# Brave New World: NATO, the EU and the New Age of Cyberspace

Neven Ahmad


Master's Thesis in Peace and Conflict Studies

Department of Political Science

University of Oslo

Spring 2020

Word Count: 34,993

## Acknowledgement

This academic journey gave me the opportunity to explore cyberspace: the final frontier. The pages to follow depict the voyages of my mission to explore strange new theories and to seek out answers that both excited and frustrated me in the past year.

This mission would not have been possible without my incredibly patient supervisor Bruno Oliveira Martins. Your knowledge, dedication, and kindness helped guide me through this process. I am eternally grateful for your generosity.

I want to thank the interviewees who shared their time, knowledge and insight during a pandemic with a master student. I want to thank Peace Research Institute Oslo (PRIO) for providing me with a vibrant research community. Working alongside you PRIOites inspired me to dig deeper and work harder. I want to especially thank the Security Dynamics Group for their valuable feedback. I also want to thank my fellow master's students for your support in this process.

I want to thank my friends and family who supported me throughout it all. Lala, thank you for always cheering me up and making me laugh after a hard day of writing. Mom, your love and warmth helped me endure this journey. Andreas, your support, love, and encouragement was a driving force on this mission- you are the best partner an explorer could ever ask for.

Dad, none of this would be possible without your bravery and hard work. You are not only my rock but my mountain and everything I do - I do for you.

All mistakes and inaccuracies are my own.

## Summary

Cyberspace presents a new arena for international relations and order. As society becomes more reliant on this domain it increases vulnerabilities against cyber threats. While the EU and NATO have been long-time partners in security and defence within traditional domains, this thesis aims to explore how we can understand EU-NATO cooperation within cyberspace with regards to cyber security and defence. Previous literature has mainly focused on their shared membership and their efforts to avoid duplication. This thesis aims to contribute to the field by providing a critical lens to this partnership in cyberspace. Through a combined critical theoretical framework that centers the impact of technologies on society, this thesis argues that their partnership is representative of the larger phenomena of blurring the lines between pre-existing parameters between military and civilian, thus allowing for maneuvering that would otherwise be contested, and to reinforce a liberal order in cyberspace. This thesis combines Critical Security Studies, Critical Military Studies and Science and Technology Studies to conduct theory driven discourse analysis on EU and NATO discourse to analyze how we can think about their partnership in cyberspace. Expert interviews are used in this thesis not as a core methodological approach, but rather as additions that help color the analysis.

This thesis argues that while shared membership and EU-NATO efforts to avoid duplication is a large part of their cooperation efforts, this cooperation goes beyond convenience. The analysis finds that the EU and NATO do not conceptualize cyberspace and cybersecurity the same way, nor do they perceive the referent object within cyberspace the same. However, I argue that it is precisely due to their diverging conceptualizations that cooperation is mutually beneficial. As this thesis will illustrate, their cooperation blurs the lines between military and civilian, thus allowing each actor room to maneuver into conceptualizations of security and cybersecurity they would otherwise not have had the opportunity to explore. Lastly, this thesis illustrates that EU-NATO cooperation is part of a larger contestation within cyberspace to impose a liberal order through the values and norms they export into this domain. Therefore, it examines how cyberspace and cybersecurity influence EU and NATO, and in reverse how NATO and EU influence this new arena to establish a liberal order.

## Table of Contents

## Abbreviations

CERT Computer Emergency Response Team

| | |
|---|---|
| CI | Critical Infrastructure |
| CMS | Critical Military Studies |
| CSS | Critical Security Studies |
| EU | European Union |
| ICT | Information and Communications Technology |
| NATO | North Atlantic Treaty Organization |
| PPP | Public-Private Partnership |
| STS | Science and Technology Studies |

# 1. Introduction

Cyberspace, unlike traditional domains such as land, air and sea, is constructed by humans. As such, the way it is conceptualized and how various actors behave within this space can determines what it becomes, thus creating this space in our own image. As society's reliance on the domain increases, so too grows its vulnerability. With the recent outbreak of COVID-19, we have seen first-hand how when physical and international borders are closed, cyberspace becomes the only domain in which we can interact and escape. However, along with the opportunities that it presents, there is a progressive increase in concern over cyber threats. Cyber attacks against Estonia in 2007 and Georgia in 2008 along with cyber weapons such as the Stuxnet worm in 2010 – which targeted Iran's nuclear facilitates for the first time causing kinetic damage – has propelled this issue into the public discourse. In 2016 the impact of election interreference in the United States Presidential election broadened the potential threat cyberspace can present for democratic institutions, aside from critical institutions such as energy, transportation, telecommunications and public services.

