen-wants-france-out-of-nato-integrated-command-backs-nato-

In conclusion, author notes the complexity of the formation of the European Union as an independent actor in international relations in security, defense and crisis management. It is so not only to historical past of the EU and many failures in experienced in the field if defense and security over the years. Ending dependence from the United States would ultimately mean for the European Union aggravated competition with NATO. That means, EU's takeover could potentially lead to the independent approach towards resolving its own reginal problems and deprive the North Atlantic Treaty Organization from 'reason d'être'. Nowadays, this scenario is practically impossible. Thus, in today's increasingly unstable geopolitical context, cooperation between two international entities is essential. NATO-EU are interconnected and not only they are united by 21 EU Member States which are currently the NATO Members, but also together EU and NATO have more possibilities to mobilize their assets and tools to enhance the security in Europe. Please see Appendix E for more information.

3.2 EU–NATO Cybersecurity and Cyber Defense Cooperation

Europe has a very particular institutional landscape in terms of collective security and defense. 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[1]. 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 inasmuch as cyber threats are reterritorialized, nebulous, opaque, relatively instantaneous and difficult to attribute, and thus, the integration of an inter-state cooperation or alliance can be particularly relevant to consolidate power relations.

russia-links (Accessed 13.05.2022).

[1] The Balance of Power and Future Peace In: The Idea of Europe: Enlightenment Perspectives. Cambridge: Open Book Publishers, 2017. – P.122-124.

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 E for more information). 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[1]. 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 Arrangement on Cyber Defense was signed between the NATO

[1] Joubert, Vincent, Jean-Loup Samaan. L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE / Joubert, Vincent, Jean-Loup Samaan // Hérodote. – 2014. № 1-2. P.261-275.

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 Cyber Defense indeed creates legal basis to facilitate information-sharing to improve cyber incident prevention, detection and response together at the European Union and NATO. NATO Secretary-General Jens Stoltenberg called this agreement "a concrete example of the two Brussels-based organizations joining forces to counter modern forms of hybrid warfare"[1].

We need to highlight that the most prominent steps towards cyber cooperation were made with the help of two signed Joint Declaration, 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).

On 10 July 2018, the President of the European Council and the President of the European Commission, together with the Secretary General of the North Atlantic Treaty Organization signed a second Joint Declaration in Brussels. Thus, nowadays cooperation between the Union and NATO in cyberspace includes information sharing, coordinated planning and concrete cooperation in the areas of hybrid threats, operational cooperation, cybersecurity, capacity-building, defense capacities, industry and research. More detailed and visualized information can be found in Appendix C. The EU-NATO cooperation is based on openness, transparency and inclusiveness.

To conclude, the European Union as well as the North Atlantic Treaty Organization should together continue elaborating long-term strategies to defend their cyberspace and prevent disruptive actions in cyberspace. Nowadays there are already, as Jens Stoltenberg puts in, concrete examples of the two Brussels-based organizations joining forces to counter modern forms of hybrid warfare. Joint actions and enhanced cooperation are beneficial for both international entities. It will strengthen not only their cooperation but also solidarity withing NATO and the EU.

[1] Staff, S. X. (2016, February 10). NATO, EU sign agreement on cyberdefense cooperation. Phys.Org. URL: https://phys.org/news/2016-02-nato-eu-agreement-cyberdefense-cooperation.html (Accessed 23.04.2022).

3.3 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 analysis 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 mutual assistance clause. The States Parties undertake above all to take all necessary measures to prevent and combat aggression[1].

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

[1] B. Tertrais. Article 5 of the Washington Treaty: Its Origins, Meaning and Future / B. Tertrais // Research Division, NATO Defense College. – 2016. – P.12.

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 2, rigorously proves the Hypothesis 1 and 2. Please see Appendix A for more detailed information.

Content analysis 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)[1].

[1] 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.

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 B.

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"[1].

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[2]. 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"[3]. It is interesting to note, however, that the

[1] 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). URL: https://www.europarl.europa.eu/doceo/document/TA-7-2013-0376_EN.html (Accessed 25.04.2022).

[2] 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.

[3] Reflection paper on the future of European defence. (2017). URL: https://ec.europa.eu/info/publications/reflection-paper-future-european-defence_en (Accessed 25.04.2022).

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, author is 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:

First, 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 insecurity.

Second, the NATO Communications and Information Agency (NCIA) supports NATO operations, connects information and communications systems, and defends NATO networks.

Then, 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[1].

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

[1] Cyberdéfense de l'OTAN. (2018). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/20180213_1802-factsheet-cyber-defence-fr.pdf (Accessed 26.04.2022).

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 European Union Intelligence and Situation Centre 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.

Second important institution is ENISA, Heraklion, Greece, is the European Network and Information Security Agency. It provides recommendations and supports the development and implementation of cyber policies.

Finally, 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. Please see Appendix D for a more detailed information,

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 NATO 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[1]. 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[2]. Thus, beyond the EDA, European research and development programs 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"[3].

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

[1] 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. - 2018.

[2] 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.

[3] Joint Communication to The European Parliament and The Council. (2019). URL: https://data.consilium.europa.eu/doc/document/ST-12211-2017-INIT/en/pdf (Accessed 27.04.2022).

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.

Next, 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.

There is also 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. Please see Appendix E for more details.

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[1]. 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"[2]. 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

[1] . Van der Meer, (2017). EU Creates a Diplomatic Toolbox to Deter Cyberattacks. Council of Foreign Affairs. URL: https://www.cfr.org/blog/eu-creates-diplomatic-toolbox-deter-cyberattacks (Accessed 28.04.2022).
[2] Consolidated text: Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02019D0797-20210519 (Accessed 28.04.2022).

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.

Thus, having analyzed and compared most critical fields of cyber defense at NATO and the EU, author defines possible articulation of the NATO and EU means. The analysis of the competences and means of the EU and NATO demonstrates a 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, as has been discussed in Chapter 3, is gradually gaining solid ground. The objective is therefore to seek complementarity or at least closer coordination between the two international entities which 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 organizations. For example, in the event of a large-scale cyberattack on the Member State of NATO or the EU, 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.

However, this coordination remains limited. As J. Joubert and J.-L. Samaan have puts in, “it is difficult to identify the elements of complementarity or subsidiarity between the two”[1]. 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[2]. 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,

[1] J. Joubert & J.-L. Samaan. L’intergouvernementalité dans le cyberespace : étude comparée des initiatives de l’OTAN et de l’UE / Vincent Joubert, Jean-Loup Samaan // Hérodote. – 2014. №152-153. – P. 261-263.

