The EU as a Collective Security Actor:
Cyber Defense Efforts of the EU Between 2013 and 2019

Shinouk Ettema (9082425)

MA. International Relations in Historical Perspective

Utrecht University

Thesis

Dr. Marten Boon

16th of January 2023

14953 words

Abstract

In the past decade, cybersecurity concerns became paramount to national and supranational security. As a security actor, the European Union has responded to the exponential rise in threats by implementing new policies aimed at defending the Union against malicious cyber-attacks. This thesis evaluates to which extent the European Union can be classified as a collective security actor in the field of cyber defense. Through a targeted sentiment analysis and a critical discourse analysis, this thesis proposes that the EU passed through multiple cycles of the collective security framework between the early 2000s and 2019. As such, the EU published the groundbreaking Cybersecurity Act in 2013 and the Cyber Defense Policy Framework in 2014. Even though the EU attempted to implement supranational decision-making, these policies remained at the intergovernmental level. In 2016, a new cycle of the collective security framework commenced, when NATO classified cyber as the fifth domain of war. Consequently, the NotPetya attack in 2017 disrupted critical infrastructures all over the world. As a response, the EU revised the Cyber Defense Policy Framework in 2018 and the Cybersecurity Act in 2019. This thesis concludes that with these documents, the EU was able to shift decision-making to the supranational level, even though some problems of institutional fragmentation persist. Therefore, the EU almost classifies as a collective security actor, but should act on intentions to solve institutional fragmentation.

Keywords: Cyber Defense, Collective Securitization, European Integration, Cybersecurity, European Union, ENISA, NotPetya

Table of Contents

List of Abbreviations

ARPA - Advanced Research Projects Agency
ARPANET - Network for non-military communication
CERT - Computer Emergency Response Team
CFSP - Common Foreign and Security Policy
CSDP - Common Security and Defense Policy
CSIRT - Computer Security Incident Response Team
DDoS - Distributed Denial of Service
EC3 - European Cybercrime Center
EEAS - European External Action Service
ENISA - European Union Agency for Cyber Security
EU - European Union
MEP - Member of the European Parliament
MILNET - Military Network
MoD - Ministry of Defense
NATO - North Atlantic Treaty Organization
PESCO - Permanent Structured Cooperation
TEU - Treaty on the European Union
US - United States
USSR - Union of Soviet Socialist Republics

Introduction

In recent years, the internet and corresponding cybersecurity risks have changed the international world order. Digital interconnectivity is now crucial to the lives of European citizens, yet the safety and security of internet usage involve enormous risks of failure. Moreover, not only personal devices are at risk, cyber is increasingly used as a means of warfare in the international arena. The concept cyber relates to information technology, which entails computer-based activities. As a consequence of increased risks in the cyber domain, the North Atlantic Treaty Organization (NATO) classified cyber as the fifth domain of war in 2016, next to the more conventional areas of land, sea, air and more recently, space.[1] Cyberwarfare attacks are often aimed at critical infrastructure, such as government services, banks or the transportation sector.

One of the most striking and well-known recent examples of how far-reaching cyber warfare has come to be, is the NotPetya attack of 2017. Starting out as an assault of one country on another, the malware was allegedly designed by the Russian elite hacker group Sandworm to disrupt and destroy Ukrainian critical infrastructure.[2] NotPetya paralyzed the Ukrainian tax software called M.E.Doc, which was used by airports, hospitals, banks, ATMs and nearly every federal agency in the country. The Ukrainian Minister of Infrastructure Volodymyr Omelyan summarized the attack with the words "The government is dead".[3] Spreading from Ukraine, NotPetya managed to disrupt critical infrastructure globally, by infecting multinational companies with relations to Ukraine, such as the world's largest shipping conglomerate Maersk, delivery company FedEx, Pharmaceutical company Merck, and the Australian division of Cadbury. In total, the damages are estimated to be $10 billion, making NotPetya the most expensive cyberattack to this day. The NotPetya attack is seen as one of the most devastating cyberattacks in history and is a leading example of how digital vulnerability can lead to enormous international disruption in critical infrastructure.[4]

Therefore, it is crucial to focus on cyber defense measures to be able to prevent large-scale cyber-attacks. Cyber defense is thus an increasingly relevant research topic, which bears strong academic and societal relevance. To ensure conceptual clarity, this thesis follows the definition by Green on cyber warfare (and correspondingly also on cyber defense):

[1] NATO, "Cyber Defence Pledge," NATO, accessed September 5, 2022, https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

[2] Andy Greenberg, "The White House Blames Russia for NotPetya, the 'Most Costly Cyberattack In History,'" *Wired*, accessed September 21, 2022, https://www.wired.com/story/white-house-russia-notpetya-attribution/.

[3] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired, August,* 2018.

[4] "What Is NotPetya?," IT PRO, accessed September 15, 2022, https://www.itpro.com/malware/34381/what-is-notpetya.

> "Cyber warfare is an extension of policy by actions taken in cyberspace by state actors (or by non-state actors with significant state direction or support) that constitute a serious threat to another state's security, or an action of the same nature taken in response to a serious threat to a state's security (actual or perceived)."[5]

Societally, this research thus finds its relevance in considering political responses to cyberwarfare tactics, the consequences of which are already shown by the NotPetya attack. Therefore, it is important to assess the efforts of the European Union (EU) after the period between 2014 and 2018 to minimize the risk of devastating cyber-attacks, as taking measures will remain of utmost importance in the foreseeable future to prevent societal paralysis as a consequence of a malicious cyberattack.

Academically, the body of research on cybersecurity is rapidly expanding due to increasing consequences to both countries as a whole and individual citizens. However, most academic articles remain in the domain of political science, international law or computer science. At the time of writing, research employing a historical perspective towards cyber defense is still underdeveloped. Furthermore, in the influential Special Issue of *West European Politics* on collective securitization in the EU, authors Sperling and Webber conclude that the sub-category of EU security governance is still outside the scholarly mainstream.[6] In the same Special Issue Christou explains that the EU's collective response to the cyber defense pillar was underdeveloped in 2018, while there was ample attention for the other two pillars: cybercrime and network and information security,[7] even though cyber warfare possibly has the most far-reaching consequences for both the EU, Member States and citizens individually. Yet, there are no academic articles applying the collective securitization framework to cyber defense specifically.

Moreover, the lack of a historical perspective to research in cyber defense is problematic, because when evaluating processes of change in the international arena, the usage of history is crucial to create a deeper level of analysis.[8] Diachronic change, or the comparison between several periods, adds context and depth to the analysis of international relations cases.[9] Therefore, in order to enhance the understanding of cyber defense measures employed by the EU, this thesis has an

[5] Richard Stiennon, "A Short History of Cyber Warfare," in *Cyber Warfare* (Routledge, 2015), 2.

[6] James Sperling and Mark Webber, "The European Union: Security Governance and Collective Securitisation," *West European Politics* 42, no. 2 (2019): 230.

[7] George Christou, "The Collective Securitisation of Cyberspace in the European Union," *West European Politics* 42, no. 2 (2019): 278–301, https://doi.org/10.1080/01402382.2018.1510195.

[8] Steve Yetiv, "History, International Relations, and Integrated Approaches: Thinking about Greater Interdisciplinarity," *International Studies Perspectives* 12, no. 2 (May 2011): 100, https://doi.org/10.1111/j.1528-3585.2011.00422.x.

[9] Yetiv, 101.

interdisciplinary nature. Not only is this study based on primary sources, the analysis is also supported by a diachronic comparison of social developments, thus providing a historical perspective to a research in international relations.[10]

Furthermore, the chosen case of cybersecurity inherently crosses multiple disciplines, therefore an interdisciplinary approach is especially suitable. This research thus contributes to the existing literature by filling the gap by applying both a historical, as well as a collective securitization perspective on the case study of the EU as a security actor in the field of cyber defense. This thesis hypothesizes that after the formulation of the Cybersecurity Act in 2013 and the 2014 Cyber Defense Policy Framework, the EU became a more meaningful actor in the field of cyber defense. This is due to an exponential rise in hybrid threats, after which securitization took place. This effect crystallized after the period between 2014 and 2018, in which cyber was officially classified as a domain of war and the NotPetya attack took place. The cyber landscape thus drastically changed between 2014 and 2018. As a result, the EU published revisions of the ground-breaking documents of 2013 and 2014 in 2018 and 2019 respectively. Furthermore, this thesis adds to understanding of the EU as a cybersecurity actor, which was identified as a gap in the literature by Carrapico and Barrinha.[11]

As Carrapico and Barrinha also show, the past two decades it has been a priority of the EU to develop a response to cyber warfare.[12] Due to the ever-increasing potential and risks of cyber warfare, shown by the NotPetya attack, this thesis aims to research the cyber defense efforts of the EU. The corresponding research question entails: *To which extent did the EU develop as a collective security actor in the field of cyber defense between the formulation of the first Cybersecurity Act in 2013 and the 2019 revision?* This period is chosen to include the policy process towards the first publication of the EU Cybersecurity Act in 2013 until the 2019 revision of the Cybersecurity Act.

This thesis proceeds with an overview of the existing literature on hybrid threats, the EU as a security actor and cyber defense in the historiography section. In the theoretical framework securitization theory and collective securitization are outlined. Then, the first chapter outlines the historical process leading up to the 2013 Cybersecurity Act, to embed the findings into a historical framework. The sub research question answered in this chapter is: *In what way has cyber defense developed from being non-politicized in the 1990s to being securitized from 2013 onwards?* To formulate an answer to the overarching research question, four central EU publications are evaluated

[10] Lucian M Ashworth, “Interdisciplinarity and International Relations,” *European Political Science* 8, no. 1 (March 1, 2009): 24, https://doi.org/10.1057/eps.2008.11.
[11] Helena Carrapico and Andre Barrinha, “European Union Cyber Security as an Emerging Research and Policy Field,” *European Politics and Society* (Taylor & Francis, 2018), 301.
[12] Carrapico and Barrinha, “European Union Cyber Security as an Emerging Research and Policy Field.”

in the analysis section. The analysis section is divided into two separate periods. The second chapter evaluates the 2013 Cybersecurity Act[13] and 2014 Cyber Defense Policy Framework[14] and answers the sub research question *In what way did the EU articulate discourses of securitization in the 2013 Cybersecurity Act and 2014 Cyber Defense Policy Framework?* Chapter three deals with the societal developments between 2014 and 2018, and with the revision of both documents, in particular the 2018 update of the Cyber Defense Policy Framework[15] and the 2019 revision of the Cybersecurity Act.[16] The sub research question answered in this chapter is: *In what way did the EU revise discourses of securitization in the 2018 Cyber Defense Policy Framework and 2019 Cybersecurity Act after the classification of Cyber as the fifth domain of war in 2016?* The concluding section compares and contrasts the findings to formulate an answer to the overarching research question. It then addresses limitations of this study and provides suggestions for further research.

Historiography

This section reviews the existing literature on hybrid threats and outlines the academic debate on the capability of the EU to act as a security actor, specifically in the field of cybersecurity.

Within war studies, a field closely related to security studies, it has been argued that from the 1990s onwards, the advance in weapons technology led to a 'revolution in military affairs,' signaling a new way in which wars are fought.[17] Der Derian argued in 2002 that war became postmodern or virtual, implying that conventional war was continued by new and hybrid threats. Usage of hybrid threats implies that international conflict is increasingly based on the usage of new and superior technology, instead of more conventional war tactics.[18] In the last two decades, literature on hybrid threats grew rapidly, even though the concept is relatively novel.

In 2010, Hoffman outlines that the hybrid threat construct found its way to speeches of the United States (US) Secretary of Defense, even though the focus mainly lied on the land warfare

[13] European Parliament and the Council of the European Union. "Regulation concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004" Regulation 2013/526, May 21, 2013. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32013R0526

[14] Council of the European Union, "EU Cyber Defence Policy Framework," November 18, 2014, https://ccdcoe.org/uploads/2018/11/EU-141118-EUCyberDefencePolicyFrame-2.pdf.

[15] Council of the European Union, "EU Cyber Defence Policy Framework (as Updated in 2018)," November 19, 2018, https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf.

[16] European Parliament and the Council of the European Union. "Regulation on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)." Regulation 2019/881, April 17, 2019. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32013R0526

[17] Andrew Heywood, *Global Politics*, 2nd edition, Palgrave Foundations (Basingstoke: Palgrave Macmillan, 2014), 260.

[18] James Der Derian, "Virtuous War/Virtual Theory," *International Affairs* 76, no. 4 (2000): 771–72, https://doi.org/10.1111/1468-2346.00164.

aspects of the threat.[19] In the same year, NATO published a *Capstone Concept for the Military Contribution to Countering Hybrid Threats* in which examples of hybrid threats included cyber war, but also global terrorism, piracy, demographic challenges or resources security.[20] In 2016, during the NATO summit in Warsaw, the cyber domain was recognized as a 'fifth domain of war', next to the already established domains of land, sea, air, and space.[21] Accordingly, much literature on cyber threats was published, mostly focusing on how to address the issue.[22]

As a response, various authors attempted to answer the question of which security actor is responsible for taking measures against cyber threats. Within the EU, attribution of cyber-attacks is classified as a sovereign act by the EU Member States. Yet, each Member State has different intelligence capabilities, may choose its own method and procedure for attribution, and has different geopolitical relations to external actors. Additionally, only a few Member States have the technical capabilities to respond with a defensive cyber counterattack on their own. Instead, most Member States rely on the intelligence level of NATO partners. As a consequence, Bendiek and Schulze argue this leads to a lack of coherence in cyber diplomacy on EU level.[23]

Christou follows this reasoning, and argues that much progress needs to be made for the EU to become resilient against cyber threats.[24] Ruohonen, Hyrynsalmi, and Leppänen add to this discussion by explaining that cybersecurity institution-building activities in the EU have halted or slowed down, while cybersecurity issues are still pressing.[25] They argue that the EU has shown its political capability by building new institutions and introducing new regulations, but experiences problems such as the lack of technological interoperability or poor strategic depth and the slowness of political responses and institutions. Sliwinksi asserts that due to conceptual differences and a lack

[19] F. G. Hoffman, "'Hybrid Threats': Neither Omnipotent Nor Unbeatable," *Orbis* 54, no. 3 (January 1, 2010): 441–42, https://doi.org/10.1016/j.orbis.2010.04.009.
[20] NATO, "Cyber Defence Pledge."
[21] NATO.
[22] Sascha-Dominik Bachmann, "Hybrid Threats, Cyber Warfare and NATO's Comprehensive Approach for Countering 21st Century Threats - Mapping the New Frontier of Global Risk and Security Management," *Amicus Curiae* 88 (2011): [iii]-28; Aapo Cederberg and Pasi Eronen, "How Can Societies Be Defended against Hybrid Threats," *Strategic Security Analysis* 9, no. 1 (2015): 1–10; Sascha Dov Bachmann and Hakan Gunneriusson, "Terrorism and Cyber Attacks as Hybrid Threats: Defining a Comprehensive Approach for Countering 21st Century Threats to Global Risk and Security," *The Journal on Terrorism and Security Analysis*, 2014; William Steingartner, Darko Galinec, and Andrija Kozina, "Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model," *Symmetry* 13, no. 4 (2021): 597; Gregory F. Treverton et al., "Addressing Hybrid Threats" (Försvarshögskolan (FHS), 2018).
[23] Annegret Bendiek and Matthias Schulze, "Attribution: A Major Challenge for EU Cyber Sanctions. An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW" (SWP Research Paper, 2021), 10–19.
[24] Christou, "The Collective Securitisation of Cyberspace in the European Union."
[25] Jukka Ruohonen, Sami Hyrynsalmi, and Ville Leppänen, "An Outlook on the Institutional Evolution of the European Union Cyber Security Apparatus," *Government Information Quarterly* 33, no. 4 (October 2016): 746, https://doi.org/10.1016/j.giq.2016.10.003.

of interoperability particular Member States will dominate the European agenda on cybersecurity, at the expense of a coordinated supranational policy response.[26]

Although literature arguing the EU lacks a coherent strategy on cybersecurity is dominant, some authors show that the EU is nonetheless striving to become a coherent security actor in the field of cyber defense. For example, Carrapico and Barrinha maintain that the EU has been moving towards the position of being a coherent actor in the field of cybersecurity over the last three decades, even though most available literature claims otherwise.[27] Coherence is especially important in the case of EU cybersecurity, because originally EU policies were highly scattered, leading to persistent problems of institutional fragmentation.[28] Carrapico and Barrinha explain that the EU clearly made efforts to consolidate their activities in the field of cybersecurity. Of the three main pillars of cybersecurity, the focus laid on cybercrime and critical information infrastructure protection. Cyber defense, although being the third pillar of the EU cybersecurity strategy, received less attention.[29]

Furthermore, the EU has explicitly articulated their ambition to become a coherent security actor, while making cybersecurity a key priority. The prioritization becomes clear from speech acts, the publication of documents such as the 2013 Cybersecurity Act and new initiatives such as the foundation of European Cybercrime Center. Alongside prioritization, the EU often articulated they are aiming for coherence in various joint frameworks.[30] Therefore, the authors conclude that the EU has been moving towards becoming a coherent security actor in the field of cybersecurity.