International actors are trying to navigate a new arena that has, for the most part, lacked rigid international rules. This thesis narrows in on two actors: the North Atlantic Treaty Organization (NATO) and European Union (EU) as they cooperate to navigate the cybersecurity dimensions of this space. In 2014, NATO Allies declared that a cyber attack could trigger the collective defence clause (Article 5) of its founding treaty and in 2016 recognized cyberspace as a domain of military operations on the same level as land, air, and sea. The EU has developed various directives, agency and centers to face challenges this domain presents. This thesis aims to critically examine how we can understand EU-NATO cooperation in cyberspace with regards to cybersecurity and defence. NATO and EU were chosen for three main reasons. The first is that they are different; one is a military alliance that over the decades grew into an international organization, while the other, originally a regional and sectoral cooperation institution, grew into a state-like international organization whose competences spans a wide range of issues. Additionally, while NATO has security and defence at its core, the EU only more recently developed competence in these areas. These differences allow the thesis to critically examine how each conceptualizes cyberspace, cybersecurity, and its implications. The second is that they are both leading actors in the international community with norm setting powers with the potential to

influence what this space can become. Finally, this cooperation, between a military alliance and a mainly civilian organization, allows this project to critically examine the blurring of lines between the military and civilian domains, and to examine its possible implications. This blurring of the line is a central area of focus in this thesis, as cyberspace is a domain that – due to its dual-use nature – challenges pre-existing parameters on what security is and is not, the divide between peace and conflict, and civilian and military roles.

### 1.1 Research Question

This thesis question stems from a larger question on the impact of emerging technologies on pre-existing security environments and partnerships. Cyber technologies have seen a rapid evolution triggering a consequent permanent change in the threats this domain presents. Cyberspace, while not new, presents us with a man-made domain that can be shaped based on how actors conceptualize and behave in the space. This thesis aims to answer:

*How can we understand EU-NATO cooperation in cyberspace with regards to cybersecurity and defence?*

While there is a large body of literature on the relationship between the EU and NATO, the same cannot be said about EU-NATO cooperation in cyberspace and even less so on EU-NATO cooperation in cyberspace from a critical lens. This thesis aims to approach this question from a critical theoretical framework that ensures that the technological impact of cyberspace on this political relationship is not overlooked. As is illustrated in the literature review, the majority of the research conducted on EU-NATO cooperation in cyberspace is based on problem-solving frameworks that point to the challenges the two face in these efforts and how these can be solved. The studies largely take these two actors' reasons for cooperation as a given, as they share most of their members and thus aim to avoid duplication of efforts. This thesis seeks to contribute to this body of literature by answering this problem from a critical lens that centers the fluidity of cyberspace, examining the political impact of emerging technologies, the relational and negotiated nature of concepts of security, and the impact of these actors' conceptualizations and practices within this domain on the creation of the space.

### 1.2 Scope

Due to the limited nature of a master's thesis, certain limitations and parameters are set to ensure a thorough research endeavor. Therefore, the focus of the question limits the actors studied, narrowing it down to the EU and NATO. Due to the methodological approach of discourse analysis, the source material from both the EU and NATO are limited to strictly official documentation material that has at the very least mentions of "cyberspace", "internet", and "cyber". However, by limiting the documents in this sense, the study can span a long period of time ranging from 2002-2020. In addition to the discourse analysis, four expert interviews were conducted that have helped provide insight on the subject manner and will be used in this thesis as an addition rather than a core methodological pillar.