[2] Fiott, D. (2017). The cybridisation of EU defence. Issue Alert, 24. URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert%2024%20Cybridisation%20of%20defence.pdf (Accessed 28.04.2022).

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 for which unanimity is the rule[1].

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.

That notwithstanding, the European Union and NATO have more in common than capacity building and operational exercises. The EU and NATO share similar approaches when it comes to the applicability of international law in cyberspace, confidence-building measures, relations with private sector and international entities. Thus, these elements are potential avenues for developing a common or complementary approach to cyber defense and cybersecurity.

First, cyber defense and cyber security in Europe must be built on cooperation and information sharing. This, in turn, will reduce emerging conflicts. To achieve this goal, confidence-building measures should be implemented. It is worth mentioning that they are one of the most effective tools for achieving the above-mentioned goal. It is known that cyberspace is an extremely obscure and opaque environment, which makes Confidence-Building Measures especially relevant in this space. The Organization for Security and Cooperation in Europe (OSCE), for example, in its Decision No. 1202 (2016), developed a detailed system of confidence-building measures (CBMs) aimed at reducing interstate conflicts arising from the use of information and communication technologies (ICTs). The use of the tools and specific CBMs outlined in Decision No. 1202 (2016) would be particularly useful for the two actors in International Relations. It is worth noting that the confidence-building measures developed in detail by the OSCE could be used in the future not only within the EU-NATO framework, but also with other European regional organizations that could potentially contribute to strengthening European cyber security.

[1] 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). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12008M042 (Accessed 28.04.2022).

Further, it is worth noting that maintaining close ties with the private sector is an integral part of achieving cybersecurity. This is primarily due to the fact that private entities own and operate a large number of networks. In fact, it is difficult to imagine a cyber defense that ignores the synergy of private sector, civilian, government and military capabilities. As noted earlier, the European Union adopted The Directive on security of network and information systems (the NIS Directive), which provides legal measures to boost the overall level of cybersecurity in the EU by ensuring: Member States' preparedness, by requiring them to be appropriately equipped. The next document which linked the EU with the private sector and industry is the 2019 EU Cybersecurity Act. EU Cybersecurity Act equipped Europe with a framework of cybersecurity certification of products, services and processes[1]. Thus, the European Union and the private sector are already interconnected on cybersecurity issues. Complementarity between NATO and the EU can also be developed in this regard, especially at the industrial level. According to D. Fiott, it is the European defense industrial and technological base that is key to European interoperability and harmonization of cyber defense capabilities[2]. 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 thus tools that should not be neglected when implementing 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" (NICP), 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 European Defence Agency and its CSRA, which can provide funding for certain cybersecurity/cyberdefense 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 cyberdefense. This standardization should be generalized to all actors involved.

[1] Bahrke, J. (2020). New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391 (Accessed 04.05.2022).

[2] Fiott, D. (2017, September). The cybridisation of EU defence. The European Union Institute for Security Studies (EUISS). URL: https://www.iss.europa.eu/content/cybridisation-eu-defence (Accessed 06.05.2022).

Third, NATO and the EU must also work closely with countries outside these international organizations. Certainly, effective cyber defense in Europe can be achieved through dialogue with states that are particularly active in cyberspace, so confidence-building measures should also be implemented with non-Allies and non-Members. The close relationship that Europe has with the United States could be an example. Also, the cooperation programs achieved between Australia and the EU, as well as with NATO, could be transferred to other countries. A coordinated EU/NATO approach with identified cyber defense partners could yield many benefits.

Finally, it is also worth noting that closer cooperation between NATO and the EU could play a major role in the establishment and implementation of international law in cyberspace. Today, despite the best efforts of international actors to establish law in cyberspace, there are no generally accepted norms and positions regarding cyberspace at the international level. As previously noted by the author, the European Union and NATO share a common position on the applicability of international law in cyberspace, which means that the two organizations have the opportunity for closer dialogue and cooperation. The European Union will play a special role in this matter, and this is due primarily to its active role in the negotiations, as well as the fact that the EU is an active member of the UN. According to the Lisbon Treaty, the European Union has a coordinating power for the positions of its member states. The EU could join with its member states in upholding the values it promotes for an "open, secure and reliable" cyberspace, as stated in the title of its cyber security doctrine. NATO, for its part, is not endowed by its founding treaty with the same competencies as the European Union. Thus, the EU's diplomatic influence prevails over that of NATO. The establishment of international law in Europe in close cooperation between NATO and the EU will make it possible to extend the applicability of that law throughout the world.

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.

Conclusion

The increasing role of cyberspace and its impact on social, economic, and technological development in a post-industrial society makes the study of how NATO and the EU could complement one another in terms of cybersecurity and cyber defense of special importance. Undoubtedly, “cyber” reaches head-of-state attention due to the increased political and economic incentives to explore the internet for malicious purposes.

The research question guiding this Master Thesis, ‘What is the current state of progress and shortcomings in cyberspace cooperation between NATO and the European Union with regard to cybersecurity and defense?’, has been answered by analyzing the results of quantitative, qualitative content, and comparative . It has been proved in the Master Thesis that the use of the term "cyber" in official NATO documents increased dramatically in the 2004-2018 time period, and the geopolitical situation in 2007-2009 as well as in 2014 is the reason for the increased presence of the term "cyber" in NATO's official documentation. Content analysis, performed in this Thesis, to determine the presence of words such as ‘cyber’, ‘cybersecurity’, ‘cyberthreat’, ‘cyber incident’ as well as ‘cyberattack’ in the official documents of both international organizations, proved that NATO and the EU’s perception of cybersecurity, cyber defense its main actors, and threats changed over time and helped the author to determine the reasons behind these changes. This proves that Hypothesis 1 and 2 hold true.

Thus, the impact of critical junctures on NATO and the EU’s perception such as cyber-attacks on its Member States should not be downplayed. It was not until the 2007 cyber-attack against Estonia (EU and NATO Member State) that the cyber threat became part of the political agenda. The 2008 cyberattacks against Georgia, an aspiring NATO and EU member country, demonstrated 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. The 2014 cyberattacks against Ukraine proved once again how a cyberattack may damage physical infrastructure, such as the power grid. These attacks 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). Thus, in 2014 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.