To summarize, this thesis thus adds to the academic debate, by analyzing to which extent the EU developed as a collective security actor in the domain of cyber defense, as the literature has not yet been provided with this perspective.

Theoretical Framework

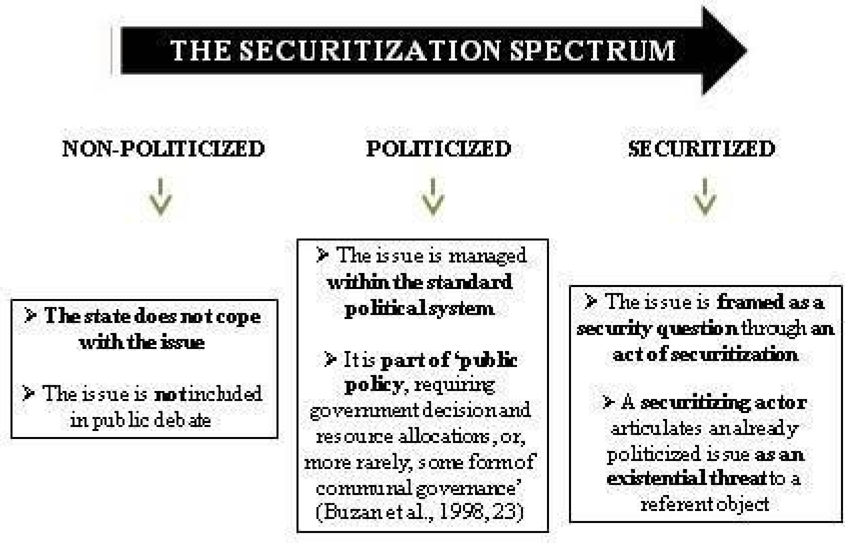
This section aims to review the existing literature on securitization theory, with a particular section dedicated to collective securitization. The theoretical framework builds on the notion of De Graaf and Zwierlein, who demonstrate that history can support the analysis of the often complex development of securitization processes. In turn, historians can profit from more recent theories of

[26] Krzysztof Feliks Sliwinski, “Moving beyond the European Union’s Weakness as a Cyber-Security Agent,” *Contemporary Security Policy* 35, no. 3 (2014): 483.
[27] Helena Carrapico and André Barrinha, “The EU as a Coherent (Cyber) Security Actor?,” *JCMS: Journal of Common Market Studies* 55, no. 6 (2017): 1254.
[28] Carrapico and Barrinha, “European Union Cyber Security as an Emerging Research and Policy Field,” 299–300.
[29] Carrapico and Barrinha, “The EU as a Coherent (Cyber) Security Actor?,” 1260.
[30] Carrapico and Barrinha, 1256; 1267.

political science and international relations.[31] Namely, studying the progression of security discourses (or political agenda setting in the security-domain) by using concepts of the social sciences can clarify the complex process that led to the process of securitization.[32]

The Copenhagen School of Securitization

Securitization theory gained ground after Buzan et al. introduced the Copenhagen School of Securitization in their authoritative book *Security: A New Framework for Analysis.* International security, they claim, is a matter of (state) survival.[33] The traditional view of securitization theory remained in the political-military domain, while Buzan et al. also recognized the economic, societal and environmental sector. In the process of securitization, a (potentially) harmful issue is presented by the securitizing actor as a threat through discourse, which justifies emergency measures which are outside of the regular political scope to counteract the threat. Therefore, the authors define a scale of political involvement, spanning from non-politicized, to politicized, to securitized. Non-politicization means there is no political involvement, while politicization involves the issue being dealt with in public policy, being part of the political agenda and being allocated resources. Securitization is explained as the more extreme version of politicization, requiring extraordinary measures outside of the regular political scope.[34] The figure below shows this process.[35]



➤ **The state does not cope with the issue**

➤ The issue is **not** included in public debate

➤ The issue is managed **within the standard political system**

➤ It is **part of 'public policy**, requiring government decision and resource allocations, or, more rarely, some form of communal governance' (Buzan et al., 1998, 23)

➤ The issue is **framed as a security question** through **an act of securitization**

➤ A **securitizing actor** articulates an already politicized issue **as an existential threat** to a referent object

[31] Beatrice de Graaf and Cornel Zwierlein, "Historicizing Security - Entering the Conspiracy Dispositive," *Historical Social Research / Historische Sozialforschung* 38, no. 1 (143) (2013): 46–48.
[32] de Graaf and Zwierlein, 50.
[33] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, Colo: Lynne Rienner Pub, 1998).
[34] Buzan, Wæver, and Wilde, 25.
[35] Alan Collins, ed., *Contemporary Security Studies*, Fourth edition (Oxford, United Kingdom ; New York, NY: Oxford University Press, 2016), 170.

Figure 1: The Securitization Spectrum

The emergency measures are to be taken by the *securitizing actor*, which in the military sector is mostly seen as the state. This is to protect the *referent object*, who is threatened by the potential harmful consequences of the *threat* and therefore is in need of protection. The *audience*, to whom the securitizing discourse is directed, is to be persuaded of the necessity of emergency measures by the securitizing actor. Only if the securitizing actor successfully convinces the audience of the security threat, the issue moves from politicization to securitization.[36] De Graaf and Zwierlein assert that securitization theory identifies security as a dynamic, communicative and intersubjective process, which relates to the historical perspective of taking the complexity of the development process into account.[37]

For this study, the Copenhagen view of securitization in the military sector remains relevant, as cyber is categorized as a new domain of war. Already in 1998, Buzan et al. recognize that supranational referent objects, such as the EU, are becoming increasingly important, although the authors focus on threats aimed at undoing the integration process by attacking collective norms.[38]

As Hansen and Nissenbaum explain, securitization theory is well-suited for evaluating threats in the cyber domain, as

> "The application of the securitisation framework to the online information space is increasingly relevant as recognition is growing that cybersecurity goes 'beyond a mere technical conception of computer security, when proponents urged that threats arising from digital technologies could have devastating social effects'".[39]

Collective Securitization

Linking the literature on the EU as a security actor and securitization theory leads to a relevant international relations theory: collective securitization. As mentioned in the introduction, this theory was proposed by Sperling and Webber in a special issue of *West European Politics* in 2019 and entails that it is possible for securitization to occur in a 'collective' setting such as the

[36] Buzan, Wæver, and Wilde, *Security*, 21–27.
[37] de Graaf and Zwierlein, "Historicizing Security - Entering the Conspiracy Dispositive," 46; 50.
[38] Buzan, Wæver, and Wilde, *Security*, 22.
[39] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53, no. 4 (2009): 1155.

EU.[40] *Collective* securitization occurs when the securitizing actor, in this case the EU, acts on behalf of other empowered actors who individually also deal with their own security concerns.[41]

This is explained by the idea that crises caused by security threats can result in consolidation of supranational (EU) policies to mitigate the crisis.[42] Many contemporary security threats, such as cybersecurity, are transnational in nature. This led states to increasingly defer parts of their sovereignty to formal intergovernmental bodies, such as NATO and the EU, leading to supranational integration within international institutions.[43] The question that is central to the collective securitization framework is to which extent the EU as a supranational actor is able to shape national understandings of what constitutes a security threat, forge policies to be implemented simultaneously by the supranational EU institutions and the Member States, and how those supranational policies affect the allocation of national resources within Member States to meet security threats defined as such.[44]

Sperling and Webber identify ‘thin’ and ‘thick’ variants of collective securitization. Within the thin variant, the supranational institution functions as a bargaining forum for negotiations between members and is thus intergovernmental in nature. The variant this thesis considers is the thick variant, where the international organization has a separate position from its members. Because the organization has autonomy, it can be classified as a securitizing actor on its own.[45] That is, even though preferences of members are considered, the decision-making power remains with the organization itself and is thus supranational.

The model of thick collective securitization is based on several assumptions. The first assumption is based on the reinforcing logics of exception and routine, which entails the necessity of a precipitating event, but the process of securitization is determined by prior experience and practice of the involved actors.[46] Second, there is an overlap (but not conflation) between the securitizing actor and the referent object. In the case of the EU this entails that the integrity of the state is not the principal referent object, but security calculations are made while reckoning with the security concerns of other Member States. According to Sperling and Webber, such calculations are channeled by well-developed rules and norms vested in the EU.[47] The third assumption is the concept of recursive interaction, in which there is a continuous bargaining between the securitizing

[40] Sperling and Webber, “The European Union,” 228.
[41] Sperling and Webber, 236.
[42] Sperling and Webber, 228.
[43] Sperling and Webber, 233.
[44] Sperling and Webber, 232.
[45] Sperling and Webber, 236–37.
[46] Sperling and Webber, 240.
[47] Sperling and Webber, 241.

move (by the EU) and the audience response (of the Member States) on the threat and mitigating measures.[48] The last assumption is the continuation of securitization beyond acts of speech into acts of policy.[49]

The securitization process is divided into six phases, which are outlined in the figure below.

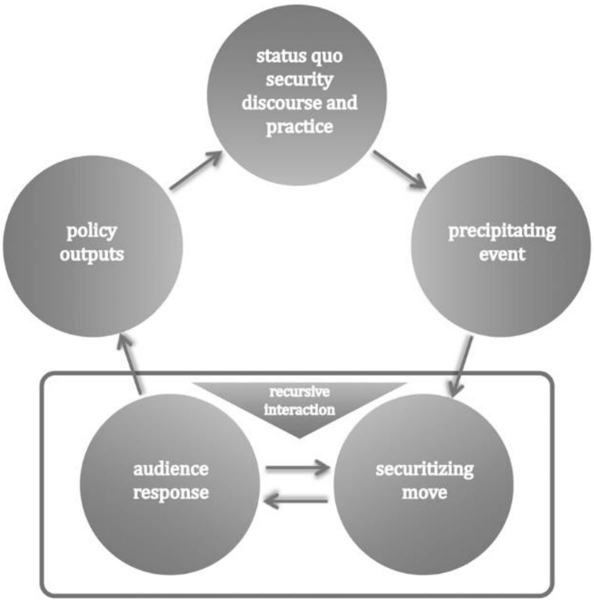


Figure 2. A Model of Collective Securitization.[50]

The first stage represents the status quo, where politicizing discourses may be present. In the second stage, an event or a series of events trigger the international organization to classify the threat as harmful by initiating a security discourse. Then, in the third and fourth stage, a process of recursive interaction takes place to move from politicization to securitization of the issue. Within the collective securitization setting of the EU, the audience is in essence composed of the 27 EU Member States. As the Member States influence policy and possess veto power, the policy responses and mitigating measures the EU is taking are repeatedly negotiated. This bargaining process within the international organization between the securitizing actor and its audience in which responses are aggravated is defined as recursive interaction.[51] In the fifth stage, policy is formulated and executed. In the EU, these policies are primarily supranational in nature, but can have profound effects on domestic policies too.[52] The sixth and final stage conflates with the first stage and represents a new status quo, in which the securitization is accomplished and forms the basis for future processes of securitization of new threats.

[48] Sperling and Webber, 242–43.
[49] Sperling and Webber, 246.
[50] Sperling and Webber, 246.
[51] Sperling and Webber, 243.
[52] Sperling and Webber, 247.

Methodology

To find a methodologically sound answer to the research question, this thesis proposes a mixed method approach. First, core concepts within the 2013 Cybersecurity Act, 2014 Cyber Defense Policy Framework, the 2018 revision of the Cyber Defense Policy Framework and the 2019 revision of the Cybersecurity Act are defined by using a targeted sentiment analysis in RStudio. The main part of the analysis is devoted to a critical discourse analysis.

These four documents are chosen as they are meaningful and extensive snapshots of EU policy during the assessed period. The Cybersecurity Acts of 2013 and 2019 are published by the Commission, which is a supranational organization. The Cyber Defense Policy Frameworks of 2014 and 2018 serve as an extension of the Cybersecurity Acts, but are published by the intergovernmental Council of the European Union. Yet, as the documents are linked in this manner this thesis assesses both to conclude to which extent each publication shows signs of collective securitization.

A targeted sentiment analysis reveals the tone of voice of a document, tailored to specific topics. For EU documents this is especially relevant, as much attention is devoted to procedures and formulations may be fuzzy. Through a targeted sentiment analysis this effect can be minimized, as relevant words are coded in their direct context. This gives a better overview of the direction of the text, which in turn provides a clearer and more exhaustive basis for the main part of the analysis: the critical discourse analysis. As such, the targeted sentiment analysis can pinpoint to which phase of the collective security framework a document belongs. For example, if a document shows considerable attention for threat identification, it points towards the phase of recursive interaction. If instead threat mitigation is emphasized, policy outputs are more important. This signals the phase of policy outputs.

To use a targeted sentiment analysis, first the most prevalent words are counted in each text, whereafter a sentiment score is constructed to determine the valence of a certain text. To make the sentiment analysis targeted to specific topics, it is necessary to define text strings consisting of key words. These text strings are defined according to collective securitization theory. The first text string with the topic ‘threat identification’ is based on the securitizing move (phase 3 and 4) and contains words such as incidents, risks or threats. The second text string has the topic ‘threat mitigation’ and is based on policy outputs (phase 5). This text string contains words such as objectives or policy. The third text string focuses on the collective component of collective securitization theory, and contains words such as cooperation, together and international. These text strings are applied to all documents in the same manner to allow for comparison. The number of occurrences in each text signals the importance of each topic. If threat identification occurs more often than threat mitigation, the EU is located in stages three and four of recursive interaction of the collective security cycle. Conversely, if threat mitigation is more important, this indicates the fifth stage of policy outputs.

The text strings consisting of the key words within the three main topics are put into code and form the basis for the targeted sentiment analysis. The result reveals the sentiment score for each topic. The targeted sentiment score thus shows in which context the main topic is presented in the text. If the sentiment score is mostly positive, this signals a positive attitude of the EU towards the topic discussed. Because the analysis is specifically directed at a certain topic, the analysis is targeted.

The main part of the analysis is devoted to a qualitative critical discourse analysis, in which the findings from the targeted sentiment analysis are evaluated according to the method of critical discourse analysis as proposed by Fairclough.[53] Fairclough argued that the use of language is central when examining societal structures, as discourses contribute to the achievement of political continuity or change. In turn, this is reflected in policy documents.[54] With this method, the language in the policy documents is critically evaluated in order to identify the underlying meaning of the policy.[55]

The main topics identified with the targeted sentiment analysis form the basis of the critical discourse analysis, putting the quantitative findings into perspective. Revealing the underlying meaning contributes to the understanding of securitization of cyber defense efforts, because securitizing discourses are an important part of the securitization process, as outlined in the theoretical framework. The aim of the critical discourse analysis is to uncover rhetoric contributing to processes of collective securitization in order to determine to which extent the EU developed as a collective cybersecurity actor between the period of 2013-2019. As becomes clear from the theoretical framework, an actor can be classified as a collective security actor if decisions are taken at the supranational level instead of the intergovernmental level.[56] Accordingly, problems of institutional fragmentation should not occur, as this inhibits supranational decision-making.

Secondary literature on the EU and cyber defense of each period supports this mixed method analysis. By combining the findings of both methods, it is assessed to which extent the EU developed as a collective cybersecurity actor. In the concluding section, the findings of the analysis are evaluated to contrast and compare the findings and formulate an overarching answer to the research

[53] Norman Fairclough, "Critical Discourse Analysis," in *The Routledge Handbook of Discourse Analysis* (Routledge, 2013), 9–20.
[54] Norman Fairclough, *Critical Discourse Analysis: The Critical Study of Language* (Routledge, 2013), 30.
[55] Fairclough, "Critical Discourse Analysis," 2013.
[56] Sperling and Webber, "The European Union," 236–37.

question. Additionally, limitations of this study are considered and suggestions for further research are made.