### 1.3 Structure of the Thesis

Following this introductory section, chapter 2 provides a literature review that presents the current landscape on this question. The chapter is broken down into multiple areas of study as the thesis question is at the intersection of several fields: international relations, with the EU-NATO cooperation component; the debate on what kind of actor the EU is and is becoming; discussions on EU-NATO cooperation in traditional domains in terms of their security and defence cooperation; the debates on the nature of cyberspace, such as cyber warfare, cyber power, securitization of cyberspace; and finally, international relations in cyberspace. Chapter 3 provides background information on both EU-NATO cooperation in traditional domains and EU-NATO cooperation in cyberspace and the challenges they face in their cooperation. Chapter 4 provides the theoretical framework that combines Critical Security Studies (CSS), Critical Military Studies (CMS) and Science and Technology Studies (STS), and how this thesis intertwines these theories to produce a framework that provides a critical lens to this question that has previously not been used, mainly taking security as a "derivative concept" from CSS, the blurring of the line between military and civilian from CMS, and the concept of co-production from STS. Chapter 4 presents the research methodology of discourse analysis to illustrate how discourse provides the parameters of possibilities in this space. Chapter 5 illustrates the theory-driven discourse analysis of representative statements from the documents, crossed with input from the expert interviews. Chapter 6 presents the discussions portion of the thesis that dives into the implications of the analysis of blurring the lines between civilian and military and the diverging conceptualization of

cybersecurity and cyberspace by both the EU and NATO. Chapter 7 concludes this thesis by answering the thesis question, providing self-reflection and recommendations for future research.

## 2. Literature Review

The European Union (EU) and the North Atlantic Treaty Organization (NATO) are entities with differing identities and purposes. In order to analyze their cooperation in the field of cyberspace in relation to security and defence, this thesis will first illustrate the varying components of this question and their subsequent discussions. Therefore, this literature review first aims to provide the state of the art on the nature of each institution regarding the kind of power they wield. Second, it examines the nature of their cooperation with one another in traditional domains relating to security and defence. Third, it provides a review of how cyberspace is conceptualized, particularly its governance, the securitization of this domain, the intersection between cyberspace and international relations, and the gaps in critical engagement with this field. Finally, the chapter provides an overview on EU-NATO cooperation in cyberspace in order to uncover the academic gaps in this field.

### 2.1 NATO, the EU, and the Power they Wield

NATO as a military alliance is understood to provide defence, while the EU, an economic power, has only recently entered the field of security and defence. In many ways, then, the EU is perceived as a "junior partner" in the relationship where security is concerned (Smith & Gebhard, 2016). There is, however, a distinction between security providers and defence providers. Defence implies a policy that aims to protect citizens and territories from attacks including or primarily using military force. By contrast, security refers to a much broader range of policy areas such as political, economic, social, police, etc. to tackle threats (Tardy, 2018). EU's role and identity is an area of rich discussion, Martin explains that "the way the EU portraits itself influences the way it acts externally, but also impacts on the way it evaluates *a posterior* those same actions" (Martins, 2011, p. 346). An example of this idea, Martin points out, is the "distinctiveness theory", that is, the "the idea according to which the EU is a *different* (read *better*) global actor due to its self-declared goal of promoting peace through integration, human rights, democracy, does not echo the most common external perceptions" (Lucarelli & Fioramonti, 2010, p. 222). The EU's image as a security provider rather than a defence provider has contributed to the perception of it as a "civilian power". This "civilian power" narrative has been attributed to the belief that Europe can only guarantee its own strategic security by ensuring sustainable global development (Manners, 2002). However, there is tension on whether the EU can still be considered a "civilian power". Simon

Duke states that the EU is no longer a civilian power and argues that it must endorse the assumption of "hard" security roles as soft power is no longer adequate to properly defend its interests (Duke, 2017). Manners (2002) describes the EU as a "normative power" and conceptualizes it as an influencer in international norms through a normative belief that "the EU *should act* to extend its norms into the international system" (Manners, 2002, p. 252).

Many authors have questioned the notion that the EU is, first and foremost, a normative power. In relation to cyberspace and cybersecurity, Helena Carrapico and André Barrinha conduct a structured approach to the issue of coherent in EU security and find that while there are road blocks, "the EU has an explicit ambition to be a coherent security actor" (Carrapico & Barrinha, 2017, p. 1267). Åsne Kalland Aarstad (2015) provides a thorough overview of critical approaches to EU's foreign policy by engaging in discussions on the common security and defence policy and the EU as an international actor (A. K. Aarstad, 2015). Michelle Pace adds to this discussion by arguing that conceptualizing the EU as a normative power limits the EU's global reach (Pace, 2007). However, Bachmann (2013), argues that "civilian" and "power" are not mutually exclusive and that the EU's ability to influence global politics is dependent on its civilian and normative orientation which legitimizes its role on a global stage. For Bachmann, both the EU's "civilian" and "power" titles are part of its geopolitical identity and role (Bachmann, 2013). Additionally, Bachman makes a strong argument for critically engaging with the views on the EU from the outside, and explains that external perceptions of the EU differ from the views that are represented in official EU geopolitical discourse (Bachmann, 2013; for further readings please refer to Chaban et al., 2006; Lucarelli, 2007).