NATO and the EU’s perception of a threat and actor in the cyber field has been determined by using a coding process of keywords and associations of official EU and 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'. The data and the findings demonstrate that NATO sees individual states and state-sponsored groups as one of the most active actors. Cyberattacks on Ukraine, Estonia, and Georgia, as it was aforesaid, largely contributed to the development of this topic at NATO and its individual states' perception as primary actors, which proves Hypothesis 2 to hold true. The European Union, in its turn, stresses upon the idea of hackers and cybercriminals are the most dangerous actors in cyberspace. According to Europol's European Cybercrime Centre (EC3) 2019 report, hackers and cyber criminals cause the Member States the most harm. Thus, perceived by two international entities, NATO and the EU, cyber threats will deeper international cooperation between aforementioned organizations.

Critical theory with a sub-section of Critical Security Theory permitted the author to determine how discourse on cyberdefense and cybersecurity progressed and changed throughout the critical junctures and how cooperation evolved between NATO and the European Union. Cyber space, as stated before, is a man-made sphere of International relations, which means that it from our understanding comes the way we perceive it. This was especially important inasmuch as the understanding of how cyber realm became a security issue helped the author to determine why cyber threats were legitimated as one of the main threats both in the European Union and NATO.

The result of the comparative analysis permitted to compare EU-NATO Cyber Strategies, their similarities and differences, which enabled the author to determine prosperities for EU-NATO cooperation in the field of cybersecurity and cyber defense.

The EU and NATO share similar approaches when it comes to the applicability of international law in cyberspace, confidence-building measures, and relations with the private sector and international entities. Thus, these elements are avenues for developing a common or complementary approach to cyber defense and cybersecurity.

Nowadays cooperation between the Union and NATO in cyberspace includes information sharing, coordinated planning and concrete cooperation in the areas of hybrid threats, operational cooperation, cybersecurity, capacity-building, defense capacities, industry and research. However, since NATO and the European Union 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.

The European Union and NATO do not cooperate deeply enough in the areas of information sharing, establishing close links with the private sector and industry, joint cooperation with non-member states and regional international entities, and the establishment and implementation of international law in cyberspace. Thus, these four areas could be potential fields for enhancing cyber cooperation between NATO and the EU.

Deeper information sharing between the EU and NATO will strengthen the cyber capabilities of both international entities. This might be achieved through confidence-building measures (CBMs). Decision No. 1202 (2016) of the Organization for Security and Cooperation in Europe (OSCE) with a detailed system of CBMs could be implemented within the EU-NATO framework.

Close ties with the private sector are an integral part of achieving cybersecurity. As noted earlier, the European Union adopted The Directive on security of network and information systems (the NIS Directive), and the 2019 EU Cybersecurity Act, which demonstrates that the EU already has ties with the private sector. It is then the European defense industrial and technological base that is key to European interoperability and harmonization of cyber defense capabilities. The standardization of security of the EU-NATO practices and means of response would allow more robust cybersecurity.

Cooperation with non-member states and regional international entities is the third possibility for deepening the cooperation between NATO and the European Union. Effective cyber defense in Europe can be achieved through dialogue with states that are particularly active in cyberspace, so confidence-building measures should also be implemented with non-Members and non-Allies. The cooperation programs achieved between Australia and the EU, as well as with NATO, could be transferred to other countries. A coordinated EU/NATO approach with identified cyber defense partners could yield many benefits.

Finally, it is also worth noting that closer cooperation between NATO and the EU could play a major role in the establishment and implementation of international law in cyberspace. As stated earlier there are no generally accepted norms and positions regarding cyberspace at the international level. The European Union and NATO share a common position on the applicability of international law in cyberspace, which means that the two organizations have the opportunity for closer dialogue and cooperation. The European Union will play a special role in this matter, and this is due primarily to its active role in the negotiations, as well as the fact that the EU is an active member of the UN. According to the Lisbon Treaty, the European Union has a coordinating power for the positions of its Member States. The EU could join with

its member states in upholding the values it promotes for an "open, secure and reliable" cyberspace, as stated in the title of its cyber security doctrine. The establishment of international law in Europe in close cooperation between NATO and the EU will make it possible to extend the applicability of that law throughout the world.

Bibliography

Official documents

1. Annual Commission Report 2011 - Information and National Security, (2011). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120125_Annual_Report_2011_en.pdf (Accessed 10.04.2022).
2. Bucharest Summit Declaration. (2007). NATO. https://www.nato.int/cps/en/natolive/official_texts_8443.htm (Accessed 17.11.2021).
3. Consolidated text: Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02019D0797-20210519 (Accessed 28.04.2022).
4. 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). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12008M042 (Accessed 28.04.2022).
5. 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). URL: https://www.europarl.europa.eu/doceo/document/TA-7-2013-0376_EN.html (Accessed 25.04.2022).
6. Joint Communication to The European Parliament and The Council. (2019). URL: https://data.consilium.europa.eu/doc/document/ST-12211-2017-INIT/en/pdf (Accessed 27.04.2022).
7. London Declaration. (2019). NATO. https://www.nato.int/cps/en/natohq/official_texts_171584.htm (Accessed 18.11.2021).
8. NATO, Speech “Projecting Stability: Charting NATO’s Future”. Washington April 6th 2016 http://www.nato.int/cps/en/natohq/opinions_129758.htm?selectedLocale=en (Accessed 22.12.2021).
9. Prague Summit Declaration. (2002, November). NATO. https://www.nato.int/docu/pr/2002/p02-127e.htm(Accessed 16.12.2021).
10. PROPOSITION DE RÉSOLUTION sur l’Estonie. (2007). Union européenne, 2007 - Source: Parlement européen. URL : https://www.europarl.europa.eu/doceo/document/B-6-2007-0220_FR.html (Accessed 23.04.2022).
11. Reflection paper on the future of European defence. (2017). URL: https://ec.europa.eu/info/publications/reflection-paper-future-european-defence_en (Accessed 09.03.2022).
12. Report on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, Directive (EU) 2016/1148 (COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)). (2021). https://www.europarl.europa.eu/doceo/document/A-9-2021-0313_EN.html (Accessed 05.05.2922).
13. Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense (2018/2004(INI)). -Strasbourg. - 2018.