Primary sources

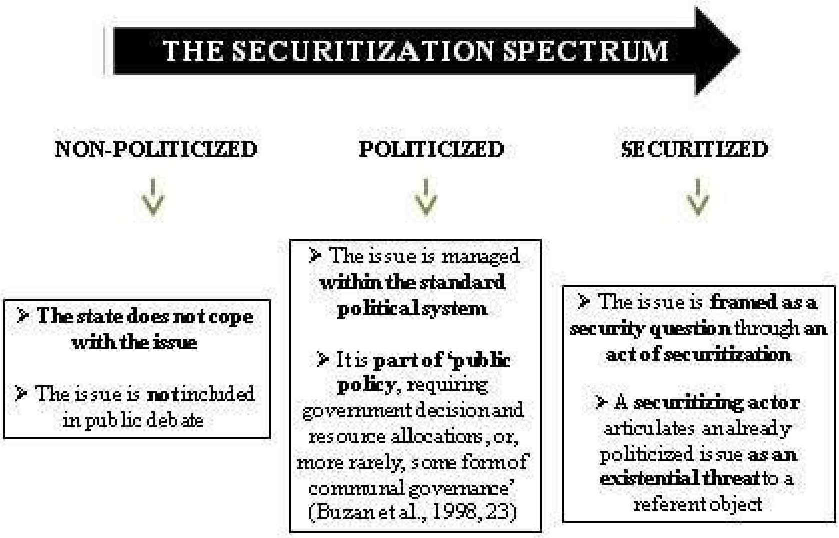
This research combines the disciplines of international relations and history, and therefore includes analysis of primary sources. As mentioned, the key primary sources analyzed are the four official EU documents examined in each section of the analysis. As outlined in the introduction, these sources are the 2013 Cybersecurity Act and the Cyber Defense Policy Framework of 2014 in the first section, and the 2018 update to the Cyber Defense Policy Framework and the 2019 revision of the Cybersecurity Act. These primary sources are chosen because they all signal meaningful steps towards building a higher resilience against cyber threats, which indicates signs of a collective security actor.

Furthermore, all documents are officially released by the EU, which allows for a collective securitization perspective with the EU as the collective security actor. Additionally, chapter three contains a section dedicated to societal developments in the period from 2014-2018, which is a historical turning point. All primary sources are listed in the bibliography under the header *Primary sources.* Due to the mixed method design of this research, a relatively modest amount of sources is analyzed. Nonetheless, each source signifies a vital point in the development of the EU as a security actor in the cyber defense realm. In addition, each source is thoroughly scrutinized and supported by other primary sources, which allows for a well-rounded answer to the research question.

Chapter 1: Historical background to cybersecurity as a domain of war, and of the EU as a defense actor

This chapter provides an historical overview of cybersecurity efforts from the 1990s until the formulation and implementation of the 2013 Cybersecurity Act. It does so by answering the sub-research question: *In what way has cyber defense developed from being non-politicized in the 1990s to being securitized in 2013?*

By providing a historical overview of discourses in the domain of cybersecurity, it is assessed in what way cyber developed into the fifth domain of war and the development of the EU as a defense actor as such. Academic literature on this topic is ubiquitous, yet a securitization perspective has not yet been applied to the processes leading up to the formulation of the 2013 Cybersecurity Act. The structure follows the logic of the securitization spectrum as explained in the theoretical framework of this thesis.[57]



➢ **The state does not cope with the issue**

➢ The issue is **not** included in public debate

➢ The issue is managed **within the standard political system**

➢ It is **part of 'public policy**, requiring government decision and resource allocations, or, more rarely, some form of communal governance' (Buzan et al., 1998, 23)

➢ The issue is **framed as a security question** through **an act of securitization**

➢ A **securitizing actor** articulates an already politicized issue **as an existential threat** to a referent object

Figure 2: The Securitization Spectrum

The three sections of this chapter thus are non-politicization of cybersecurity, politicization of cybersecurity and securitization of cybersecurity.

Non-politicization between 1990s - 2004

Literature on the development of the internet centers on the developments in the US, which is why this section mostly focuses on US-based literature. Driven by cold war tensions between the US and the USSR during the 1960s, the US Department of Defense established the first step towards the

[57] Collins, *Contemporary Security Studies*, 170.

internet: the Advanced Research Projects Agency (ARPA). [58] ARPA was aimed at promoting research that would ensure the US would have technological dominance over the USSR.[59] During the first decades of development, the internet was mostly used by researchers, developers and US federal agencies to allow for information exchange.[60] However, everyone with the means to access a computer could access the information sent over the ARPANET.

In 1980, the groundbreaking defense standard TCP/IP was implemented, which allowed the US Department of Defense to share information over the then dominant ARPANET, as information could now be protected. As a consequence, this led directly to the separation between military (MILNET) and non-military communities (ARPANET) on the internet.[61] Within MILNET, a higher standard of information security was implemented. Therefore, the commercial phase of the internet started in 1984. During this period, the first international connections between the US, the United Kingdom and France were made, which led to rapid network expansions during the following year.[62]

Security concerns arose when the amount of network connections increased exponentially in the late 1980s and early 1990s. These concerns were a result of the open communication principle of the ARPANET system, which was founded on the basis of free and open information exchange. Information thus remained relatively unprotected. Open information exchange contributed to the rapid development of the technology, but also led to risk of critical information leakages. That is, on the very premise of the system, it proved difficult up until 1980 to shield any information from any individual with access to ARPA. After the implementation of TCP/IP security standards rose, but risks of information leaks were not fully solved.[63]

In 1994, the National Research Council published an extensive report titled *Realizing the Information Future: The Internet and Beyond*.[64] The main issues discussed are intellectual property rights, ethics, pricing, education, architecture and regulation. When discussing the possibilities of attacks on the internet, the report states: “Although attacks are not a common problem on the Internet, their occurrence must be anticipated”.[65] Information security is only briefly mentioned, and the only possible solution presented is encryption. The problem is then shifted to the protection of

[58] The Advanced Research Projects Agency (ARPA) changed its name to Defense Advanced Research Projects Agency (DARPA) in 1971, then back to ARPA in 1993, and back to DARPA in 1996. This thesis consistently uses the ARPA nomination.

[59] Raphael Cohen-Almagor, “Internet History,” in *Moral, Ethical, and Social Dilemmas in the Age of Technology: Theories and Practice* (IGI Global, 2013), 46.

[60] Barry M. Leiner et al., “A Brief History of the Internet,” *ACM SIGCOMM Computer Communication Review* 39, no. 5 (2009): 22–31.

[61] Leiner et al., 26.

[62] Cohen-Almagor, “Internet History,” 52.

[63] Leiner et al., “A Brief History of the Internet.”

[64] *Realizing the Information Future: The Internet and Beyond* (Washington, D.C: National Academy Press, 1994).

[65] *Realizing the Information Future*, 81.

the encryption key, which often also needs to be sent to the receiver over the internet.[66] The possibility of a state actor using the network to carry out an attack on another state was still an unknown phenomenon in this report.

Academic literature on this period supports this lack of attention for security measures. In general, most literature on the internet of the 1990s is aimed at exploring the possibilities and future scenarios of the technology.[67] Only a few articles on the possible perils of cyber warfare were published in 2000, and are mostly aimed at explaining the concept.[68] In 2002, Lewis placed cyber warfare in a historical context of attacks against infrastructure, claiming that attacks in the cyber domain can have profound consequences on infrastructure.[69] However, Lewis asserts that ‘cyber weapons seem to be of limited value in attacking national power or intimidating citizens’.[70] Therefore, the possibility of cyber warfare becoming a security threat was not considered during the early 2000s.

Even though cyber defense was not yet a salient topic on the political agenda, the EU still attributed much attention to supranational defense collaboration during the 1980s and 1990s. In this period, renewed efforts of deeper and wider integration were undertaken after a period of Eurosclerosis during the 1970s in which Euroscepticism halted integration efforts.[71] For example, the Single European Act of 1986 articulated the aim of establishing a single market by 1992, and the Maastricht Treaty of 1992 created a foundation for the European Union. Therefore, the societal and political developments during this period are geared towards deeper integration, also in the field of defense collaboration. This is outlined by Paulo, who argues that even after the failure of the European Defense Community, defense integration still occurred and became especially visible from 1999 onwards.[72] In that year a letter of intent was signed to establish a Common Security and Defense Policy (CSDP) as an element of the Common Foreign and Security Policy (CFSP). The CSDP sets the policy framework for defense coordination and cooperation between Member States,

[66] *Realizing the Information Future*, 82.
[67] For example, see: Jörn Kleinert and Daniel Piazolo, “Governing the Cyber Space,” in *The New Economy and Economic Growth in Europe and the US*, ed. David B. Audretsch and Paul J. J. Welfens, American and European Economic and Political Studies (Berlin, Heidelberg: Springer, 2002), 271–92, https://doi.org/10.1007/978-3-540-24826-2_14.
[68] For example, see: Lionel D. Alford, “Cyber Warfare: Protecting Military Systems” (AIR FORCE MATERIEL COMMAND WRIGHT-PATTERSON AFB OH, 2000); Jean Kumagai, “The Web as Weapon [Cyber Warfare],” *IEEE Spectrum* 38, no. 1 (2001): 118–21; Don Stauffer, “Electronic Warfare: Battles without Bloodshed,” *The Futurist* 34, no. 1 (2000): 23; Christopher Bellamy, “What Is Information Warfare?,” in *Managing the Revolution in Military Affairs* (Springer, 2001), 56–75.
[69] James Andrew Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats* (Center for Strategic & International Studies Washington, DC, 2002), 2.
[70] Lewis, 10.
[71] Herbert Giersch, “Eurosclerosis” (Kieler Diskussionsbeitrage, 1985).
[72] Jorge Silva Paulo, “The European Defense Sector and EU Integration,” *Connections* 8, no. 1 (2008): 11.

although still intergovernmental in nature.[73] The CSDP is focused on defense and crisis management, and draws on military and civilian assets which are provided by Member States. Since cyber has only been officially classified as a domain of war from 2016 onwards, cyber defense measures were not included in the CDSP during the 1990s and early 2000s.

All in all, until the early 2000s the issue of cybersecurity and defense did not seem to be included in the international public debate. Even though the EU integrated defense cooperation and coordination in other fields, cyber defense did not reach the political agenda. Therefore, this section concludes that during the 1990s and early 2000s, cyber defense remained non-politicized, as both the EU and the US did not classify cyber-attacks as a (security) issue and did not take security measures as such.

Politicization from 2004 - 2012

From 2004 onwards, cybersecurity received more attention from the public and the EU. The British company mi2g, in possession of the largest digital risk database of the time, identifies the year 2004 as the year of the 'Global Malware Epidemic', asserting that the year is set to become the 'worst year on record for malware variants'.[74] In total, mi2g estimates that nearly 115 million computers around 200 countries experienced infection with malware during the year. Of those, 11 million were believed to function as 'permanently infected zombies', unknowingly used by sophisticated criminals to send out spam, carry out Distributed Denial of Service (DDoS) attacks or disseminate new malware. According to mi2g, the risk was rapidly expanding, as the then available antivirus toolkits, firewalls or intrusion detection systems were unable to deal with malware spread by hyperlink, the most common form in 2004.[75]

In 2004, MyDoom became the fastest-spreading email virus ever, beating the well-known ILOVEYOU virus, a record that has not been surpassed even in 2022.[76] MyDoom was aimed at computers operating a Microsoft Windows system, and when infected, the attacker would get full access to the infected computer system.[77] Overall, at least 500.000 computers were infected.

[73] "Common Security and Defence Policy | Fact Sheets on the European Union | European Parliament," accessed October 20, 2022, https://www.europarl.europa.eu/factsheets/en/sheet/159/common-security-and-defence-policy.

[74] mi2g, "2004: Year of the Global Malware Epidemic - Top Ten Lessons," November 21, 2004, http://mi2g.com/.

[75] mi2g.

[76] "CNN.Com - Security Firm: MyDoom Worm Fastest yet - Jan. 28, 2004," accessed November 14, 2022, http://edition.cnn.com/2004/TECH/internet/01/28/mydoom.spreadwed/.

[77] "Win32/Mydoom Threat Description - Microsoft Security Intelligence," accessed November 14, 2022, https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Mydoom.

To counteract the exponential rise of malware, ENISA[78] (the EU Agency for Cybersecurity) was established in the same year.[79] The aim of ENISA was 'to create a platform for a culture of network and information security in Europe, in order to facilitate stakeholders, including EU Institutions and Member States, to promote secure solutions in using eNetworks and eInformation'.[80] Initially, ENISA's essential tasks were raising awareness and promotion of best practices. As security breaches and malware already caused serious financial damage, the EU expected malware to have more harmful consequences such as the obstruction to essential services in the future. In 2004, cross-border cooperation was not yet in place, but was deemed necessary to counteract security breaches. Therefore, with the foundation of ENISA the EU shows the issue of security in the cyber domain is becoming a pressing problem.[81]

Like the EU, private actors such as Microsoft shifted attention towards identification and combating of cyber threats. Following the MyDoom attack, Microsoft has been publishing yearly digital defense reports from 2005 onwards, in which it is outlined how online safety and the threat landscape has changed.[82] Microsoft shows that the issue was not only discussed in political spheres, but also gained importance in the public debate.

However, some authors argue the initial mandate of ENISA was insignificant and not fit to actually address threats in cybersecurity. More specifically, during the mid-2000s the mandate of ENISA corresponded with the soft power approach of the EU, to harmonize national cybersecurity strategies through facilitation of cooperation and diffusion of information on a common platform.[83] Accordingly, the EU thus attempted to address the problem, but was not yet capable of taking measures outside of the regular political scope.

In April 2007, the first large-scale cyberattack on a country, Estonia, marked the beginning of cyber warfare being applied by a hostile state. Allegedly, Russia retaliated against Estonia after the country decided to move a Soviet statute commemorating the Soviet liberation from Nazi-Germany to a less prominent location in Talinn.[84] For several weeks, large-scale cyber-attacks paralyzed the Estonian society. During the attacks, cash machines and online banking services were frequently

[78] Officially, ENISA is an abbreviation of the European Union Agency for Cybersecurity. However, the organization always is mentioned as ENISA. This thesis follows this general provision.

[79] "Regulation (EC) No 460/2004 of the European Parliament and o... - EUR-Lex," accessed October 20, 2022, https://eur-lex.europa.eu/EN/legal-content/summary/european-network-and-information-security-agency-enisa.html.

[80] Konstantinos Voudouris, *The European Networks and Information Security Agency – ENISA*, 2005, 2.

[81] "Regulation (EC) No 460/2004 of the European Parliament and o... - EUR-Lex."

[82] "Microsoft Digital Defense Report and Security Intelligence Reports," accessed November 7, 2022, https://www.microsoft.com/en-us/security/business/security-intelligence-report.

[83] Louis Brun and Rocco Bellanova, "The Role of the European Union Agency for Network and Information Security (ENISA) in the Governance Strategies of European Cybersecurity," *Université Catholique de Louvain*, 2018, 8.

[84] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 50–51.

unavailable, government officials could not communicate over email and media outlets were unable to deliver the news.[85] The EU offered that ENISA would perform expert technical assessments of the developing situation. However, the Estonian Computer Emergency Response Team (CERT) not only required bilateral assistance from Israel, Slovenia, Finland and German teams, but also needed NATO support to restore regular network operations.[86] Thus, the EU was not able to defend one of the Member States and could not act as a fully functioning collective cybersecurity actor.

In the following year, the introduction of the first smartphone simultaneously accelerated network connections but also heightened concerns about cybersecurity. Due to the ever more pressing need for international cooperation in the cybersecurity field, ENISA's mandate was extended until 2012.[87]

All in all, during the years between 2004 and 2012, cybersecurity developed into a deeply pressing problem. However, even though the problem was acknowledged, the EU remained unable to fully counteract the fast-developing risks of cyber warfare, as shown by the attacks on Estonia in 2007. Therefore, politicization of cybersecurity was in place during this period, but the developments during the period from 2004 until 2012 cannot be classified as securitized. To solve this institutional gridlock, the EU intended to adopt a Cybersecurity Act in 2013, to develop into a meaningful security actor within the domain of cybersecurity.