Nicolaïdis and Lacroix (2003) explain that there are two different visions in the context of the EU in international affairs. The competing ideas asking "should Europe exist globally through power projection or attraction, as a "hegemon" or as a "beacon", as a "superpower" or as a "model"?"(Lacroix & Nicolaïdis, 2003). These are the same questions that we ask today, when we examine the role of the EU in cyberspace. However, as this this thesis's focus is not the nature of the EU, I will utilize Karen E. Smith's perspective on how to approach this part of the discussion. Smith (2005) argues that we should be concentrating on what the EU does rather than what it is (K. E. Smith, 2005).

## 2.2 EU-NATO Cooperation in Traditional Domains of Security and Defence

For this thesis to explore EU-NATO cooperation in cyberspace, it is important to first understand the discussions and issues raised with their cooperation in traditional domains. Overall, the literature on EU-NATO relations in the field of security and defence paints a picture of a balancing act. Jolyon Howorth coined the term "Euro-Atlantic security dilemma" to describe this tension (Howorth, 2005). The literature on EU-NATO relations in the field of security and defence mainly focuses on two key areas. The first is EU-NATO cooperation in the field of security and defence, and the challenges they face (Lété, 2017; Simion, 2018; H. Smith, 2019; Szewczyk, 2019; Tardy & Lindstrom, 2019). The second is the discussion on EU strategic autonomy (Camporini et al., 2017; Fiott, 2018; Howorth, 2017, 2018; Posen, 2004).

The Euro-Atlantic security dilemma illustrates an internal tension within the EU regarding whether to build security and defence capabilities. Britain represented the fear that a strong European drive in the direction of security and defence autonomy would create an isolationist response from the United States. This position was countered by France who argued that the United States would welcome this drive and would eventually result in the United States taking Europe as a serious ally (Howorth, 2005, 2019). This tension can be partly attributed to the ambiguous position of the United States and by extension NATO, on their hopes for European defence and security. On the one hand, the United States and NATO actively encourages the EU to develop strong defence capabilities in order to protect the region. On the other, there is a fear that this capacity can lead to Europe obtaining the capabilities to one day challenge the United States on the world stage (Posen, 2004).

Regardless of this tension, Howorth (2018) argues that if the EU is serious about its drive to become a strategically autonomous actor it must develop its capacity in security and defence to merge CSDP into NATO and proceed to take over command of the major NATO agencies. Thus, allowing the United States to focus on areas in the world that are of strategic importance to them, and as a result, ending the EU's dependency on the US (Howorth, 2018). He cites Dwight D. Eisenhower who believed that "[i]f NATO is still needed in 10 years, it will have failed in its mission" (Howorth, 2017).

Ivaylo Angelov provides an economic perspective to EU-NATO cooperation in the field of security and defence. Angelov argues that due to the evolving security environment, with the

increase in Russian aggression and emerging domains such as cyberspace and energy concerns, there is a gap between the "old" and the "new" EU member states in terms of their capabilities and resources assigned to defence. Therefore, it is more important now, due to the economic challenges and the lack of proper defence budgets, to ensure an EU-NATO coordinated approach to resources and costs so member states are not spending more but rather spending wiser (Angelov, 2019). While the EU and NATO cooperation faces challenges – one critical issue being Cyprus-Turkey relations – from an economic standpoint, it is vital that the EU and NATO pool their resources together more efficiently, and strengthen their integration process to ensure synergy in this field in order to meet emerging security challenges (Angelov, 2019).

While policy coordination between the EU and NATO can be challenging, and considering that the two organizations are not always in sync as they face these new challenges, Eduard Simion argues that a close examination reveals that both organizations have proved that they are able to re-invent themselves to provide what the evolving security environment needs, and are versatile enough to survive these evolutions (Simion, 2018). Additionally, Nina Græger illustrates this versatility by analyzing the relationship through a micro-analysis lens, and applies a practice approach to find that there has been a gradual shift from formal to informal cooperation between EU and NATO personnel, e.g. civilian and military staff, diplomats, and that this is a reaction to the deadlock on cooperation presented under the Berlin Plus agreement (Græger, 2017). This illustrates versatility and ability to change frameworks, but Simon Smith (2011) illustrates that the informal actors, such as military actors and international staff, who coordinate and cooperate with one another, are experiencing institutional fatigue (S. J. Smith, 2011). These cooperation issues the two organizations display in traditional domains are set to spill over into cyberspace. However, in order to understand how this can happen, a dive into the various academic discussions present with regards to cyberspace.