14. Strasbourg / Kehl Summit Declaration. (2009). NATO. https://www.nato.int/cps/en/natolive/news_52837.htm (Accessed 17.11.2021).
15. Summit Declaration Lisbon. (2010). NATO. http://www.nato.int/cps/en/natolive/official_texts_68828.html (Accessed 17.11.2021).
16. The 9th Annual European Cyber Security Conference. (2022, March 31). EU Cyber Security 2021. URL: https://eucybersecurity.com/ (Accessed 17.11.2021).
17. Wales Summit Declaration. (2014). NATO. https://www.nato.int/cps/en/natohq/official_texts_112964.htm (Accessed 17.11.2021).

Analytical reports

18. Anna Zygierewicz. (2020, November). Directive on security of network and information systems (NIS Directive). European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/654198/EPRS_BRI(2020)654198_EN.pdf (Accessed 07.05.2022).
19. Bahrke, J. (2020). New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391 (Accessed 04.05.2022).
20. Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT) | PESCO. (2018). Permanent Structured Cooperation (PESCO). URL: https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/ (Accessed 07.04.2022).
21. Cyberdéfense de l'OTAN. (2018). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/20180213_1802-factsheet-cyber-defence-fr.pdf (Accessed 26.04.2022).
22. Cybersécurité européenne : comment construire une société numérique plus sûre ? (2019). Corporate. URL: https://www.orange.com/fr/cybersecurite/cybersecurite-europeenne-comment-construire-une-societe-numerique-plus-sure (Accessed 04.04.2022).
23. Digital Around the World. (2022, April). DataReportal – Global Digital Insights. URL: https://datareportal.com/global-digital-overview#:%7E:text=A%20total%20of%205%20billion,12%20months%20to%20April%20202 (Accessed 12.05.2022).
24. European Court of Auditors. (2019). Challenges to effective EU cybersecurity policy. URL: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf (Accessed 02.05.2022).
25. Fiott, D. (2017, September). The cybridisation of EU defence. The European Union Institute for Security Studies (EUISS). URL: https://www.iss.europa.eu/content/cybridisation-eu-defence (Accessed 06.05.2022).
26. Five years after Estonia's cyber-attacks: lessons learned for NATO? (2012). Research Division - NATO Defense College, Rome.
27. Internet Organized Crime Threat Assessment (IOCTA). (2019). URL: https://www.europol.europa.eu/publications-events/main-reports/iocta-report (Accessed 16 May 2022).
28. NATO in U.S. Global Politics: American Concepts of Transformation, 2013. URL: https://www.dissercat.com/content/nato-v-globalnoi-politike-ssha-amerikanskie-kontseptsii-transformatsii (Accessed 19 April 2022).

29. Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA. (2021). Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. URL: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a (Accessed 16.05.2022).
30. ŠTrucl, D. (2021). Tallinn 2021 Comparative study on the cyber defence of NATO Member States. NATO CCDCOE. https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf (Accessed 13.02.2022).
31. The Cybersecurity Challenge in Central and Eastern Europe. (2018). CMS. URL: https://cms.law/en/media/local/cms-cmno/files/publications/publications/the-cybersecurity-challenge-and-central-and-eastern-europe (Accessed 04.02.2022).

Dissertations and abstracts

32. André Tosbotn R. NATO and Cyber Security. MA thesis, Leiden University, Leiden, 2020.
33. Boguslavskaya, Y. NATO v globalnoi politike SSHA amerikanskie kontseptsii transformatsii [NATO in U.S. Global Politics: American Concepts of Transformation]. Ph.D. thesis. 23.00.04. Saint-Petersburg State University, Saint Petersburg, 2013.
34. E. Nagyfejo, Transatlantic collaboration in response to cybercrime: how does strategic culture affect EU-US collaboration in the fight against cyber crime? MA thesis, Université de Warwick, 2016.
35. Neven A. Brave New World: NATO, the EU and the New Age of Cyberspace. MA thesis, Department of Political Science, University of Oslo, Oslo, 2020.
36. Shidukov A. Evropeiskii soiuz problemy i perspektivy [European Union: Problems and Prospects]. Bachelor thesis, Pyatigorsk University, Pyatigorsk, 2020.

Articles and Scientific Monographs

37. Adam Posen (2013). The Euro at Five: Ready for a Global, 01(01). URL: https://doi.org/10.4172/2375-4389.1000e101. (Accessed 02.03.2022).
38. 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. URL: http://www.jstor.org/stable/resrep21140.13. (Accessed 16 May 2022).
39. Amoore, L., de Goede, M. Risk and the War on Terror. – London: Routledge, 2008. – P. 156.
40. B. Tertrais. Article 5 of the Washington Treaty: Its Origins, Meaning and Future / B. Tertrais // Research Division, NATO Defense College. – 2016. – P.12.
41. Booth, Ken. (1991). "Security and Emancipation", Review of International Studies, Vol. 17, No. 4 (Oct., 1991), pp. 313-326.
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.
43. Christou G. Cybersecurity in the European Union: resilience and adaptability in governance policy / George Christou // New Security Challenges Series. Palgrave Macmillan UK, London. – 2016. – P.35-61.
44. Christou, G. Conclusions: Towards Effective Security as Resilience in the European Union? / George Christou // New Security Challenges Series. Palgrave Macmillan UK, London. – 2016. – P.171-189.