Securitization from 2012 onwards

As mentioned in the previous section, the political deliberations of the EU started to intensify. According to Akamai, a company with one of the largest globally distributed networks at the time, incidents of cyber warfare surged in 2012. Clients of the company reported triple the amount of DDoS attacks compared to 2011. The company states that DDoS attacks became the 'weapon of choice' for both political activists and criminals, and potentially even nation-states. Akamai notices that from the observed attack traffic, a substantial share originates in China, possibly signaling state-led attacks.[88]

Cyber-attacks thus became increasingly of political nature, which is also addressed by the EU. This period is marked by recursive interaction, in which a bargaining process between the

[85] "How a Cyber Attack Transformed Estonia," *BBC News*, April 27, 2017, sec. Europe, https://www.bbc.com/news/39655415.
[86] Herzog, "Revisiting the Estonian Cyber Attacks," 54.
[87] "Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards Its Duration (Text with EEA Relevance)," 293 OJ L § (2008), 100, http://data.europa.eu/eli/reg/2008/1007/oj/eng.
[88] Shara Tibken, "Cyberattacks Triple in 2012, Akamai Says," CNET, accessed November 15, 2022, https://www.cnet.com/news/privacy/cyberattacks-triple-in-2012-akamai-says/.

securitizing actor (the EU) and its audience (the Member States) took place. This process is typical for issues moving from being politicized to being securitized.

For instance, in November 2012 the implementation of the CSDP was discussed, including a section dedicated to a report on Cyber Security and Defense.[89] In this report, it is stated that 'the EU and its Member States have become crucially reliant on safe cyberspace' and that 'a majority of highly visible and disruptive cyber incidents are now of a politically motivated nature'.[90] In this report, the EU acknowledges the action on the field of both network and information security, and cybercrime, but explains that the EU 'yet lacks any concrete plan at the level of security and defence'. Therefore, the report proposes measures needed to counteract and neutralize the established level of threat, such as a global and coordinated response at the supranational EU level by formulating a comprehensive cybersecurity strategy. Especially cyber defense receives substantial attention and should be made an active capability of CDSP, which is notable.

Defense measures are especially seen as a topic that should be dealt with mostly on the national level, as it is paramount to national sovereignty. Originally, the CDSP was purposefully located under Pillar Two of the Maastricht treaty. This pillar entails the intergovernmental cooperation method, and deals with the Common Foreign and Security Policy. Therefore, within defense matters the principle of intergovernmentalism remained crucial.[91] Formally, decisions within CDSP are taken by the 27 Foreign Ministers, or by the Heads of State in the European Council.[92]

In spite of the usual intergovernmental approach, the EU is proposing a global, supranational approach, which is thus outside of the ordinary political scope. This signals securitization of cyber warfare, as the EU is identifying cyber incidents as an existential threat to the audience. In this case, the audience can both be identified as being the Member States, as well as their citizens. Within this discourse, the first traces of collective securitization are already apparent.

In 2013, ENISA received a permanent mandate, while several other supranational institutions were founded. For cybercrime, the European Cybercrime Center was established in 2013 to specifically deal with cybercrime.[93] Cyber defense did, however, not receive a specialized organization, but the issue started to gain ground in policies of the European Defense Agency and

[89] "Debates - Implementation of the Common Security and Defence Policy - EU Mutual Defence and Solidarity Clauses: Political and Operational Dimensions - Cyber Security and Defence - Role of the Common Security and Defence Policy in Cases of Climate-Driven Crises and Natural Disasters (Debate) - Wednesday, 21 November 2012," accessed October 28, 2022, https://www.europarl.europa.eu/doceo/document/CRE-7-2012-11-21-ITM-013_EN.html.

[90] Parliament. Regulation 2012/2096(INI). paragraph A and C

[91] Jolyon Howorth, "Decision-Making in Security and Defense Policy: Towards Supranational Inter-Governmentalism?," *Cooperation and Conflict* 47, no. 4 (December 1, 2012): 434, https://doi.org/10.1177/0010836712462770.

[92] Howorth, 435.

[93] "European Cybercrime Centre - EC3," Europol, accessed October 27, 2022, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

was seen as a top priority as of 2012.[94] Therefore, in 2013 a multiplicity of actors within the EU dealing with cyber issues arose, as was also outlined by Carrapico and Barrinha.[95]

All in all, from 2012 onwards the issue of cybersecurity moved from being politicized towards being securitized through the process of recursive interaction. In this context, the EU adopted the 2013 Cybersecurity Act. In 2014, the Cyber Defense Policy Framework was published as the implementation tool in the field of cyber defense. The analysis section of this thesis evaluates these documents to identify if the EU successfully capitalized on the securitization of the issue and moved towards a phase of implemented policy outputs. If the decisions are made on the supranational level, the EU can be classified as a collective cybersecurity actor.

[94] European Parliament. Regulation 2012/2096(INI). paragraph Q
[95] Carrapico and Barrinha, “The EU as a Coherent (Cyber) Security Actor?”

Chapter 2: Initial securitization of cyber defense in 2013 and 2014

This chapter analyzes the 2013 Cybersecurity Act and the 2014 Cyber Defense Policy Framework. It does so by answering the sub research question: *In what way did the EU articulate discourses of securitization in the 2013 Cybersecurity Act and the 2014 Cyber Defense Policy Framework?* This analysis builds on the historical overview provided by the previous chapter, and thoroughly assesses if the EU has developed as a coherent security actor in the field of cybersecurity. First, the data is quantitatively explored through a targeted sentiment analysis which provides a starting point for critical discourse analysis, in which the documents are contextualized and explained. In the sub-conclusion, it is concluded that even though the EU shows an increasing desire to act as a supranational collective security actor, it still operates on the principle of intergovernmentalism.

2013 Cybersecurity Act

The 2013 Cybersecurity Act was the first official regulation in which cybersecurity on the European level was streamlined. As explained in the previous chapter, this document marked the initial securitization of the issue, moving towards the fifth stage of the collective securitization framework: policy formulation and output. This section explores this document quantitatively to pave the way for the critical discourse analysis, in which it is assessed to which extent the EU shows signs of a collective security actor.

Targeted Sentiment Analysis

The document is first loaded into RStudio and is purged for numbers, symbols, punctuation and stop words, as these are not relevant for the analysis. Furthermore, words clouding the analysis such as European, Union, Member and States are removed from the document. Among the most occurring words then remain Agency, Information, Security, Network and Management. For a visual overview of the most occurring words, see figure 3.

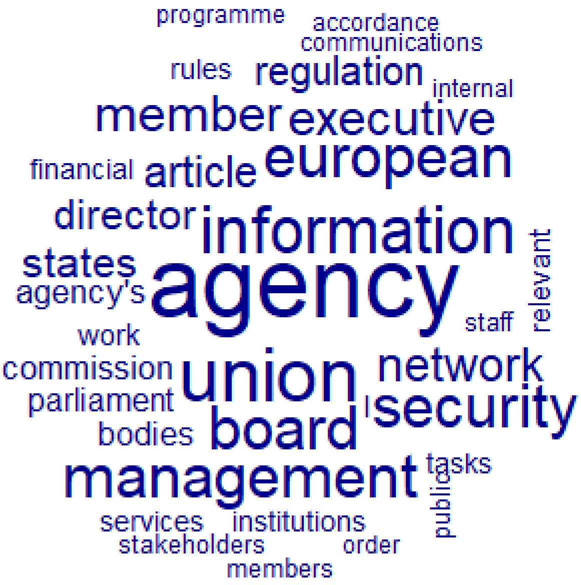


Figure 3: Wordcloud 2013 Cybersecurity Act

In order to formulate text strings, three main topics are identified to target for topics signaling collective securitization. The first two topics are structured along the phases of the securitization process. The first topic is threat identification, which corresponds with phase 3 and 4: the securitizing move. The second topic is the mitigation of these threats, corresponding with phase 5: policy outputs. The third topic adds a collective perspective to the securitization process and entails international cooperation and integration. By using these topics, the analysis is able to trace in which stage of the collective securitization the EU falls on the basis of these documents.

Threat identification. The text string evaluating the securitizing discourse consists of the words Incidents, Threats, Attacks, Risk, Defence[96] and Cyber. The targeted sentiment analysis returns a sentiment score of 66. This score is the amount of times these words were used in a positive context (113) minus the amount of times they were used in a negative context (47). Even though the words are more often used in a positive context, a substantial amount of times the words occur in negatively coded sentences. This text string encompasses by far the least occurrences in the text, which shows that the EU is moving from the recursive interaction phase towards the threat mitigation phase of collective securitization.

Threat mitigation. The next text string consists of the words Objectives, Solution, Policy, Security, Protect and the Agency. Here, the targeted sentiment score is overwhelmingly positive with 306. That is, 374 times these words were used in a positive context, while 68 times they occurred in a

[96] This thesis follows American spelling. However, the published EU documents are in British spelling, therefore the code follows British spelling.

negatively coded context. This signals the EU beliefs in the competence of mitigating cyber threats, but still recognizes obstacles.

Supranational cooperation. The last text string is expressed by the words Cooperation, International, NATO, Together, Facili(tate)/(ting), EU and Member States. This text string encompasses by far the most occurrences in the text, and receives a targeted sentiment score of 287. In 374 cases, these words were used in a positive context, versus 77 negatively coded connotations. Compared to threat identification, this score shows the EU is clearly focusing on the collective aspect within the policy framework. However, the EU is not fully dedicating attention to collectively tackling cyber threats, shown by the relatively significant negative score. This can indicate a more intergovernmental approach, as the EU is not fully committing to a supranational strategy.

The document as a whole receives a mostly positive sentiment score with 133 negatively coded words and 639 positively coded words. The EU thus seems to be mostly positive about the possibilities of tackling the issue.

This phenomenon can be explained through the theory of collective securitization. That is, within a collective security framework, the audience the securitizing discourse is directed to consists of the Member States. The EU, as the security actor, needs to act on the behalf of the other empowered actors. Therefore, it is crucial that all Member States remain loyal to the mandate of the EU. By focusing on the possibility of collectively tackling the issue, the EU is able to forge policies to be implemented simultaneously by the supranational EU institutions and the Member States. If the issue is presented as a direct threat, there is a substantial risk that Member States would move away from a collective approach and formulate their own national policies. This is due to the more bureaucratic nature of the EU as a supranational institution: policy formulation and implementation inherently is a more time-consuming process when compared to national policy making. It is, however, in the interest of the EU to remain the main security actor in the field to expand their mandate as a collective security actor. The positive discourse can thus be classified as an example of how the EU is striving to become a coherent security actor. As such, the approach of positively presenting the opportunities of tackling the threat, instead using a more directly articulated securitizing discourse can be explained.

In general, the targeted sentiment analysis shows that the document is predominantly focused on threat mitigation and collectively tackling the issue of cyber threats. Threat identification is becoming less relevant however. All topics have a considerable positive sentiment score, which can signal a confident attitude of the EU on the topic. The following part of the analysis interprets these quantitative results in a qualitative manner.

Critical Discourse Analysis

The main concepts identified by the targeted sentiment analysis form the basis for the critical discourse analysis. The aim of this section is to delve deeper into the three topics and provide context to the previous section. Additionally, it is assessed to which extent the information presented by the EU can be explained by the collective security framework as outlined in the theoretical framework.

Discourse of threat identification. In the second section of the preamble, the EU asserts that 'the threat landscape is continuously changing and security incidents can undermine the trust of users'.[97] This is an example of a negative occurrence, which arises already in the very beginning of the document. By classifying the threat as harmful to European citizens, the EU is actively using securitizing discourse. Contrarily, positive discourse is also used, to showcase the necessity and possibilities of policy on the EU level. An example thereof is found in section 52, in which the 'expected evolution' of the EU on network and information security is mentioned, as the 'threat landscape is continually changing'.[98] The positive outlook the EU allocates to a changing threat landscape is a sign of collective securitization, as the EU is positively presenting the opportunities of what otherwise would be regarded as a direct threat.

Discourse of threat mitigation. In most sections, the objectives of ENISA are outlined. In general, ENISA is expected to provide relevant expertise and promote best practices on both Union level as well as to Member States. The objectives are outlined as maintaining a high level of expertise, assisting Union bodies in network and information security, and assisting both the Union as well as the Member States specifically to 'enhance their capability to prevent, detect and respond to network and information security problems and incidents'.[99] In sentences such as the previous, the EU clearly mentions problems and incidents, but allocates a positive connotation to problems by stating the objectives of ENISA. Through the tasks set out in Article 3, which are supporting the development of Union policy and law, supporting capacity building, supporting cooperation between public bodies, and promoting international cooperation, ENISA is expected to mitigate the threats.

Discourse of supranational cooperation. In general, the 2013 Cybersecurity Act strives for more cooperation to combat cyber threats. However, this document shows that the EU still mostly operates on an intergovernmental principle. In several instances, the efforts of the EU institutions are categorized as separate from the efforts of the Member States. For example, ENISA is asked to assist the Commission, but also 'where relevant, the Member States'.[100] Furthermore, one of ENISA's

[97] Parliament and Council, Cybersecurity Act 2013, paragraph 2
[98] Parliament and Council, Cybersecurity Act 2013, paragraph 52
[99] Parliament and Council, Cybersecurity Act 2013, Art. 2
[100] Parliament and Council, Cybersecurity Act 2013, paragraph 21 and 22

main tasks is facilitating cooperation between the 'independent authorities'[101] or 'public bodies'[102] of the Member States.

Moreover, it is carefully explained that ENISA should adhere to the principles of subsidiarity and proportionality.[103] Proportionality entails that policy measures proposed by the EU may not go beyond what is necessary to achieve the objectives set by the regulation in question. Subsidiarity is in this document explained as 'ensuring an appropriate degree of coordination between the Member States'. However, the principle of subsidiarity is defined by article 5 of the Treaty on the European Union (TEU) in the way that the Union may only act insofar the proposed action cannot be sufficiently achieved by the Member States.[104] This entails that policy options should be, to the extent that is possible, implemented locally or nationally before more invasive options on an supranational level are imposed. The EU thus only holds the competence to impose power when policy issues cannot be locally or nationally resolved. Since the main function of ENISA is providing a common platform for information exchange between Member States and the promotion of best practices and by functioning as a central center of expertise, it is logical that these tasks cannot be carried out on the national level. Thus far, the mandate does not allow ENISA nor the EU as such to function as a supranational decision-making power, which was also argued by Brun and Bellanova.[105]

However, the EU does show its attempts to move from an intergovernmental approach towards a supranational approach. For instance, the EU upholds that there is a 'need for closer international cooperation to improve security standards'.[106] Furthermore, it is explained that 'the heterogeneous application of technical requirements can lead to inefficiencies and create obstacles to the international market.' To overcome this, the EU proposes that ENISA becomes a center of expertise, functioning at the EU level.

Yet, the document states that within ENISA's Management Board, each Member State will have one representative. In turn, the Commission only sends two representatives in total.[107] Therefore, the balance within the Management Board is severely shifted to the representatives of Member States, which in total occupy 27 seats. However, the presence of two Commission

[101] Parliament and Council, Cybersecurity Act 2013, paragraph 26

[102] Parliament and Council, Cybersecurity Act 2013, paragraph 30

[103] Parliament and Council, Cybersecurity Act 2013, paragraph 37

[104] "Art. 5 Treaty on European Union - (Ex Article 5 TEC)," accessed November 21, 2022, https://lexparency.org/eu/TEU/ART_5/.

[105] Brun and Bellanova, "The Role of the European Union Agency for Network and Information Security (ENISA) in the Governance Strategies of European Cybersecurity," 8.

[106] Parliament and Council, Cybersecurity Act 2013, paragraph 35

[107] Parliament and Council, Cybersecurity Act 2013, Art. 6.1

representatives does signal a move towards a more supranational management, even though the organization remains mostly intergovernmental at the point of founding.

Nonetheless, the necessity of supranational actions outside of facilitation of information exchange and the promotion of best practices is not sufficiently explained in this document. Actions such as the formulation of a central supranational policy with EU decision making power are not justified. If the EU would classify as a collective security actor, it would consider preferences of Member States, but the decision-making power would remain with the organization itself. Even though discourses moving to further supranational actions are sporadically mentioned, actions moving beyond facilitating the international dialogue are not yet in place. Thus, on the basis of the 2013 Cybersecurity Act, the EU cannot be classified as a fully functioning collective security actor.

In sum, the 2013 Cybersecurity Act shows the EU is still operating on the verge between showing attempts to become a supranational security actor and remaining loyal to the principle of intergovernmentalism. Therefore, on the basis of discourses of threat identification, threat mitigation and international cooperation, this section concludes the EU is making small progress towards becoming a collective security actor but cannot be classified as such yet. The next section interprets the 2014 Cyber Defense Policy Framework.