### 2.3 Cyberspace

Cyberspace literature presents us with a new and vast domain where there are competing understandings of this arena and its impact on traditional concepts of warfare, power, securitization and international relations. These discussions are mainly tackling with whether this is a new domain, and these concepts that we have in traditional domains transfer over to cyberspace or not.

In addition to cyberspace as a new domain, cyberwar can be viewed as a new way of conducting war based on a high-tech model of warfare (Mehmetcik, 2014). One of the prominent discussions in the field of cybersecurity and defence is whether cyber threats such as cyberwar are real or exaggerated. On the one side, there are scholars who argue that cyberspace presents a real and unavoidable security issue and have the potential to damage our way of life (Ducheine, 2016; McConnell, 2009; Petr Hruza & Cerny, 2017; Siroli, 2018; Stone, 2013). In opposition are those who claim that the threat has been overstated and therefore believe that there is not enough evidence to foresee unavoidable future cyberwars that militaries should be ready for. In this latter camp, scholars argue that as a concept, cyberwar cannot be a war in terms of classic theory of war or that as it stands, cyber attacks have not had a significant amount of impact on battlefields (Betz & Stevens, n.d.; Gray, 2013; Kostyuk & Zhukov, 2019; Libicki, 2009; Rid, 2012a, 2012b; Yoran, 2010).

The next discussion that takes place is whether cyberspace diffuses power or if it reinforces the existing global power dynamic. Joseph Nye, an expert on power, explains that "[t]he characteristics of cyberspace reduce some of the power differentials among actors, and thus provide a good example of the diffusion of power that typifies global politics in this century" (J. Nye, 2010, p. 1). However, when critically examining the current reality of the domain, both Betz and Carr argue it does the complete opposite; instead it reinforces the already existing asymmetry and power dynamics. For Betz, cyber power rewards already powerful states (Betz, 2012; Carr, 2015).

### 2.3.1 Securitization of Cyberspace

Myriam Dunn Cavelty makes the point that the act of framing a threat is a choice that comes with political and societal effects. She argues that militarization of cyberspace through focusing on the strategic-military aspects of cyber security means subjecting it to the rule of a zero-sum game. This leads to the creation of an image of the enemy that might not exist in reality, which wrongly leads states into believing that they can control this domain, which she argues they cannot (Dunn Cavelty, 2012). Control of cyberspace leads to a larger discussion on cyber governance with  Furthermore, Cavelty extends this to argue that the reason why the current approaches to cyber-security are not working is due to the lack of focus on "people", which makes it easier for state actors to militarize cyber security and (re-) assert their power in cyberspace, thereby

overriding the different security needs of human beings in that space (Dunn Cavelty, 2014). For Cavelty, this new space must be examined from a balanced approach in order to avoid policy overreactions with unnecessary costs and uncertain benefits.

### 2.3.2 Cyberspace and International Relations

The literature at the intersection between cyberspace and international relations is sparse, mainly due to it being a relatively new field of study. However, within this space there are varying opinions on how international relations operate and whether the theories we have for the physical world can apply or should apply to the cyberworld.

Joseph Nye makes a comparison between the cybersecurity research to the time period where nuclear weapons were introduced into international relations, and the disturbance this new discovery caused. Illustrating that, much like the strategic and theoretical work done in the early days of nuclear development, the academic work on the impact of distrusting technologies will lack empirical content (J. S. Nye, 2011). Tim Stevens echoes this sentiment and points to the lack of diversity in the theory and methods used to understand this evolving environment and to comprehend the political responses to its problems (Stevens, 2018).

There are, though, some exceptions to this lack of academic diversity in the field. The first is the increasing literature on the securitization of cybersecurity through a Science and Technology Studies (STS) lens which provides International Relations and Security Studies with an added level of nuance and insight. A growing field critically examines the construction of cyber threats and identifies the tensions between political claims, such as cyber-doom scenarios, and objective conditions (Conway, 2008; Dunn Cavelty, 2008, 2013, 2014, 2014, 2012; Hansen & Nissenbaum, 2009; Lawson, 2013; Warf, 2015). In addition to STS, there is rich literature on risk and governmentality which takes a critical approach to importing security issues into cyberspace, and questions whether cyberspace can be governed or not (Barnard-Wills & Ashenden, 2012; Boyle, 1997; Deibert & Rohozinski, 2010; Demchak & Dombrowski, 2011; Fahey, 2014; Fliegauf, 2016; Franzese, 2009; Joyner & Lotrionte, 2001; Mattice, 2014; Mihr, 2014; Schmitt, 2014).