45. Christou, G. Cybersecurity in the Global Ecosystem. In: Cybersecurity in the European Union. New Security Challenges Series / George Christou // New Security Challenges Series. Palgrave Macmillan UK, London. – 2016. – P.70-94.
46. Christou, G. What is the Difference Between a Realist and a Gramscian Understanding of Hegemony? International Relations. URL: https://www.e-ir.info/2012/06/08/what-is-the-difference-between-a-realist-and-a-gramscian-understanding-of-hegemony/ (Accessed 13.11.2021).
47. Coker, C. (2013). Why NATO Should Return Home The Case for a Twenty-First Century Alliance. The RUSI Journal, 158(4), 122–138.
48. Comprehensive study on cybercrime: draft - February 2013 / UNODC. Imprint New York : United Nations, 2013. 287 p.
49. Cox, Robert W. "Gramsci, Hegemony and International Relations : An Essay in Method." Millennium 12, no. 2 (June 1983): 162–75.
50. 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.
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.
52. Desforges, A. (2014). Les représentations du cyberespace : un outil géopolitique. Hérodote, 152-153, 67-81.
53. Douzet, F. (2014). La géopolitique pour comprendre le cyberespace. Hérodote, 152-153, 3-21.
54. Duke, S. Europe's Harder Edges: Security and Defence. Europe as a Stronger Global Actor, - 2016. -P.171–203.
55. Dunn Cavelty, M.,Wenger, A. Cyber security meets security politics: Complex technology, fragmented politics, and networked science / Dunn Cavelty, M.,Wenger, A. // Contemporary Security Policy. – 2019. № 41(1). P.5–32.
56. Eriksson, J., & Giacomello, G. The Information Revolution, Security, and International Relations: (IR)relevant Theory? / Eriksson, J., & Giacomello, G. // International Political Science Review. – 2003. № 27(3). P.221–244.
57. Fiott, D. (2017). The cybridisation of EU defence. Issue Alert, 24. URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert%2024%20Cybridisation%20of%20defence.pdf (Accessed 28.04.2022).
58. Fuster, G.G., Jasmontaite, L. (2020). Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In: Christen, M., Gordijn, B., Loi, M. (eds) The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, vol 21. Springer, Cham.
59. Giles, Keir (2015) Russia and Its Neighbours: Old Attitudes, New Capabilities. Chapter 2 in Cyber War in Perspective: Russian Aggression Against Ukraine. NATO CCD COE Publications, Tallinn 2015.
60. Henrikson, Allan K. The Creation of the North Atlantic Alliance 1948-1952 / Henrikson, Allan K. // Naval War College. - 1980. №33. -P.33-62.
61. Herz, J. H. Idealist Internationalism and the Security Dilemma / Herz, J. H // World Politics. – 1950. № 2(2). - P.157–180.
62. Howorth, J. NATO and ESDP: Institutional Complexities and Political Realities / Howorth, J. // Politique étrangère. - 2009. – P. 95-106.

63. Howorth, Jolyon. Jolyon Howorth: Great Britain and Europe: From Resistance to Rancor / Howorth, Jolyon // Politique étrangère, vol. i, no. 2. – 2010. – P. 259-271.
64. Hsieh, H. F., & Shannon, S. E. Three Approaches to Qualitative Content Analysis. Qualitative Health Research / Sarah E. Shannon, Hsiu-Fang Hsieh // Qual Health Res, 15(9). – 2005. -P. 1277–1288.
65. Hunker, Jeffrey. Cyber war and cyber power Issues for NATO doctrine / Hunker, Jeffrey // Semantic Scholar. – 2010. – №3. – P. 158.
66. Joubert, Vincent, Jean-Loup Samaan. L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE / Joubert, Vincent, Jean-Loup Samaan // Hérodote. – 2014. № 1-2. P.261-275.
67. 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.
68. Krause, Keith. "Critical Theory and Security Studies: The Research Programme of 'Critical Security Studies'." Cooperation and Conflict 33, no. 3 (1998): 298-333. URL: http://www.jstor.org/stable/45083929 (Accessed 07.12. 2020).
69. Kristi Raik. Not Yet Fit for the World: Piecemeal Buildup of EU Military, Cyber and Intelligence Assets / Kristi Raik // European Union. URL: https://www.iai.it/sites/default/files/joint_rp_4.pdf (Accessed 07.04.2022).
70. Leysens A. The Legacy of Coxian Critical Theory. In: The Critical Theory of Robert W. Cox / Anthony Leysens // International Political Economy Series. Palgrave Macmillan, London. – 2008. – P.115-144.
71. Lucas K. Cyber legalism: why it fails and what to do about it / Lucas Kello // Journal of Cybersecurity. – 2021. - Volume 7, Issue 1.
72. M. Storm Jensen. Five good reasons for NATO's pragmatic approach to offensive cyberspace operations / Mikkel Storm Jensen // Defence Studies. – 2022. URL: DOI: 10.1080/14702436.2022.2080661 (Accessed 02.05.2022)
73. 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. URL: http://www.jstor.org/stable/25144714. (Accessed 16.05.2022).
74. Masoumifar, A. Cyberspace Sovereignty: Is Territorializing Cyberspace Opposed to Having a Globally Compatible Internet? / //Journal of Cyberspace Studies. – 2022. № 6(1). P.1-20.
75. Matt Davies, IR Theory: Problem-Solving Theory Versus Critical Theory. – International Relations. URL: https://www.e-ir.info/2014/09/19/ir-theory-problem-solving-theory-versus-critical-theory/.
76. Moolakkattu JS. Robert W. Cox and Critical Theory of International Relations. International Studies. 2009;46(4):439-456. doi:10.1177/002088171004600404 (Accessed 07.12. 2020).
77. Nazario, J. DDoS attack evolution / Janson Nazario // Network Security. – 2008. № (7). - P.7–10.
78. Nunes, João. "Reclaiming the Political: Emancipation and Critique in Security Studies." Security Dialogue 43, no. 4 (2012): 345-61.URL: http://www.jstor.org/stable/26301921 (Accessed 25. 10. 2021).
79. Poptchev, Peter. NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages / Peter Poptchev // Information & Security: An International Journal. – 2020. № 45. - P.35-55.
80. Risk and the War on Terror / Louise Amoore, Marieke de Goede [et al.] – London: Routledge, 2008. – 156 p.