2014 Cyber Defense Policy Framework

The 2014 Cyber Defense Policy Framework was adopted in November 2014 by the Council of the European Union and was meant as an additional support document for the European institutions working in relation to cyber defense activities. Furthermore, this document functions as an implementation tool for the 2013 Cybersecurity Act.[108] This section proceeds with a quantitative targeted sentiment analysis, followed by a qualitative critical discourse analysis. This document directs much attention to threat identification and cooperation, but less on threat mitigation. Therefore, this document shows the EU still falls within the recursive interaction phase, as the bargaining process is still ongoing. The analysis shows that the EU is striving for more supranational cooperation, but still mostly operates on the principle of intergovernmentalism. This is not surprising, as the Council is an intergovernmental body of the EU. The EU is thus striving towards becoming a collective security actor, but cannot be classified as such yet.

[108] Kamil Halouzka and Ladislav Buřita, “Cyber Security Strategic Documents Analysis,” in *2019 International Conference on Military Technologies (ICMT)*, 2019, 1, https://doi.org/10.1109/MILTECHS.2019.8870088.

Targeted Sentiment Analysis

The same procedure is executed and the document is purged for numbers, symbols, punctuation, stop words and irrelevant words as these cloud the analysis. The most occurring words then remain Cyber, Defense, Cooperation, Security, Training, Military and Capability. For a visual overview, see figure 4.

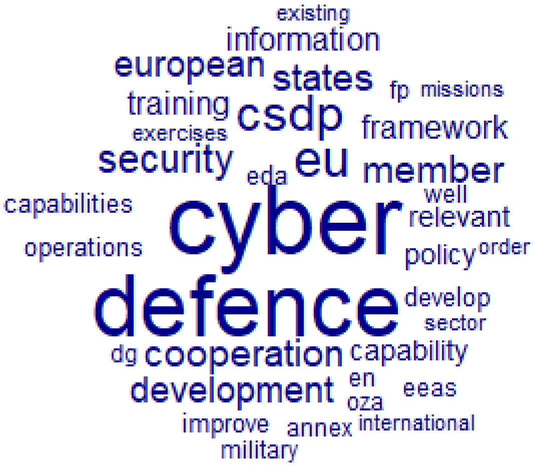


Figure 4: Wordcloud 2014 Cyber Defense Policy Framework

The text strings remain the same and are threat identification, threat mitigation and cooperation.

Threat identification. The sentiment score of this text string is 251, which is noticeably positive. 34 times the words associated with this topic were phrased in a negative context, while 285 times the words contained a positive connotation. However, in the document as a whole only 35 negatively coded sentences appear. Therefore, the sentiment score relative to the document is still reasonably high. Furthermore, it was expected that this text string would relatively receive a substantially lower sentiment score than the other categories. This is due to the words threat and incidents, which appear more often with a negative connotation. Threat identification thus receives substantially more attention in this document when compared to the 2013 Cybersecurity Act.

Threat mitigation. The sentiment score is 155, with 173 positive connotations and only 18 negative connotations. It was already expected that this text string would receive the lowest negative score. Relatively, the words signaling threat mitigating are mentioned fewer times than the other two categories. This shows the focus of the Cyber Defense Policy Framework on the other two categories: threat identification and collective securitization.

Supranational cooperation. The sentiment score is 230, with 261 positive mentions and 31 negative mentions. Nonetheless, the sentiment score still signals a predominantly positive meaning of the coded words in this category. Therefore, this document shows a focus on international cooperation and is positive about the possibilities international cooperation can bring. However, the amount of negative words is still relatively high, possibly indicating a focus on intergovernmental approaches.

The document as a whole recceives a high sentiment score, with only 35 negatively coded words, versus 295 positively coded words. A high positive score is again in the interest of the EU. Namely, by positively presenting the opportunities of collectively counteracting threats instead of articulating them as directly dangerous, the EU is overcoming risks of losing the security mandate to national decision-making. Positively presenting threats is thus an example of how the EU is striving to become a collective security actor.

In general, the targeted sentiment analysis shows a predominantly positive outlook on the three main topics of the document. Yet, it is still expected that the main negative connotations are to be found in sentences relating to threat mitigation, as the negative score was the highest of all three categories, possibly indicating difficulties in policy making. The next section interprets and contextualizes these results.

Critical Discourse Analysis

The main concepts as introduced in the targeted sentiment analysis form the basis for the critical discourse analysis. The aim of this section is to delve deeper into the text and provide context to the previous section. Moreover, it is assessed in which way the information is presented by the EU and to which extent this can be explained by the collective security framework as outlined in the theoretical framework.

Discourse of threat identification. As outlined in the targeted sentiment analysis, threat identification receives a substantial amount of attention. Multiple times, cyberspace is described as the fifth domain of military activity, which precedes the official classification of 2016. Within this document, the EU defines cyberspace as being 'equally critical to the implementation of the CDSP as the domains of land, sea, air and space'.[109] Furthermore, cyber is characterized as a rapidly developing domain, for which it is necessary to address new challenges it presents, which is an example of positive attribution towards threat identification. Moreover, the EU considers economies of scale to be necessary to 'face the ever-increasing number of threats and vulnerabilities', which is an example of a negative connotation.[110] This discourse shows the EU is willing to further integrate in the domain of cyber and believes achieving operational economies of scale on the supranational level is an appropriate way of combating threats. However, it is also asserted that the internal

[109] Council of the European Union, "EU Cyber Defence Policy Framework," 2.
[110] Council of the European Union, 9.

organization and competences of Member States should be respected.[111] This again shows that the EU is prepared to move from acting on the principles of intergovernmentalism, but still needs to recognize the individual interests of the Member States.

Discourse of threat mitigation. The primary focus of threat mitigation in this document is the development of cyber defense capabilities.[112] The EU states that in order to mitigate threats and vulnerabilities, it is essential to 'develop strong technological capacities in Europe'.[113] To do so, the 'European External Action Service (EEAS) shall develop an adequate and autonomous understanding of security and network defence matters and develop its own IT security capacity'.[114] The EEAS is the diplomatic service of the EU,[115] which means that an individual EEAS IT security capacity is a step towards supranational threat mitigation.

Discourse of supranational cooperation. In the Cyber Defense Policy Framework, the distinction between the supranational level and the intergovernmental competences is still clearly present. For example, it is stated that the EU should enable 'national forces to enhance their preparedness to operate within a multinational environment'.[116] The underlying assumption entails a focus on national protection, whereas the EU desires to create a multinational environment. This notion also becomes clear when security rules for information systems are discussed, which need to be streamlined.[117] In order to deliver an effective cyber defense capacity, the document states that the Member States should work with the EEAS and the European Defense Agency, because a 'certain degree of strategic convergence is necessary'.[118] Moreover, the cooperation should stretch out to ENISA and the European Cybercrime Center as well.[119] The existence of multiple actors uncovers the multiplicity of actors discussed by Carrapico and Barrinha.[120] The document thus shows a tendency towards intergovernmentalism.

Yet, the EU also repeatedly emphasizes further cooperation on the supranational level to be necessary to combat cyber threats. As such, the goal is to 'develop a common cyber defense culture at all levels of the CSDP chain of command'[121] or act on the 'political will to cooperate further with NATO'.[122] Besides, the EU strives to pool and share cyber defense education and training at the

[111] Council of the European Union, 3.
[112] Council of the European Union, 3.
[113] Council of the European Union, 9.
[114] Council of the European Union, 6.
[115] "EEAS | EEAS Website," accessed November 29, 2022, https://www.eeas.europa.eu/_en.
[116] Council of the European Union, "EU Cyber Defence Policy Framework," 12.
[117] Council of the European Union, 6.
[118] Council of the European Union, 4.
[119] Council of the European Union, 8.
[120] Carrapico and Barrinha, "The EU as a Coherent (Cyber) Security Actor?"
[121] Council of the European Union, "EU Cyber Defence Policy Framework," 11.
[122] Council of the European Union, 13.

European level.[123] By shifting critical military capacities, such as cyber defense education, towards the supranational level, the EU is clearly initiating a move towards becoming a more coherent cybersecurity actor.

All in all, this analysis has shown that the threat of cyber warfare has presented new challenges for the EU, which give reasons for increased integration. The EU positively presents the supranational opportunities for combating cyber warfare to boost trust and create further support for integration. Yet, the EU is still mostly operating based on the principle of intergovernmentalism, as the focus is still directed to the national capabilities of the Member States. Moreover, the multiplicity of actors in which EU institutions are bargaining with national authorities is a central tenet of intergovernmentalism. This is shown by the fact that increased cooperation is often seen as cooperation between the EU institutions and the Member States. Nonetheless, the discourses present in these documents show the EU is striving for increased integration on the supranational level, by integration of cyber defense capacities and setting up an EEAS IT security capacity. To summarize, this analysis has shown that the EU articulates an even more pressing need for supranational actions, even in the domain of defense. Yet, the principle of intergovernmentalism still prevails, which is why the EU cannot yet be classified as a coherent security actor between 2013 and 2014.

[123] Council of the European Union, 11.

Chapter 3: Reinforced securitization of cyber defense in 2018 and 2019

This section outlines the societal developments between 2014 and 2018, where after the 2018 Cyber Defense Policy Framework and the 2019 Cybersecurity Act are evaluated.

In 2014, shortly before the Crimean referendum, NATO websites were hit in a cyberattack. Although according to NATO none of the critical systems were targeted, the main NATO website and the NATO-affiliated cybersecurity center in Estonia experienced a DDoS attack.[124] The attack on NATO was claimed by a pro-Russian group of Ukrainians with alleged links to the Kremlin calling itself 'CyberBerkut', who were retaliating against what they saw as NATO interference in their country.[125]

Politically motivated cyberattacks similar to the attack on NATO sparked an academic and public debate on the question whether to classify cyber as a fifth domain of war.[126] In 2016, NATO officially classified cyber as the fifth domain of war during the bi-annual summit in Warsaw. In their Cyber Defense Pledge, NATO guarantees to 'keep pace with the fast-evolving cyber threat landscape' and ensures the Member States 'will be capable of defending themselves in cyberspace as in the air, on land and at sea'.[127]

This was preceded by the period from 2014 onwards, during which the Russian elite hacker group Sandworm launched various attacks not only on Ukraine, but also sporadically on transatlantic targets in the US. For example, in 2016 the group was alleged to have attacked the US Democratic Party in the light of the American elections.[128] Most Sandworm attacks however caused hours of power outages in several hundred thousand Ukrainian homes, often by overtaking the energy companies' own internal interface.[129] The only solution to regain power was to manually switch on all systems again, which is a tedious work, often taking hours.

In May 2017, the WannaCry ransomware attack infected over 200.000 computers in 150 countries, among which were FedEx, Honda and the UK's National Health Service. The malware was neutralized within a few hours, but the already infected computers remained unusable until the

[124] Suryakanthi Tripathi, "Cyber: Also a Domain of War and Terror," *Strategic Analysis* 39, no. 1 (January 2, 2015): 7, https://doi.org/10.1080/09700161.2014.980549; Paul Withers, "What Is the Utility of the Fifth Domain?," *Royal Air Force Air Power Review* 18, no. 1 (2015): 128–29.

[125] "NATO Websites Hit in Cyber Attack Linked to Crimea Tension," *Reuters*, March 16, 2014, sec. Internet News, https://www.reuters.com/article/us-ukraine-nato-idUSBREA2E0T320140316.

[126] For example, see: Tripathi, "Cyber."

[127] NATO, "Cyber Defence Pledge."

[128] David Martosko, "FBI & Homeland Sec. Point Finger at Russia for Democratic Party Hacks," Mail Online, December 29, 2016, http://www.dailymail.co.uk/~/article-4074710/index.html.

[129] Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, accessed November 30, 2022, https://www.wired.com/story/russian-hackers-attack-ukraine/.

victims paid the ransom or were able to break the encryption. Presumably, the North-Korean Lazarus group was responsible for WannaCry, making it again a political threat.[130]

To counteract this threat and prepare for future cyber-attacks, the EU developed a Cyber Security Toolbox in which tools for a diplomatic response after a large-scale cyber-attack are outlined. The Cyber Security Toolbox was implemented on the 7th of June 2017 and outlines measures such as the imposing of sanctions. The main aim is to deter potential aggressors with a unified response to malicious cyber activities.[131]

A mere 20 days later, the most expensive cyberattack in history, NotPetya, attacked targets primarily in Ukraine, but spread out worldwide through international companies. Associated with Sandworm, the attack was allegedly part of Russia's cyber war tactics on the West.[132] The extremely widespread consequences of the highly dangerous hacker group caused a new sense of crisis in the EU. Because the attack was so refined, the degree of possible future harm was seen as extraordinarily high. As a response to WannaCry and NotPetya, the EC published the Joint Communication on building strong cybersecurity in the EU in September 2017. The Communication proposed to commit to new measures to counteract the 'ever-growing challenges' and 'put cybersecurity at the heart of the EU as a digital society'.[133]

Even in the military domain the EU launched a binding cooperation framework: the Permanent Structured Cooperation (PESCO). PESCO is a commitment by 25 Member States to increase efforts not only in the domain of cyber defense, but also increase military cooperation altogether.[134] Even though the threat was soaring, in 2017 the cybersecurity strategy of the EU still consisted of many actors resulting in institutional fragmentation, as was argued by Carrapico and Barrinha.[135]

To sum up, the cyber landscape drastically changed during the period from 2014 until 2018. Therefore, this chapter evaluates the research question: *In what way did the EU revise discourses of securitization in the 2018 Cyber Defense Policy Framework and 2019 Cybersecurity Act after the classification of Cyber as the fifth domain of war in 2016?* In the conclusion, it is summarized that

[130] "What Was the WannaCry Ransomware Attack?," Cloudflare, accessed December 1, 2022, https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/.

[131] Erica Moret and Patryk Pawlak, *The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?* (JSTOR, 2017).

[132] Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar."

[133] "Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU" (2017), 20, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450.

[134] "COUNCIL DECISION (CFSP) 2017/ 2315 - of 11 December 2017 - Establishing Permanent Structured Cooperation (PESCO) and Determining the List of Participating Member States," n.d., 21.

[135] Carrapico and Barrinha, "The EU as a Coherent (Cyber) Security Actor?"

the EU clearly is becoming a collective security actor, by moving policies toward the supranational level. Problems of institutional fragmentation still persist, but measures are taken to remedy this problem.

Revised Cyber Defense Policy Framework (2018)

The 2014 Cyber Defense Policy Framework was updated by the Council of the European Union by request of the Member States in November 2018 and was meant to respond to changing security challenges in cyberspace. As such, the 2018 document's main objective is further developing the EU cyber defense policy. The Council asserts that it is necessary to take 'relevant developments', such as the classification of cyber as the fifth domain of war or the publication of the Cyber Diplomacy Toolbox and the Joint Communication for building strong cybersecurity for the EU into account.[136] This section first explores the 2018 revision of the document quantitatively to pave the way for the critical discourse analysis. It is concluded that the EU is moving towards being a collective security actor, as decisions such as the invocation of the Mutual Defense Clause are now made at the supranational level. This is striking, as the Council is an intergovernmental body of the EU.

Targeted Sentiment Analysis

Again, the document is prepared for text analysis by removing stop words, numbers, symbols and punctuation. Among the most occurring words then are Cyber, Defense, capabilities, training, CDSP and military. For a visual overview, see figure 5.

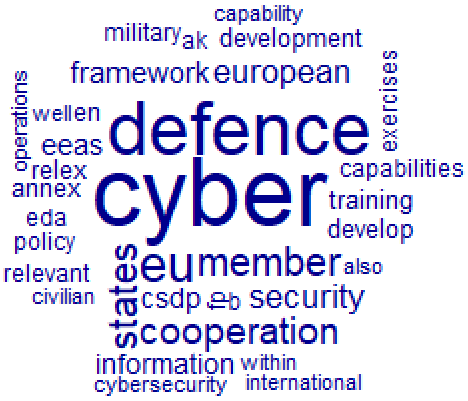


Figure 5: Wordcloud 2018 Cyber Defense Policy Framework

The text strings used in the previous chapter again form the basis of the analysis. Overall, the document receives a high positive sentiment score of 398. 476 times words were positively coded,

[136] Council of the European Union, "EU Cyber Defence Policy Framework (as Updated in 2018)," 2–4.

while 78 times words were negatively coded. The even higher sentiment score reveals the predominantly positive attitude of the EU towards their capability of counteracting cyber threats.