The second is the emergence of the study of “cyber-diplomacy”, which is a response to geopolitics spilling over into cyberspace. André Barrinha & Thomas Renard define cyber diplomacy as “the use of diplomatic resources and the performance of diplomatic function to

secure national interests with regard to cyberspace" (Barrinha & Renard, 2017, p. 355). They argue that cyber-diplomacy is an emerging international practice attempting to construct a "cyber-international society" by bridging the national interests of states with world society dynamics (Barrinha & Renard, 2017). Barrinha & Renard (2020) continue this work on cyber-diplomacy by exploring how power dynamics are evolving in cyberspace. This includes how norms, values, and institutions are challenged and created (Barrinha & Renard, 2020). The authors explain that the liberal order that was established under US leadership post WWII, which consisted of norms such as international law, values such as free trade, democracy and human rights, are behind us, and that we are now in a post-liberal world order, which widely means a "post-western" or "post-American" one (Barrinha & Renard, 2020, p. 4).

The discussion on cyberspace governance and risk mainly focuses on whether cyberspace *can* be governed or if it *should* be governed and whether the risk that is attributed to this space is accurate or overstated. Barnanrd-Wills & Ashenden (2012) use governmentality and discourse analysis approach to analyze cyber security literature, and find that the discourse constructs cyberspace as "ungovernable, unknowable, a cause of vulnerability, inevitably threatening, and a home to threatening actors" (Barnard-Wills & Ashenden, 2012). This is very much in line with Boyle (1997), who claimed that cyber space cannot be controlled. This line of argument tends to originate from a premise that due to the interconnection of this domain and the general globalization trend prevents states to control it, because unlike physical domains, cyber does not stop at a national border (Joyner & Lotrionte, 2001).

On the other side of the discussion are claims that the current state of cyberspace is comparable to the wild west and is in need of governance structure, such as laws and regulations and increased responsibility on software and hardware producers (Mattice, 2014). Thus, giving rise to a cybered Westphalian age in which borders are negotiated and international relations extends beyond the physical and into the cyber (Demchak & Dombrowski, 2011). Unlike scholars who believe that the space cannot be governed, Franzese (2009) systematically illustrates that this new domain is not immune to control, in this case through state sovereignty. This argument is in alignment with The Manual Expert group which explains that while cyber activities are interconnected, they are still conducted by both people and machines that are subject to jurisdiction of states (Schmitt, 2017)

In this discussion, as mentioned previously, the different camps seem to be talking past each other as they argue whether cyberspace *can* be governed or whether it *should* be governed. Deibert & Rohozinski (2010), have some insight on why this might be. They conceptualize cyberspace security and divide it into two connected dimensions of risks. The first "risk" describes the physical components of computers and communication technologies which can be described as the "risk to cyberspace". The second is "risks" that come from cyberspace and are facilitated or generated by its technologies, but do not directly target the infrastructure. Those can be described as "risks *through* cyberspace". Where there is a gap in international consensus is on the second aspect of risk. This leads the authors to argue that the inconsistency between the two types of risks is what has led to the current contradictory policies and inadequate outcomes. (Deibert & Rohozinski, 2010)**.**

To govern this domain, it is vital that we understand that it is at the intersection of public security concerns through Critical Infrastructure Protection (CIP) and private security concerns through protection of private property rights and civil liberties. To navigate this, Public-Private Partnerships (PPP) have been embraced as the best way to meet the challenges of cybersecurity as it enables cooperation between the private and public (McCarthy, 2018). Benjamin Farrand and Helena Carrapico explore how these partnerships blur the lines between public and private in cybersecurity, illustrating how private actors, due to their perceived knowledge and expertise in the field, are incorporated into security-related regulatory (Carrapico & Farrand, 2018, p. 214). Bruno Oliveira Martins and Christian Küsters argue that hybrid nature of public-private endeavors along with their centrality of technological expertise make these partnerships "less visible", this is particularly relevant to dual-use technologies (Martins & Küsters, 2019). The governance structures that are established will have to consider the private sector as one of the key actors in this new space. However, there is tension between national governments and their private sectors regarding cybersecurity. Madeline Carr argues that this is due to the disconnected expectations from both partners (Carr, 2016). Carr explains that on the one hand the government regards privately owned and operated critical infrastructure as a key component of national security, but that it is reluctant to issue these private companies formal mandate to oversee network security. On the other hand, the private sector does not want to accept responsibility or liability for national cyber security (Carr, 2016).