81. Sallach, David L. Class Domination and Ideological Hegemony / Sallach, David L // The Sociological Quarterly 15. – 1974. № 1. -P.38-50. URL: http://www.jstor.org/stable/4105619 (Accessed 25.10.2021).
82. SETH, Catriona, VON KULESSA, Rotraud. The Idea of Europe : Enlightenment Perspectives. Nouvelle édition [en ligne]. Cambridge : Open Book Publishers, 2017.
83. Singer, Peter and Friedman, Allan (2014) Cybersecurity and Cyberwar. Oxford University Press.
84. Staff, S. X. (2016, February 10). NATO, EU sign agreement on cyberdefense cooperation. Phys.Org. URL: https://phys.org/news/2016-02-nato-eu-agreement-cyberdefense-cooperation.html (Accessed 23.04.2022).
85. Tardy, T. Does European defence really matter? Fortunes and misfortunes of the Common Security and Defence Policy / Tardy, T // European Security. – 2018. № 27(2). - P.119–137.
86. Tardy, T., Lindstrom, G. (2019). The scope of EU-NATO cooperation. In NATO and the EU: The essential partners / Tardy, T., Lindstrom, G. // NATO Defense College. – 2019. – P.5-14.
87. Tertrais. Article 5 of the Washington Treaty: Its Origins, Meaning and Future / B. Tertrais // Research Division, NATO Defense College. – 2016. – P.12-35.
88. The Balance of Power and Future Peace In: The Idea of Europe: Enlightenment Perspectives. Cambridge: Open Book Publishers, 2017. – P.122-124.
89. Theodora Dame Adjin-Tettey, Keith M. Johnston (2022) Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education / Theodora Dame Adjin-Tettey, Keith M. Johnston // Cogent Arts & Humanities. – 2022. №9:1. DOI: 10.1080/23311983.2022.2037229 (Accessed 11.05.2022).
90. Thomas, E., Thompson, N., Wanless, A. (2020, June 10). The Challenges of Countering Influence Operations. Carnegie Endowment for International Peace. URL: https://carnegieendowment.org/2020/06/10/challenges-of-countering-influence-operations-pub-82031 (Accessed 03.12.2021).
91. Varwick, J. (2019). The European Union and NATO: Partnership or Rivalry? Worldsecuritynetwork. URL: https://www.worldsecuritynetwork.com/Other/Varwick-Prof.-Dr.-Johannes/The-European-Union-and-NATO-Partnership-or-Rivalry (Accessed 22.01.2022).
92. Vosoughi, S., Roy, D., Aral, S. (2018). The spread of true and false news online / Vosoughi, S., Roy, D., Aral, S //Science (New York, N.Y.). – 2018. № 359(6380). – P.1146–1151.
93. Wyn Jones, R. (1999). Security, strategy and critical theory. Colorado: Lynne Rienner Publications.
94. Zaslavskaya N. (2017). 'Theories of International Relations', in Russia and the World. (ed.). Lexington Books: Maryland. pp. 35-37.

Communication and Mass Media

95. Berlinger, J. C. (2022, May 16). Finland and Sweden want to join NATO. Here's how it works and what comes next. CNN. URL: https://edition.cnn.com/2022/05/14/europe/sweden-finland-nato-next-steps-intl/index.html (Accessed 19.05.2022).
96. How Estonia became a global heavyweight in cyber security. Invest in Estonia (February 11, 2022). URL: https://investinestonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/ (Accessed 04.02.2022)

97. Kerner, S. M. (2022, March 15). 34 Cybersecurity Statistics to Lose Sleep Over in 2022. WhatIs.Com. URL: https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020 (Accessed 12.05.2022).
98. Le Pen wants France out of NATO integrated command, backs NATO-Russia links (2022). France 24. URL: https://www.france24.com/en/france/20220413-le-pen-wants-france-out-of-nato-integrated-command-backs-nato-russia-links (Accessed 13.05.2022).
99. Milmo, D. (2022, February 28). Anonymous: the hacker collective that has declared cyberwar on Russia. The Guardian. URL: https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia (Accessed 13.03.2022).
100. Thomson, I., & Thomson, I. (2007, June 1). Russia “hired botnets” for Estonia cyber-war. iTnews. URL: https://www.itnews.com.au/news/russia-hired-botnets-for-estonia-cyber-war-82600 (Accessed 13.02.2022).
101. Van der Meer, (2017). EU Creates a Diplomatic Toolbox to Deter Cyberattacks. Council of Foreign Affairs. URL: https://www.cfr.org/blog/eu-creates-diplomatic-toolbox-deter-cyberattacks (Accessed 28.04.2022).

Appendix A.

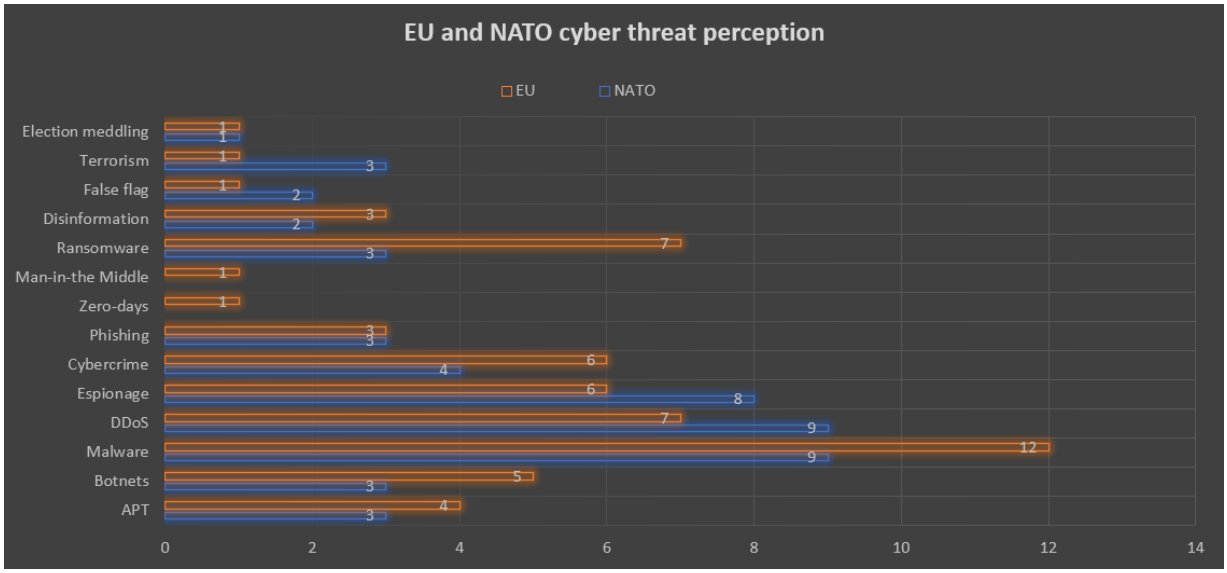
The Increasing Prominence of Cybersecurity as perceived by NATO

Year	Cyber	New Threats	Terrorism	Russia	Article 5
2004	1	3	36	16	0
2005	1	0	4	21	0
2006	2	0	13	14	0
2007	6	2	3	1	0
2008	9	0	12	22	1
2009	7	0	1	0	0
2010	20	0	8	19	2
2011	3	1	1	4	0
2012	15	0	14	35	1
2013	2	3	2	0	0
2014	20	0	13	46	3
2015	9	0	0	8	1
2016	2	0	3	42	1
2017	13	7	4	33	1
2018	6	3	2	7	0
Total	116	19	116	268	10

This table demonstrates the dramatic increase on ‘cyber’ term on NATO summits from 2004 Summit in Istanbul to the 2018 Brussels Summit. The consistency of the use of “Russia” and “terrorism” is of special interest. ‘Cyber” and “terrorism” shares the second place in the rank behind Russia. According to this table, Russia represents the main threat to NATO.