Threat identification. Threat identification is significantly more important than threat mitigation in this document. That is, the sentiment score is 361, with 433 positive mentions and 72 negative mentions. The high importance of threat identification indicates the stage of recursive interaction. Namely, since 2014, a first cycle of the collective securitization model was rounded off as policy outputs were implemented which 'contributed to significantly enhance Member States' cyber defense capabilities' and a new security order was established.[137] During the period of societal developments between 2014 and 2018, a new cycle of the collective securitization model commenced due to large scale cyber-attacks (the precipitating events) and the classification of cyber as the fifth domain of war (the securitization move). Renewed attention for threat identification thus indicates the renewed bargaining between the EU and the Member States.

Threat mitigation. Threat mitigation receives by far the least attention in this document. The sentiment score is 222, with 261 positively coded sentences and 39 negatively coded sentences. It is expected that threat mitigation will be more important in later stages of the collective security cycle.

Supranational cooperation. However, the collective aspect is the most extensively mentioned category in this document with a sentiment score of 368 and 441 positive mentions and 73 negative mentions. This indicates a strong focus on international and supranational cooperation, hinting at increased supranational measures.

All in all, this targeted sentiment analysis shows the Cyber Defense Policy Framework emphasizes supranational cooperation and threat identification. This shows the EU entered a new cycle of the collective security framework, in which bargaining was reinforced. The next section evaluates to which extent the discourses of threat identification, threat mitigation and supranational cooperation signal increased supranational integration.

Critical Discourse Analysis

This section evaluates to which extent the discourses of threat identification, threat mitigation and supranational cooperation show increased supranational integration.

Discourse of threat identification. In the document, it is asserted that 'Cyberspace is the fifth domain of operations'.[138] Other discourses of crises are present, such as statements regarding malicious cyber-attacks, which were not mentioned in the original document. The EU asserts that 'a

[137] Council of the European Union, 3.
[138] Council of the European Union, 2.

particularly serious cyber incident or crisis could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause and/or the Mutual Assistance Clause',[139] referring to Article 222 TFEU. The Solidarity Clause states that: 'the Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster'.[140]

Furthermore, the EU stresses that 'to deal with the effects of a cyber crisis, relevant provisions of the TEU and the Treaty on the Functioning of the EU may be applicable'.[141] The relevant provisions are the aforementioned Article 222 TFEU and 42(7) TEU. Article 42(7) is the mutual defense clause, and states:

> 'If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with article 51 of the United Nations charter'.[142]

Both provisions mean that the EU sees a cyber-attack as an attack on a Member State. Therefore, a malicious cyber-attack with serious consequences, such as the 2007 attack on Estonia, now classifies as an act of war. The EU is using strong language to deter hostile states and foster a mutual sense of the need to pool and integrate cyber defense resources to counteract the 'ever-increasing threats'.[143] This is consistent with the statement 'Actors of malicious cyber activities need to be held accountable for their actions' and 'there is a need to foster mutual cooperation to respond to malicious cyber activities'.[144] Therefore, threat identification is an important tool for the EU to emphasize the need for new extraordinary measures, such as invoking the mutual defense clause after a cyber-attack. The invocation of the clause is a strong sign of increased integration, because Member States now are obliged to support other attacked Member States. The decision to help is thus no longer a national decision made at the intergovernmental level, but a supranational decision. This is striking, as the document was published by the Council, which is an intergovernmental body. This means that the securitization of cyber threats even extended towards an intergovernmental body presenting supranational measures.

[139] Council of the European Union, 6.
[140] "CCDCOE," accessed December 2, 2022, https://ccdcoe.org/incyder-articles/eu-solidarity-clause-and-cyber-disaster/.
[141] p. 9
[142] "Article 42(7) TEU - The EU's Mutual Assistance Clause | EEAS Website," accessed December 2, 2022, https://www.eeas.europa.eu/eeas/article-427-teu-eus-mutual-assistance-clause_en.
[143] Council of the European Union, "EU Cyber Defence Policy Framework (as Updated in 2018)," 17.
[144] Council of the European Union, 9.

Discourse of threat mitigation. After 2016 both the EU and NATO committed to 'mainstreaming cyber into crisis management'.[145] This indicates a move towards phase 6 of the collective security cycle, in which extraordinary measures become the status quo. Yet, measures already proposed in the 2014 Cyber Defense Policy Framework are still not implemented. Namely, the European External Action Service would set up a central IT security capacity. However, the 2018 document states that 'the EEAS will develop an adequate and autonomous understanding of security and network defense matters and develop its own IT security capacity', which will be 'an integral part of existing operational entities'.[146] Thus, the move towards a supranational entity, already intended in 2014, was not yet executed in 2018. The EU thus still shows willingness to increase integration, but was not able to act on this particular intention yet.

Discourse of supranational cooperation. In general, the document displays strong discourses of cooperation. For example, it is stated that 'security and defense efforts should enhance the EU's strategic role and its capacity to act autonomously when and where necessary'.[147] This strategic role should in turn contribute to a common goal: EU's strategic autonomy.[148] Strategic autonomy refers often to the national capacity to act independently in defense matters.[149] However, the EU is referring to strategic autonomy as a European affair, in which Member States are internally extremely dependent on each other. By proposing strategic autonomy on the supranational level, the EU is clearly acting as a collective security actor. The EU still considers national preferences, but decision-making power remains at the supranational level.

Moreover, the EU upholds that 'achieving economies of scale is a necessity in order to face the ever-increasing number of threats and vulnerabilities'.[150] Economies of scale within the policy and the operational domain imply increased cooperation. Instead of organizing capabilities at the national level, efficiency can only be achieved when Member States work together supranationally.

Also, the EU also aims to collaborate with other international organizations, in particular the UN, the OSCE and the ASEAN Regional Forum, to formulate a 'strategic framework for conflict prevention, cooperation and stability in cyberspace'.[151] According to the EU, this could help to 'promote EU principles and values'.[152] By shifting focus from internal organization towards external influence, the EU is positioning itself as a collective security actor towards other international

[145] Council of the European Union, 4.
[146] Council of the European Union, 12.
[147] Council of the European Union, 3.
[148] Council of the European Union, 5.
[149] Daniel Fiott, "Strategic Autonomy: Towards 'European Sovereignty' in Defence?" (European Union Institute for Security Studies (EUISS), 2018), 4, https://www.jstor.org/stable/resrep21120.
[150] Council of the European Union, "EU Cyber Defence Policy Framework (as Updated in 2018)," 17.
[151] Council of the European Union, 8.
[152] Council of the European Union, 8.

entities. That is, by acting on behalf of the Member States in the international arena, the EU shows it competes as a serious collective security actor with autonomous decision-making power.

To sum up, the EU clearly is showing it is becoming a collective security actor. That is, when comparing the discourse of 2018 to 2014, the EU certainly shows supranational decision making, which is a sign of a fully functioning collective security actor. Additionally, even the intergovernmental Council is implementing supranational decision-making by invoking the Mutual Defense Clause after a cyber-attack. Nonetheless, not all intentions were fully fulfilled yet. Therefore, the EU can almost be classified as a collective security actor, but the intentions to solve problems of institutional fragmentation should still be fulfilled first.

Revised Cybersecurity Act (2019)

In 2019, the original 2013 Cybersecurity Act was updated, as 'the connected economy and society is more vulnerable to cyber threats and thus requires stronger defense'.[153] Therefore, the mandate of ENISA was extended and enlarged, which is described in the 2019 document.

Targeted Sentiment Analysis

Again, the document is prepared for text analysis by removing stop words, numbers, symbols and punctuation. Among the most occurring words then are ICT, Cybersecurity, Certification, and ENISA. For a visual overview, see figure 6.

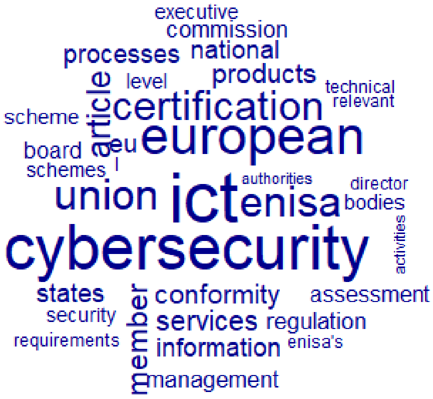


Figure 6: Wordcloud 2019 Cybersecurity Act

The same words constitute the text strings. Overall, the document receives a remarkably high positive sentiment score of 1111. 1456 times words were positively coded, while 345 times words were negatively coded. Compared to the 2013 version, the updated document is three times more extensive. This already shows the need for additional measures since 2013.

[153] Parliament and Council, Cybersecurity Act 2019, paragraph 5

Threat identification. In this document, threat identification has a relatively low score of 685. 249 times the text strings occurred in a negative context, while 934 times a positive connotation was detected. As the focus of this document is shifting towards threat mitigation, the EU is moving from the recursive interaction phase towards the policy output phase.

Threat mitigation. Compared to the 2018 Cyber Defense Policy Framework, threat mitigation receives substantially more attention. The overall sentiment score is 766, with 1003 positive mentions and 237 negative mentions. Again, the overwhelming positive score signals the optimistic belief of the EU in their ability to mitigate threats.

Supranational cooperation. The words indicating a focus on international cooperation received a sentiment score of 773, with 990 positive mentions and 217 negative mentions. Relatively, the negative connotations are quite low compared to the other two categories. This points in the direction of more supranational measures, especially when compared to the 2013 version.

To conclude, this targeted sentiment analysis has shown that the EU is rapidly moving through the phases of the collective security framework. By attributing substantially more attention to threat mitigation, this document signals policy outputs are achieved. Therefore, in 2019 the EU reached phase five of the collective security framework in which supranational decision-making prevails.

Critical Discourse Analysis

This section evaluates to which extent the discourses of threat identification, threat mitigation and supranational cooperation signal increased supranational integration.

Discourses of threat identification. The EU acknowledges that an increasing number of devices are connected to the internet, but ‘security and resilience are not sufficiently built-in by design, leading to insufficient cybersecurity.’[154] This is caused by policy responses being predominantly national, while large-scale incidents have the ability to ‘disrupt the provision of essential services across the Union’. Therefore, the EU stresses the need for ‘effective and coordinated responses and crisis management and the Union level’.[155] Therefore, it is acknowledged that the current situation is still focused on national remedies. Yet, the EU emphasizes the need for supranational strategies, because large-scale attacks cross borders and cannot be combated using national approaches. The EU thus positively presents the threat, which is a sign of a collective security actor.

[154] Parliament and Council, Cybersecurity Act 2019, paragraph 2

[155] Parliament and Council, Cybersecurity Act 2019, paragraph 5

Discourses of threat mitigation. Regarding threat mitigation, the EU uses stronger language and states that 'in order to mitigate risks, all necessary actions need to be taken to improve cybersecurity in the Union'.[156] In the 2013 document, the task set of ENISA remained superficial and centered on promoting best practices and information-sharing. Yet, in the revision the tasks of ENISA are expanded and much more substantial. For example, ENISA functions as the secretariat to the supranational Computer Security Incident Response Team (CSIRT)-network, consisting of the EU Computer Emergency Response Team (CERT-EU) and the national Computer Emergency Response Teams. The European CSIRT-network is responsible for joint responses after attacks, but also engages in science diplomacy. As Tanczer, Brass and Carr explain, CSIRTs function as an epistemic community that, through 'shared technical expertise, norms and best practices, have established knowledge-based networks that support international coordination in cybersecurity'.[157] In this way, the European CSIRT network functions as a non-state actor which facilitates supranational cooperation in case of a large-scale cyber-attack.

Additionally, the EU addresses the need to overcome institutional fragmentation, as 'ENISA shall contribute to reducing the fragmentation and the cooperation among its members'.[158] In doing so, 'ENISA shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market'.[159] Furthermore, ENISA's mandate is now extended for an indefinite period, signaling the importance of the organization within the supranational framework.[160]

All in all, the tasks of ENISA are much more supranational than in 2013. Yet, the Management Board still consists of 27 delegates of Member States and two members of the Commission,[161] therefore the internal structure still resembles the intergovernmental principle. However, by having a supranational task set, the organization itself functions at the supranational level. An example is the task that 'ENISA shall contribute to the Union's efforts to cooperate with third countries and international organizations as well as within relevant international cooperation frameworks to promote international cooperation on issues related to cyberse-curity'.[162] ENISA thus functions as an expertise center representing the EU. All in all, ENISA shows to be operating mainly at the Union level representing Member States at the supranational level.

[156] Parliament and Council, Cybersecurity Act 2019, paragraph 3

[157] Leonie Maria Tanczer, Irina Brass, and Madeline Carr, "CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy," *Global Policy* 9, no. S3 (2018): 60, https://doi.org/10.1111/1758-5899.12625.

[158] Parliament and Council, Cybersecurity Act 2019, Art. 3(4)

[159] Parliament and Council, Cybersecurity Act 2019, Art. 4(6)

[160] Parliament and Council, Cybersecurity Act 2019, Art. 68(4)

[161] Parliament and Council, Cybersecurity Act 2019, Art.14

[162] Parliament and Council, Cybersecurity Act 2019, Art. 12

Discourses of supranational cooperation. In this document, the principle of subsidiarity is explained differently than in 2013. The EU asserts that 'the objectives cannot be sufficiently achieved by the Member States but can rather, by reason of its scale and effects, be better achieved at the Union level'.[163] This remains in accordance with the principle of subsidiarity as set out in Article 5 of the TEU. This means that the EU now justifies actions on the Union level, which in 2013 was only still aimed at ENISA being an information hub that promotes best practices. Now, the EU explains that 'given the borderless nature of cyber threats, there is a need to increase capabilities at Union level'.[164]

One of these supranational measures is the proposition of an EU-wide cybersecurity certification framework, which functions as 'a comprehensive set of rules, technical requirements, standards and procedures established at Union level'.[165] By adopting a cybersecurity certification framework at the supranational level, the EU is able to enforce standards and increase interoperability across the Union. Furthermore, the EU certification supersedes any national certifications, as these 'cease to be effective' to 'avoid fragmentation of the internal market' from the moment of implementation of the EU certification onwards.[166]

On top, the EU proposes the inter-institutional CERT-EU will function as an overarching supranational organization in which the national CERTs will form a CSIRT network. The CERT-EU was founded to overcome the multiplicity of actors and was established by arrangement of inter alia the EP, the EC, and the Council of the European Union.[167] As mentioned, ENISA takes up the role of being the secretariat of the European CSIRT network, again functioning supranationally.[168]

To summarize, this analysis has shown that the EU is clearly taking the lead in tackling cyber threats by implementing policy on the supranational level. A new cycle of the collective securitization processes began in 2016, after the classification of cyber as the fifth domain of war and large-scale cyber-attacks such as WannaCry and NotPetya. The 2018 Cyber Defense Policy Framework showed that decision-making now becomes supranational, as a cyber-attack classifies as a reason to invoke the Mutual Defense Clause. Member States are then obliged to help in case of an attack on critical infrastructure. In 2019, the EU justified supranational measures by explaining the

[163] Parliament and Council, Cybersecurity Act 2019, paragraph 109
[164] Parliament and Council, Cybersecurity Act 2019, paragraph 6
[165] Parliament and Council, Cybersecurity Act 2019, Art. 2(9)
[166] Parliament and Council, Cybersecurity Act 2019, paragraph 94
[167] Parliament and Council, Cybersecurity Act 2019, paragraph 31
[168] Parliament and Council, Cybersecurity Act 2019, paragraph 46

principle of subsidiarity differently. ENISA’s tasks now are at the supranational level, by functioning as the secretariat of the CERT-EU network or representing the Union externally.

Even though the EU shows clear supranational decision-making, problems of institutional fragmentation still persist. Interoperability remains a priority and not all intentions, such as the EEAS IT capacity, were implemented. However, when compared to 2013 and 2014, the EU is almost fully functioning as a collective security actor in the field of cyber defense in 2018 and 2019. Yet, problems of institutional fragmentation still inhibit a classification of a complete cybersecurity actor.