### 2.3.3 Gap in Critical Engagement

McCarthy makes an insightful point, which is that the literature in this area has focused on the division between public and private, state and market, and political and economic, but has failed to reflect on them from a broader theoretical perspective. He states that this includes analyzing them and their place in reproducing specific forms of political order by using critical theory to place the discussion in a larger conversation on the constitution of political order and the political economy of liberal democratic societies (McCarthy, 2018). Perhaps one of the exceptions to this is Madeline Carr who critically examines the multi-stakeholder model of global internet governance and the legitimacy and accountability of the "rule-makers" and "rule-takers", and finds that it reinforces existing power dynamics (Carr, 2015). From the literature, it is evident that McCarthy (2018) and Stevens (2018) have a point when drawing attention to an academic gap for critical engagement with this domain, both in its securitization and its governance.

One of the areas of study to critically engage with is the "blurring of lines". As part of emerging technologies and domains, which cyber threats and cyberspace itself is part of, cyber helps to create postmodern warfare. Namely, that emerging technologies and domains, such as cyber, blur the line between peace and war. George R. Lucas argues that while these technologies threaten to make war more pervasive, they also offer potential for decreasing the indiscriminate destructive power of war (Lucas Jr, 2010). Hand-Georg Ehrhart echoes this sentiment and adds that because cyber-attacks are hard to identify it creates an ideal field for covert operations from a distance, thus contributing to the change of warfare on all levels and enables new forms of intervention (Ehrhart, 2017).

There is a trend of "de-bounding" that takes place both between the forms of warfare, but also between war and peace. Ehrhart explains that the increase in civil-military forms of warfare, which is widening the grey zone between war and peace, is in part due to states not wanting to fully commit to a fully visible operation, such as Iraq or Afghanistan. Instead, opting for widening the grey zone which could increase room for political maneuvering and blurring not only the lines between peace and war, but also blurring their own responsibilities. This is especially incentivizing for democratic states as it is harder to sustain support for "war of choice". Ehrhart points to an interesting consequence of this blur, which is that as military and civilian lines are made indistinct, it could contribute to the militarization of society. We can see that cyber-attacks have been

willingly blurred or legitimized in the case of Estonia where civilian hackers organized attacks on the state as their response to a political decision. Or in the case of Ukraine, where the lines between Russian military force and civilians were blurred for the first stage of the annexation.

This domain provides a transitional environment for individuals and states to easily move from military to civilian and vice versa. Critical Military Studies can provide a theoretical view which questions strict boundaries such as civilian versus military, but also what is "inside" the military and what is "outside" the military apparatus (Basham et al., 2015).

### 2.4 EU-NATO Cooperation in Cyberspace

The academic literature on EU-NATO cooperation in cyberspace is largely limited and provides problem-solving analysis, thus there is a lack of critical engagement with their cooperation in cyberspace. László Kovács provides a comparison of the cyber security strategy of the EU to the cyber defence policy of NATO, and while the text provides technical information, it lacks a theoretical analysis (Kovács, 2018). Bruno Lété and Piret Pernik (2017) provide a short review of EU and NATO cooperation in cyberspace along with the challenges they face and ways of overcoming those challenges which include their lack of shared situational awareness and information sharing, and lack of joint cyber exercises. The second area of literature on this topic is in the form of a persuasive case for NATO-EU cooperation in cyberspace and the importance of a coordinated approach in this domain (Lété, 2017; Rugge, 2012). Piret Pernik stresses the need for stronger cooperation between the EU and NATO and tracks how cyber threats were first introduced to each organization, and how their understandings of them have evolved, with an emphasis on NATO's approach to find that the EU has been lagging behind NATO in developing comprehensive cybersecurity policies (Pernik, 2014).