Appendix B.

EU and NATO cyber threat perception

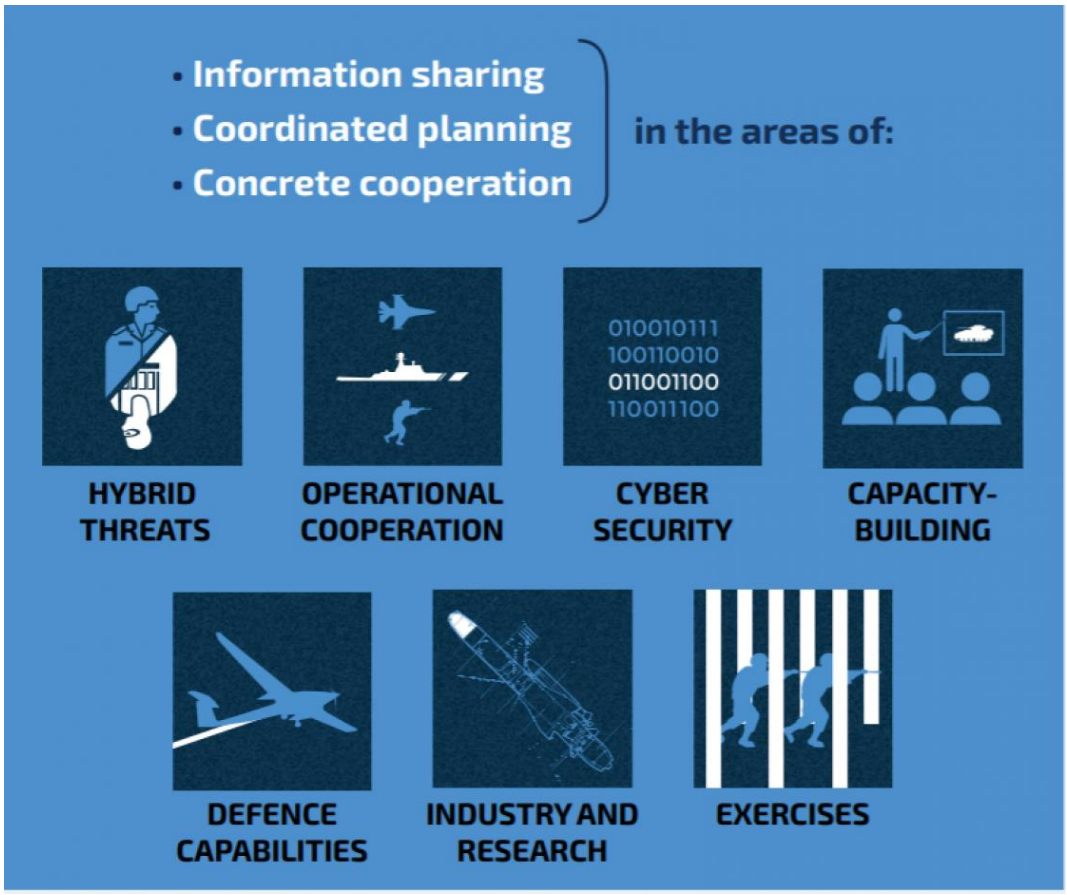


Content analysis that performed to determine the presence of words such as 'cyber', 'cybersecurity', 'cyberthreat', 'cyber incident' as well as 'cyberattack', themes, or concepts within some given qualitative data permitted to determine NATO and the EU's perception of a threat and actor in the cyber 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 2004 up to 2018 insofar as its Member States have been targeted by the state-sponsored groups (the USA, France, Germany as well as Australia)[1].

[1] 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.

Appendix C.

Areas of EU-NATO cooperation in cybersecurity and cyberdefense



URL: https://www.eeas.europa.eu/eeas/eu-nato-cooperation-factsheets_en

According to the 2018 Joint Declaration between the European Union and NATO, cooperation between two international entities in cyberspace includes information sharing, coordinated planning and concrete cooperation in the areas of hybrid threats, operational cooperation, cybersecurity, capacity-building, defense capacities, industry and research. The EU-NATO cooperation is based on openness, transparency and inclusiveness.

Appendix D.

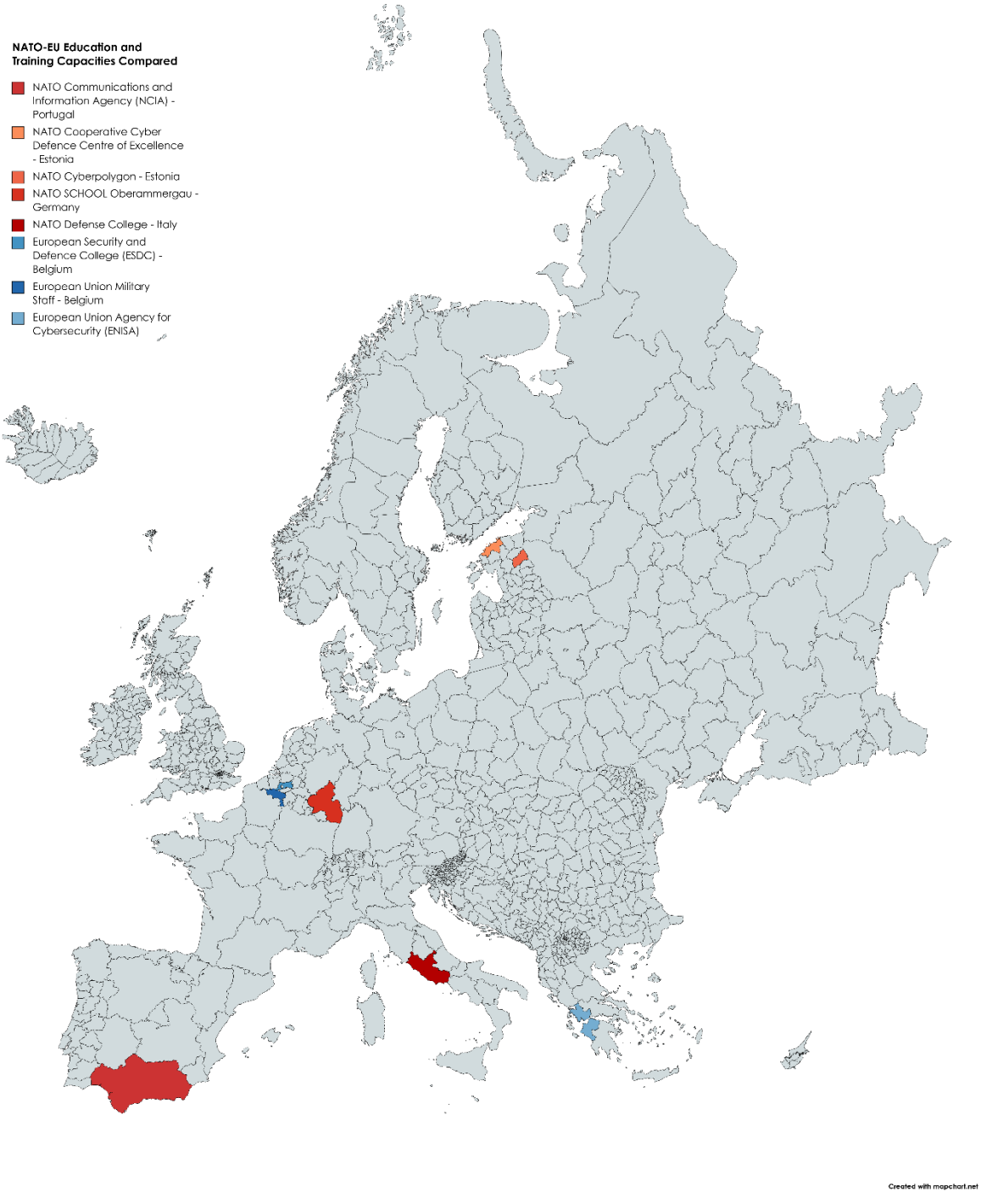
EU-NATO Cyber Resilience Capabilities Compared