Discussion and Conclusion

All in all, the cyber landscape drastically changed between 2013 and 2019 as threats surged and became politically motivated. This thesis has shown that the EU went through multiple cycles of the collective security framework during this period. The analysis of the 2013 Cybersecurity Act and the 2014 Cyber Defense Policy Framework signaled attempts of the EU to implement further supranational policies. However, decision-making remained primarily intergovernmental, as the national capacities of Member States still prevailed. Therefore, problems of institutional fragmentation were recognized, but not yet dealt with. After the publication of the 2014 Cyber Defense Policy Framework and the fulfillment of the first collective security cycle, cyber-attacks were increasingly politically motivated and aimed at disrupting critical infrastructures. As a result, NATO classified cyber as the fifth domain of war in 2016. Large-scale cyber-attacks were carried out, with the NotPetya attack of 2017 serving as a prime example. Therefore, the EU passed a new cycle of the collective security framework. The 2018 Cyber Defense Policy Framework showed that the EU was again in the phase of recursive interaction, as the focus laid on threat identification. Most importantly, this document ensured that if a Member State would be the victim of a disrupting cyber-attack, the Mutual Defense Clause could be invoked. This entails that Member States are obliged to assist another Member State in case of an attack. Therefore, the decision to help is no longer intergovernmental, but became supranational with the 2018 Cyber Defense Policy Framework. In 2019, the EU moved towards the policy output phase of the collective security cycle. ENISA became a supranational institution and the EU certification framework now precedes national certifications. However, not all problems of institutional fragmentation were solved, which was shown by the fact that mitigation measures still were predominantly national.

To conclude, the EU thus almost fully developed into a collective security actor in the field of cyber defense between 2013 and 2019. However, problems of institutional fragmentation, although recognized and addressed, still persist. Therefore, on the basis of this research the EU cannot yet be classified as a fully functioning collective security actor.

Linking back to the existing academic literature, the historical perspective of this thesis has shown that wars are indeed becoming virtual, which was already argued by Der Derian in 2002.[169] Therefore, it became a key priority for the EU to design measures aimed at defending the Union against cyber warfare. According to Ruohonen, Hyrynsalmi, and Leppänen, institution-building activities halted or slowed down around 2016.[170] Yet, this thesis has shown that in 2016 a new cycle

[169] Der Derian, "Virtuous War/Virtual Theory," 771–72.

[170] Ruohonen, Hyrynsalmi, and Leppänen, "An Outlook on the Institutional Evolution of the European Union Cyber Security Apparatus," 746.

of the collective security framework commenced because of the classification of war by NATO, leading up towards more supranational decision-making and thus institutional development.

Moreover, Bendiek and Schulze argued there is a lack of coherence in cyber defense strategies up until 2021.[171] However, this thesis has shown that the EU is becoming a collective security actor, even though some problems of institutional fragmentation still persist. This reaffirms the conclusion of Carrapico and Barrinha, who explained that the EU clearly made efforts to consolidate their activities in the field of cybersecurity, concluding there is in fact no complete lack of coherence, as institutional efforts are made to supranationally cooperate.[172] While both Carrapico and Barrinha, as well as Christou, outline that cyber defense measures remained underdeveloped,[173] this thesis argues that the EU has actually is becoming a collective cyber security actor in the field of cyber defense. Therefore, this thesis has provided the academic literature with an alternative perspective to the functioning of the EU as a collective security actor in the field of cybersecurity, and cyber defense more specifically.

Yet, this thesis does contain some limitations, which could be used as a basis for further research. First, this thesis experienced a limited scope, as the focus laid on the EU as a supranational entity. However, the role of the different Member States within policy formation could provide new perspectives. Further research therefore should focus on the contributions of individual Member States or the differences between national cybersecurity strategies. Furthermore, supranational cooperation between the EU and NATO is ever-increasing. New research could focus on the collaboration between these entities. Second, the topic of cyber defense is extremely relevant and circumstances change almost daily. This research has not taken recent societal developments such as the Covid-19 pandemic or the Russian invasion of Ukraine of 2022 into account. However, these events have had profound consequences on the cyber landscape, and further research should take these into account. Third, this thesis has attempted to integrate social science and historical methods to clarify the complex process that led to the process of securitization. Even though a targeted sentiment analysis is able to categorize, detailed research cannot be yet be entirely based on methods of text mining as these should be further developed. In this research, the methodological choice was made to use a targeted sentiment analysis, but direct emphasis towards a critical discourse analysis. Future research could however use a targeted sentiment analysis to compare and contrast the responses of multiple countries on EU cybersecurity measures. Lastly, this thesis has opted to analyze documents published by both the Commission, which is a supranational body, as well as the

[171] Bendiek and Schulze, "Attribution."
[172] Carrapico and Barrinha, "The EU as a Coherent (Cyber) Security Actor?"
[173] Christou, "The Collective Securitisation of Cyberspace in the European Union."

Council, which is an intergovernmental body. Future research could further focus on the differences in organization to evaluate in which way these bodies cooperate within the EU as a whole.

It is expected that cyber threats will exponentially become more paramount to modern warfare. The risks of attacks on critical infrastructures are ever-increasing, as cyber tactics are becoming more sophisticated and refined. In 2020, the EU imposed sanctions against cyberattacks for the first time. In 2022, the new EU Strategic Compass was published, in which the overarching military goals are outlined for the coming decade. Unsurprisingly, cyber not only functioned as the fifth domain, but was integrated within each domain of war.[174] Cyber will unequivocally become ever more important in the lives of the citizens of not only the EU, but the entire world. The question remains if and how cyber defense measures will be able to safeguard citizens from the ever-increasing risks caused by attacks on critical infrastructures.

[174] "A Strategic Compass for a Stronger EU Security and Defence in the next Decade," March 21, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/.

Bibliography

Primary sources

"A Strategic Compass for a Stronger EU Security and Defence in the next Decade," March 21, 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/.

"Art. 5 Treaty on European Union - (Ex Article 5 TEC)." Accessed November 21, 2022. https://lexparency.org/eu/TEU/ART_5/.

"Article 42(7) TEU - The EU's Mutual Assistance Clause | EEAS Website." Accessed December 2, 2022. https://www.eeas.europa.eu/eeas/article-427-teu-eus-mutual-assistance-clause_en.

BBC News. "How a Cyber Attack Transformed Estonia," April 27, 2017, sec. Europe. https://www.bbc.com/news/39655415.

Bhattacharjee, Subimal. "Q1 2004 Tops In Cyber Attacks." The Financial Express, May 3, 2004. https://www.financialexpress.com/archive/q1-2004-tops-in-cyber-attacks/105661/.

"BI-SC Input to a NEW Capstone Concept for the Military Contribution to Countering Hybrid Threats." Brussels: NATO, 2010.

"CCDCOE." Accessed December 2, 2022. https://ccdcoe.org/incyder-articles/eu-solidarity-clause-and-cyber-disaster/.

"CNN.Com - Security Firm: MyDoom Worm Fastest yet - Jan. 28, 2004." Accessed November 14, 2022. http://edition.cnn.com/2004/TECH/internet/01/28/mydoom.spreadwed/.

"Common Security and Defence Policy | Fact Sheets on the European Union | European Parliament." Accessed October 20, 2022. https://www.europarl.europa.eu/factsheets/en/sheet/159/common-security-and-defence-policy.

Council of the European Union. "EU Cyber Defence Policy Framework," November 18, 2014. https://ccdcoe.org/uploads/2018/11/EU-141118-EUCyberDefencePolicyFrame-2.pdf.

Council of the European Union. "EU Cyber Defence Policy Framework (as Updated in 2018)," November 19, 2018. https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf.

"Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions." Accessed September 5, 2022. https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.

"Debates - Critical Information Infrastructure Protection: Towards Global Cybersecurity (Short Presentation) - Monday, 11 June 2012." Accessed October 28, 2022. https://www.europarl.europa.eu/doceo/document/CRE-7-2012-06-11-ITM-024_EN.html.

"Debates - Cyber Defence (Debate) - Tuesday, 12 June 2018." Accessed September 28, 2022. https://www.europarl.europa.eu/doceo/document/CRE-8-2018-06-12-ITM-018_EN.html.

"Debates - European Union's Internal Security Strategy (Short Presentation) - Monday, 21 May 2012." Accessed October 28, 2022. https://www.europarl.europa.eu/doceo/document/CRE-7-2012-05-21-ITM-017_EN.html.

"Debates - Implementation of the Common Security and Defence Policy - EU Mutual Defence and Solidarity Clauses: Political and Operational Dimensions - Cyber Security and Defence - Role of the Common Security and Defence Policy in Cases of Climate-Driven Crises and Natural Disasters (Debate) - Wednesday, 21 November 2012." Accessed October 28, 2022. https://www.europarl.europa.eu/doceo/document/CRE-7-2012-11-21-ITM-013_EN.html.

"Debates - Organised Crime, Corruption and Money Laundering (A7-0175/2013 - Salvatore Iacolino) - Tuesday, 11 June 2013." Accessed October 28, 2022. https://www.europarl.europa.eu/doceo/document/CRE-7-2013-06-11-ITM-013-11_EN.html.

"Debates - Security Threats Connected with the Rising Chinese Technological Presence in the EU and Possible Action on the EU Level to Reduce Them (Debate) - Wednesday, 13 February 2019." Accessed September 28, 2022. https://www.europarl.europa.eu/doceo/document/CRE-8-2019-02-13-ITM-027_EN.html.

"Debates - Stress Tests of Nuclear Power Plants in EU and Nuclear Safety in EU Neighbourhood Countries (Debate) - Thursday, 9 June 2011." Accessed October 28, 2022. https://www.europarl.europa.eu/doceo/document/CRE-7-2011-06-09-ITM-005_EN.html.

"Declaration by the High Representative Josep Borrell, on Behalf of the European Union, on Malicious Cyber Activities Exploiting the Coronavirus Pandemic." Accessed September 5, 2022. https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, 218 OJ L § (2013). http://data.europa.eu/eli/dir/2013/40/oj/eng.

"EU Digital Diplomacy: Council Agrees a More Concerted European Approach to the Challenges Posed by New Digital Technologies." Accessed September 5, 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/07/18/eu-digital-diplomacy-council-agrees-a-more-concerted-european-approach-to-the-challenges-posed-by-new-digital-technologies/.

"EU Imposes the First Ever Sanctions against Cyber-Attacks." Accessed September 5, 2022. https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

European Parliament. "Cyber security and defence." Regulation 2012/2096(INI), November 22, 2012. https://www.europarl.europa.eu/doceo/document/TA-7-2012-0457_EN.html

European Parliament and the Council of the European Union. "European Network and Information Security Agency (ENISA)." Regulation 460/2004, October 20, 2004. https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32004R0460

European Parliament and the Council of the European Union. "Regulation concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004" Regulation 2013/526, May 21, 2013. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32013R0526

European Parliament and the Council of the European Union. "Regulation on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)." Regulation 2019/881, April 17, 2019. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32019R0881

European Parliament and the Council of the European Union. "Regulation establishing the European Network and Information Security Agency as regards its duration." Regulation 1007/2008. September 24, 2008. http://data.europa.eu/eli/reg/2008/1007/oj/eng.

European Parliament and the Council of the European Union. "Regulation concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004." Regulation 2013/526, May 21, 2013. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32013R0526

European Parliament and the Council of the European Union. "Regulation Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards Its Duration." Regulation 580/2011. June 8, 2011. https://eur-lex.europa.eu/eli/reg/2011/580/oj

General Secretariat of the Council of the European Union, 'Council Conclusions on Cyber Diplomacy,' February 11, 2015. Unclassified. | National Security Archive." Accessed September 5, 2022. https://nsarchive.gwu.edu/document/15355-general-secretariat-council.

mi2g. "2004: Year of the Global Malware Epidemic - Top Ten Lessons," November 21, 2004. http://mi2g.com/.

NATO. "Cyber Defence Pledge." NATO. Accessed September 5, 2022. https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

Paet, Urmas. "REPORT on Cyber Defence | A8-0189/2018 | European Parliament." Accessed September 28, 2022. https://www.europarl.europa.eu/doceo/document/A-8-2018-0189_EN.html.

"Plenardebatten - Rechtsakt zur EU-Cybersicherheit - Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung und Netz nationaler Koordinierungszentren (Aussprache) - Montag, 11. März 2019." Accessed September 28, 2022. https://www.europarl.europa.eu/doceo/document/CRE-8-2019-03-11-INT-1-110-0000_DE.html.

"Plenardebatten - Rechtsakt zur EU-Cybersicherheit - Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung und Netz nationaler Koordinierungszentren (Aussprache) - Montag, 11. März 2019." Accessed September 28, 2022. https://www.europarl.europa.eu/doceo/document/CRE-8-2019-03-11-INT-1-140-0000_DE.html.

Rains, Tim. "Cyber-Threats in the European Union: First Half 2012." *Microsoft Security Blog* (blog), October 22, 2012. https://www.microsoft.com/en-us/security/blog/2012/10/22/cyber-threats-in-the-european-union-first-half-2012/.

Realizing the Information Future: The Internet and Beyond. Washington, D.C: National Academy Press, 1994.

"Response to Malicious Cyber Activities: Council Adopts Conclusions." Accessed September 5, 2022. https://www.consilium.europa.eu/en/press/press-releases/2018/04/16/malicious-cyber-activities-council-adopts-conclusions/.

Reuters. "NATO Websites Hit in Cyber Attack Linked to Crimea Tension," March 16, 2014, sec. Internet News. https://www.reuters.com/article/us-ukraine-nato-idUSBREA2E0T320140316.

"Win32/Mydoom Threat Description - Microsoft Security Intelligence." Accessed November 14, 2022. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Mydoom.

Secondary sources

Alatalu, Siim. “Dealing with an Evolving Cyber Threat Picture–Developing a Joint European Response.” *Cyber Defense-Policies, Operations and Capacity Building: CYDEF 2018* 147 (2019): 10.

Alford, Lionel D. “Cyber Warfare: Protecting Military Systems.” AIR FORCE MATERIEL COMMAND WRIGHT-PATTERSON AFB OH, 2000.

Ashworth, Lucian M. “Interdisciplinarity and International Relations.” *European Political Science* 8, no. 1 (March 1, 2009): 16–25. https://doi.org/10.1057/eps.2008.11.

Bachmann, Sascha Dov, and Hakan Gunneriusson. “Terrorism and Cyber Attacks as Hybrid Threats: Defining a Comprehensive Approach for Countering 21st Century Threats to Global Risk and Security.” *The Journal on Terrorism and Security Analysis*, 2014.

Bachmann, Sascha-Dominik. “Hybrid Threats, Cyber Warfare and NATO’s Comprehensive Approach for Countering 21st Century Threats - Mapping the New Frontier of Global Risk and Security Management.” *Amicus Curiae* 88 (2011): [iii]-28.

Balzacq, Thierry, and Myriam Dunn Cavelty. “A Theory of Actor-Network for Cyber-Security.” *European Journal of International Security* 1, no. 2 (2016): 176–98.

Balzacq, Thierry, Sarah Léonard, and Jan Ruzicka. “‘Securitization’Revisited: Theory and Cases.” *International Relations* 30, no. 4 (2016): 494–531.

Barrinha, Andre. “Virtual Neighbors: Russia and the EU in Cyberspace.” *Insight Turkey* 20, no. 3 (2018): 29–42.

Bellamy, Christopher. “What Is Information Warfare?” In *Managing the Revolution in Military Affairs*, 56–75. Springer, 2001.

Bendiek, Annegret, and Matthias Schulze. “Attribution: A Major Challenge for EU Cyber Sanctions. An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW.” SWP Research Paper, 2021.

Brown, Chris, and Robyn Eckersley. *The Oxford Handbook of International Political Theory*. Oxford University Press, 2018.

Brun, Louis, and Rocco Bellanova. “The Role of the European Union Agency for Network and Information Security (ENISA) in the Governance Strategies of European Cybersecurity.” *Université Catholique de Louvain*, 2018.

Buzan, Barry, Barry G. Buzan, Ole W'ver, Ole Waever, and Ole Waever Barry Buzan. *Regions and Powers: The Structure of International Security*. Vol. 91. Cambridge University Press, 2003.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder, Colo: Lynne Rienner Pub, 1998.

Carrapico, Helena, and Andre Barrinha. "European Union Cyber Security as an Emerging Research and Policy Field." *European Politics and Society*. Taylor & Francis, 2018.

Carrapico, Helena, and André Barrinha. "The EU as a Coherent (Cyber) Security Actor?" *JCMS: Journal of Common Market Studies* 55, no. 6 (2017): 1254–72.

Cederberg, Aapo, and Pasi Eronen. "How Can Societies Be Defended against Hybrid Threats." *Strategic Security Analysis* 9, no. 1 (2015): 1–10.

Christou, George. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. Springer, 2016.

"The Collective Securitisation of Cyberspace in the European Union." *West European Politics* 42, no. 2 (2019): 278–301. https://doi.org/10.1080/01402382.2018.1510195.

Cini, Michelle, and Nieves Pérez-Solórzano Borragán, eds. *European Union Politics*. Fifth Edition. Oxford ; New York, NY: Oxford University Press, 2016.

Claessen, Eva. "Reshaping the Internet – the Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance: The Case of Russia and the EU." *Journal of Cyber Policy* 5, no. 1 (January 2, 2020): 140–57. https://doi.org/10.1080/23738871.2020.1728356.

Cohen-Almagor, Raphael. "Internet History." In *Moral, Ethical, and Social Dilemmas in the Age of Technology: Theories and Practice*, 19–39. IGI Global, 2013.

Collins, Alan, ed. *Contemporary Security Studies*. Fourth edition. Oxford, United Kingdom ; New York, NY: Oxford University Press, 2016.

Craig, Anthony JS, and Brandon Valeriano. "Realism and Cyber Conflict: Security in the Digital Age." *Realism in Practice* 85 (2018).

Crane, Casey. "42 Cyber Attack Statistics by Year: A Look at the Last Decade." *InfoSec Insights* (blog), February 21, 2020. https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/.

"Department of Defense Strategy for Operating in Cyberspace," n.d., 19.

Der Derian, James. "Virtuous War/Virtual Theory." *International Affairs* 76, no. 4 (2000): 771–88. https://doi.org/10.1111/1468-2346.00164.

"EEAS | EEAS Website." Accessed November 29, 2022. https://www.eeas.europa.eu/_en.

Europol. "European Cybercrime Centre - EC3." Accessed October 27, 2022. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

Fairclough, Norman. "Critical Discourse Analysis." In *The Routledge Handbook of Discourse Analysis*, 9–20. Routledge, 2013.

Fayi, Sharifah Yaqoub A. "What Petya/NotPetya Ransomware Is and What Its Remidiations Are." In *Information Technology-New Generations*, 93–100. Springer, 2018.

Fiott, Daniel. "Strategic Autonomy: Towards 'European Sovereignty' in Defence?" European Union Institute for Security Studies (EUISS), 2018. https://www.jstor.org/stable/resrep21120.

Giersch, Herbert. "Eurosclerosis." Kieler Diskussionsbeitr‰ ge, 1985.

Graaf, Beatrice de, and Cornel Zwierlein. "Historicizing Security - Entering the Conspiracy Dispositive." *Historical Social Research / Historische Sozialforschung* 38, no. 1 (143) (2013): 46–64.

Greenberg, Andy. "How an Entire Nation Became Russia's Test Lab for Cyberwar." *Wired*. Accessed November 30, 2022. https://www.wired.com/story/russian-hackers-attack-ukraine/.

Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. First edition. New York: Doubleday, 2019.

"The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired, August*, 2018.

Halouzka, Kamil, and Ladislav Buřita. "Cyber Security Strategic Documents Analysis." In *2019 International Conference on Military Technologies (ICMT)*, 1–6, 2019. https://doi.org/10.1109/MILTECHS.2019.8870088.

Hansen, Lene, and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53, no. 4 (2009): 1155–75.

Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49–60.

Heywood, Andrew. *Global Politics*. 2nd edition. Palgrave Foundations. Basingstoke: Palgrave Macmillan, 2014.

Hoffman, F. G. "'Hybrid Threats': Neither Omnipotent Nor Unbeatable." *Orbis* 54, no. 3 (January 1, 2010): 441–55. https://doi.org/10.1016/j.orbis.2010.04.009.

Horst, Savannah ter. "Thin or Thick Collective Securitization?," 2021.

Howorth, Jolyon. “Decision-Making in Security and Defense Policy: Towards Supranational Inter-Governmentalism?” *Cooperation and Conflict* 47, no. 4 (December 1, 2012): 433–53. https://doi.org/10.1177/0010836712462770.

Ilves, Luukas K., Timothy J. Evans, Frank J. Cilluffo, and Alec A. Nadeau. “European Union and Nato Global Cybersecurity Challenges.” *Prism* 6, no. 2 (2016): 126–41.

Ivan, Paul. “Responding to Cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox. EPC Discussion Paper, 18 March 2019,” 2019.

Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (2017). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450.

Kleinert, Jörn, and Daniel Piazolo. “Governing the Cyber Space.” In *The New Economy and Economic Growth in Europe and the US*, edited by David B. Audretsch and Paul J. J. Welfens, 271–92. American and European Economic and Political Studies. Berlin, Heidelberg: Springer, 2002. https://doi.org/10.1007/978-3-540-24826-2_14.

Krasner, Stephen D. “Sovereignty.” In *Sovereignty*. Princeton University Press, 1999.

Kumagai, Jean. “The Web as Weapon [Cyber Warfare].” *IEEE Spectrum* 38, no. 1 (2001): 118–21.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. “A Brief History of the Internet.” *ACM SIGCOMM Computer Communication Review* 39, no. 5 (2009): 22–31.

Lewis, James Andrew. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Center for Strategic & International Studies Washington, DC, 2002.

Limnell, Jarno, S. Alatalu, I. Borogan, E. Chernenko, S. Herpig, O. Jonsson, X. Kurowska, P. Pawlak, P. Pernik, and T. Reinhold. “Russian Cyber Activities in the EU.” *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, 2018, 65–74.

Linkov, Igor, Lada Roslycky, and Benjamin D. Trump. *Resilience and Hybrid Threats: Security and Integrity for the Digital World*. Vol. 55. IOS Press, 2019.

Martosko, David. “FBI & Homeland Sec. Point Finger at Russia for Democratic Party Hacks.” Mail Online, December 29, 2016. http://www.dailymail.co.uk/~/article-4074710/index.html.

“MEPs Work to Boost Europe’s Cyber Security (Infographic) | News | European Parliament,” March 11, 2019. https://www.europarl.europa.eu/news/en/headlines/security/20190307STO30713/meps-work-to-boost-europe-s-cyber-security-infographic.

“Microsoft Digital Defense Report and Security Intelligence Reports.” Accessed November 7, 2022. https://www.microsoft.com/en-us/security/business/security-intelligence-report.

Moret, Erica, and Patryk Pawlak. *The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?* JSTOR, 2017.

Nardi, Maria Luisa. “Origin of Cyber Warfare and How the Espionage Changed: A Historical Overview.” Chapter. Transdisciplinary Perspectives on Risk Management and Cyber Intelligence. IGI Global, 2021. https://doi.org/10.4018/978-1-7998-4339-9.ch011.

Ooijen, Marleen van. “Cyber Securitization or Cyberization of Conflict?,” n.d., 41.

Paulo, Jorge Silva. “The European Defense Sector and EU Integration.” *Connections* 8, no. 1 (2008): 11–57.

Ruohonen, Jukka, Sami Hyrynsalmi, and Ville Leppänen. “An Outlook on the Institutional Evolution of the European Union Cyber Security Apparatus.” *Government Information Quarterly* 33, no. 4 (October 2016): 746–56. https://doi.org/10.1016/j.giq.2016.10.003.

Sliwinski, Krzysztof Feliks. “Moving beyond the European Union’s Weakness as a Cyber-Security Agent.” *Contemporary Security Policy* 35, no. 3 (2014): 468–86.

Sperling, James, and Mark Webber. “NATO and the Ukraine Crisis: Collective Securitisation.” *European Journal of International Security* 2, no. 1 (2017): 19–46.

Sperling, James, and Mark Webber “The European Union: Security Governance and Collective Securitisation.” *West European Politics* 42, no. 2 (2019): 228–60.

Stauffer, Don. “Electronic Warfare: Battles without Bloodshed.” *The Futurist* 34, no. 1 (2000): 23.

Steingartner, William, Darko Galinec, and Andrija Kozina. “Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model.” *Symmetry* 13, no. 4 (2021): 597.

Stiennon, Richard. “A Short History of Cyber Warfare.” In *Cyber Warfare*. Routledge, 2015.

Stritzel, Holger. “Towards a Theory of Securitization: Copenhagen and Beyond.” *European Journal of International Relations* 13, no. 3 (2007): 357–83.

Tanczer, Leonie Maria, Irina Brass, and Madeline Carr. “CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy.” *Global Policy* 9, no. S3 (2018): 60–66. https://doi.org/10.1111/1758-5899.12625.

Tibken, Shara. “Cyberattacks Triple in 2012, Akamai Says.” CNET. Accessed November 15, 2022. https://www.cnet.com/news/privacy/cyberattacks-triple-in-2012-akamai-says/.

Treverton, Gregory F., Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue. “Addressing Hybrid Threats.” Försvarshögskolan (FHS), 2018.

Tripathi, Suryakanthi. “Cyber: Also a Domain of War and Terror.” *Strategic Analysis* 39, no. 1 (January 2, 2015): 1–8. https://doi.org/10.1080/09700161.2014.980549.

Urbinati, Martina, and Sonia Lucarelli. “The Securitization of Cyberspace: Building the Cyber-Resilient European Union of Tomorrow,” n.d.

Van der Meulen, Nicole, Eun A. Jo, and Stefan Soesanto. “Cybersecurity in the European Union and beyond: Exploring the Threats and Policy Responses,” 2015.

Voudouris, Konstantinos. *The European Networks and Information Security Agency – ENISA*, 2005.

Wæver, Ole. *Securitization and Desecuritization*. Centre for Peace and Conflict Research Copenhagen, 1993.

Warner, Michael. “Cybersecurity: A Pre-History.” *Intelligence and National Security* 27, no. 5 (October 1, 2012): 781–99. https://doi.org/10.1080/02684527.2012.708530.

Wessel, Ramses A. “Cybersecurity in the European Union: Resilience through Regulation?” In *The Routledge Handbook of European Security Law and Policy*, 283–300. Routledge, 2019.

IT PRO. “What Is NotPetya?” Accessed September 15, 2022. https://www.itpro.com/malware/34381/what-is-notpetya.

Cloudflare. “What Was the WannaCry Ransomware Attack?” Accessed December 1, 2022. https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/.

Withers, Paul. “What Is the Utility of the Fifth Domain?” *Royal Air Force Air Power Review* 18, no. 1 (2015): 126–50.

Yetiv, Steve. “History, International Relations, and Integrated Approaches: Thinking about Greater Interdisciplinarity.” *International Studies Perspectives* 12, no. 2 (May 2011): 94–118. https://doi.org/10.1111/j.1528-3585.2011.00422.x.

Appendix: R Script

This Annex includes the R script for the targeted sentiment analysis of the 2013 Cybersecurity Act. The code for the other documents is available upon request.

```
# ---------------------------------------------------------------------------
#
# Thesis: Chapter II
# 2013 CSA and 2014 CDPF
#
#----------------------------------------------------------------------------
remove(list=ls())
cat("\f")

setwd("~/MBA Rotterdam/R/Tutorials/Data")
dir <- "/Users/shino/OneDrive/Documents/MBA Rotterdam/R/Tutorials/"

dirData <- paste0(dir, "Data/")
dirProg <- paste0(dir, "Programs/")
dirRslt <- paste0(dir, "Results/")

library(quanteda)
library(quanteda.textstats)
library(tidyverse)
library(readtext)
library(tm)
library(quanteda.textplots)
devtools::install_github("quanteda/quanteda.corpora")
library(seededlda)
library(stargazer)
library(dplyr)
library(rmarkdown)

# loading the data into R
rtextch2 <- readtext::readtext("C:/Users/shino/OneDrive/Documents/MBA
Rotterdam/R/Tutorials/Data/Data Thesis ch2")
tm::Corpus(VectorSource(rtextch2[["text"]]))
```

```
rtext2013 <- readtext::readtext("C:/Users/shino/OneDrive/Documents/MBA
Rotterdam/R/Tutorials/Data/Data Thesis ch2/CSA 2013.pdf")
tm::Corpus(VectorSource(rtext2013[["text"]]))

rtext2014 <- readtext::readtext("C:/Users/shino/OneDrive/Documents/MBA
Rotterdam/R/Tutorials/Data/Data Thesis ch2/CDPF 2014.pdf")
tm::Corpus(VectorSource(rtext2014[["text"]]))

corpus.2013 <- corpus(rtext2013, docid_field = "doc_id", text_field = "text")

summary(corpus) %>%
  head()

# cleaning up the data
corpus.2013 <- tokens(corpus.2013, what = "word", remove_punct = T, remove_symbols = T,
remove_numbers = T, remove_url = T,
                 include_docvars = T, verbose = T)

docvars(corpus)

# transforming the corpus into dfm
dfm.2013 <- dfm(corpus.2013)



# cleaning up the dfm
dfm.2013 <- dfm_remove(dfm.2013, pattern = stopwords("en"))
dfm.2013 <- dfm_remove(dfm.2013, pattern = cbind("shall", "council", "ec", "may"))

topfeatures(dfm.2013, n=50)

#exploring the data
textplot_wordcloud(dfm.2013, max_words = 35)
textstat_frequency(dfm.2013, 5)

#lexical diversity

textstat_lexdiv(dfm.2013) %>%
  tail() %>%
  arrange(desc(TTR))

# text strings
textstring.identification <- c("[Ii]ncident|[Tt]hreat|[Aa]ttack|[Rr]isk|[Dd]efence|[Cc]yber")
textstring.mitigation <- c("[Oo]bjective[s]|[Ss]olution[s]|[Pp]olicy]|[Ss]ecurity|[Pp]rotect[ion]|the Agency")
textstring.collective <- c("[Cc]ooperation|[Ii]nternational|NATO|[Tt]ogether|[Ff]acili|EU|[Mm]ember [Ss]tates")



# sentiment analysis

lsd.dict <- data_dictionary_LSD2015

sent.analysis.2013 <- dfm.2013 %>%
  dfm_lookup(dictionary = lsd.dict[1:2])
head(sent.analysis.2013)

sent.analysis.2013 <- sent.analysis.2013 %>%
  convert(to = "data.frame")

sent.analysis.2013 <- sent.analysis.2013 %>%
  mutate(length = ntoken(dfm.2013),
         sentiment.score = (positive - negative)/length)

sent.analysis.2013 %>%
  summary()

sent.analysis.2013 <- sent.analysis.2013 %>%
  mutate(sentiment.score.z.2013 = scale(sentiment.score))
sent.analysis.2013

# targeted sentiment analysis
tokens.corpus.2013 <- tokens(corpus.2013, remove_punct = TRUE, remove_symbols = TRUE)
tokens.corpus.2013 <- tokens_select(tokens.corpus.2013, pattern = stopwords("en"), selection = "remove") # slightly different way to remove stopwords from token objects
tokens.corpus.2013 <- tokens_tolower(tokens.corpus.2013)

# pattern threat identification string
tokens.corpus.2013 <- tokens_select(tokens.corpus.2013, pattern =textstring.identification, window
= 20, valuetype="regex")

dfm.documents.2013 <- dfm(tokens.corpus.2013)

documents.sent.analysis.2013.threatidentification <- dfm_lookup(dfm.documents.2013, dictionary =
lsd.dict[1:2]) %>%
  convert(to = "data.frame") %>%
  mutate(sentiment.score = (positive - negative))

documents.sent.analysis.2013.threatidentification

# pattern mitigation string
tokens.corpus.2013 <- tokens(corpus.2013, remove_punct = TRUE, remove_symbols = TRUE)
tokens.corpus.2013 <- tokens_select(tokens.corpus.2013, pattern = stopwords("en"), selection =
"remove") # slightly different way to remove stopwords from token objects
tokens.corpus.2013 <- tokens_tolower(tokens.corpus.2013)
tokens.corpus.2013 <- tokens_select(tokens.corpus.2013, pattern =textstring.mitigation, window =
20, valuetype="regex")

dfm.documents.2013 <- dfm(tokens.corpus.2013)

documents.sent.analysis.2013.mitigation <- dfm_lookup(dfm.documents.2013, dictionary =
lsd.dict[1:2]) %>%
  convert(to = "data.frame") %>%
  mutate(sentiment.score = (positive - negative))

documents.sent.analysis.2013.mitigation

# pattern collective string
tokens.corpus.2013 <- tokens(corpus.2013, remove_punct = TRUE, remove_symbols = TRUE)
tokens.corpus.2013 <- tokens_select(tokens.corpus.2013, pattern = stopwords("en"), selection =
"remove") # slightly different way to remove stopwords from token objects
tokens.corpus.2013 <- tokens_tolower(tokens.corpus.2013)
tokens.corpus.2013 <- tokens_select(tokens.corpus.2013, pattern =textstring.collective, window =
20, valuetype="regex")

dfm.documents.2013 <- dfm(tokens.corpus.2013)

documents.sent.analysis.2013.collective <- dfm_lookup(dfm.documents.2013, dictionary =
lsd.dict[1:2]) %>%
  convert(to = "data.frame") %>%
  mutate(sentiment.score = (positive - negative))

documents.sent.analysis.2013.collective
```