N	European Union	North Atlantic Treaty Organization
1	European Union Intelligence and Situation Centre (EU INTCEN)	Emerging Security Challenges Division (ESCD)
2	European Union Agency for Cybersecurity (ENISA)	NATO Communications and Information Agency (NCIA)
3	Cyber Rapid Response Team (CRRT)	NATO Computer Incident Response Capability (NCIRC)
4	Cyber Crises Liaison Organisation Network (CyCLONe)	Cyber Operations Centre (CYOC)

Table compiled by the author based on data collected from official NATO and European Union websites.

Appendix E.

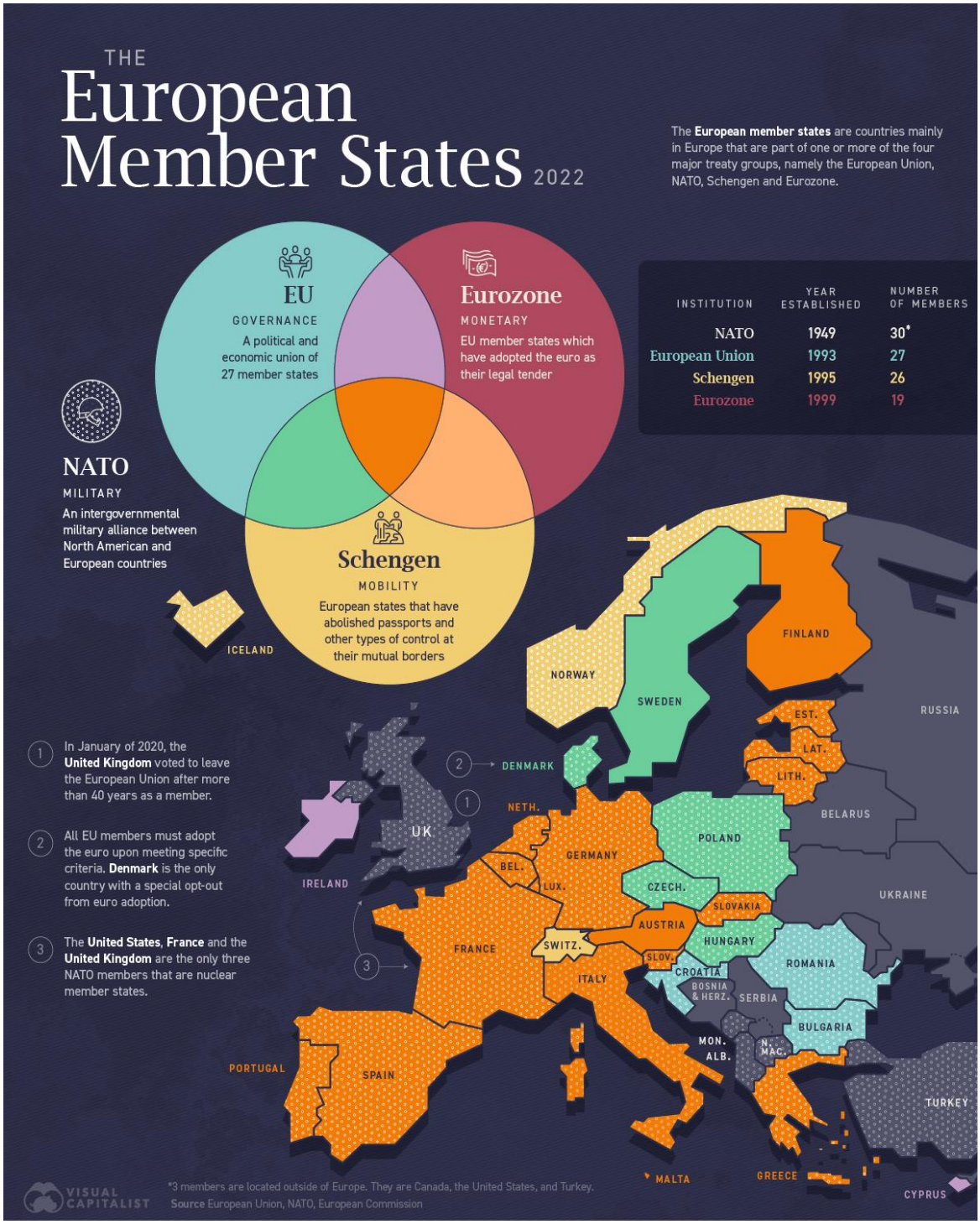
EU-NATO Cyber Education and Training Capabilities Compared



Map compiled by the author based on data collected from official NATO and European Union websites.

Appendix E.

A Visual Guide to Europe's Member States



URL: https://www.visualcapitalist.com/a-visual-guide-to-europes-member-states/

The European Union and the North Atlantic Organization on the map