Darius Štitilis, Paulius Pakutinskas & Inga Malinauskaitė conduct a comprehensive analysis on EU-NATO cybersecurity strategies and compare them to their member states' cyber security strategies (Štitilis et al., 2016). Their work provides an insightful reason as to *why* the EU and NATO are significant in this space. They state that because cyber security is not internationally regulated, this increases the importance of NATO and the EU as they can provide a path forward. Their study finds that regardless of their shared goals, assurance of cyber resilience, their strategies and norms differ.

## 2.5 Academic Gap

As a topic, there is an evident academic gap on EU-NATO cooperation in cyberspace. In general, there is a gap in critical theoretical approaches to examine the level of threat this domain poses, the militarization of this domain, and how this new space is perceived by both member states and organizations like NATO and the EU. Štitilis et al. provide significant insight into how cyber security is perceived differently by NATO and the EU Member States, which is problematic as one of the key takeaways from the technical analysis has been that a critical point of cooperation is that of shared situational awareness in this space. Additionally, there is a gap in critically engaging with this material through conceptualizing this space as blurring the line between civilian and military and war and pace, both in EU-NATO cooperation on its own, but also due to the dual-use nature of this domain.

# 3. Background

This section aims to provide a general overview of EU-NATO cooperation in traditional domains and their dynamic and then provide an overview of their cooperation in cyberspace along with the obstacles facing this endeavor.

## 3.1 EU-NATO Cooperation

EU-NATO cooperation in cyberspace is an extension of an already existing defence cooperation between the two entities. Currently, through the Joint Declaration in 2016 and 2018, NATO and the EU cooperate in seven different areas: countering hybrid threats, operational cooperation in the maritime domain, defence capabilities, defence industry and research, cyber security and defence, exercises and resilience of partners (NATO & European Union, 2016, 2018). EU-NATO partnership is imperative, Thierry Tardy and Gustav Lindstrom identify three areas of division of labour between the two organizations, namely geography, the nexus between defence and security, and the nexus between internal and external security (Tardy & Lindstrom, 2019).

Geographically, they face similar threats from Russia's resurgence and cyber threats, and instability in their southern perimeters. This presents an advantageous objective for both parties to create synergies, thus maximizing their capacities. Historically, NATO was meant to only operate in the North Atlantic region north of the Northern Tropic (NATO, 1949). However, after the 1990s, the operations in both Afghanistan and Iraq have shown that traditional regional restrictions no longer apply. The EU has acknowledged the importance of NATO defence of its members but has emphasized that Europeans must be able to defend themselves against external attacks by being better equipped. In the EU's 2016 global strategy it states: "as Europeans we must take greater responsibility for our security. We must be ready and able to deter, respond to, and protect ourselves against external threats" (European External Action Service, 2017, p. 19). As the EU is expanding its responsibilities in the security field, the need for a division of labor is critical as not to replicate security tasks. This sentiment was clearly outlined in NATO Secretary General Jens Stoltenberg response to EU defence projects such as the European Defence Fund (EDF), PESCO, and military mobility. He clearly stated that these initiatives are welcomed, but that "the EU efforts must not compete with NATO, must not duplicate NATO, because NATO remains the bedrock for European security"(Stoltenberg, 2018a).

When exploring EU and NATO operations, it is evident that while there are certain areas in which they assist one another in their respective operations, there are no apparent overlaps. For example, in the case of NATO's presence in three Baltic States and Poland following Russia's activities in Ukraine, EU assistance came through sanctions against the Russian oil sector (Fjærtoft & Øverland, 2015). While there were sanctions against Russia, there was a lack of EU response within its Common Security and Defence Policy (CSDP) framework. In comparison, there are operations and regions where the EU operates where NATO does not, such as the EU-led mission in Sub-Saharan Africa, in which NATO is absent south of Libya. Additionally, the EU is able to conduct missions in areas that NATO would have a harder time in due to political sensitivities such as the Palestinian territories and Georgia (Tardy & Lindstrom, 2019).

The division of labour is also clarified more when looking at the nature of EU and NATO as organizations. NATO-EU cooperation operates on two different axes, with NATO as a defence force and the EU as a security force. Additionally, an axis between civilian and military exists. This axis is especially important when examining cyberspace due to its dual-use nature. While neither organization is limited to security or defence, by mandate NATO is a defence alliance while the EU has a much larger mandate and one which requires a lower level of "use-of-force". This is also evident in the operations that both organizations take part in such as those in Kosovo and Afghanistan. The EU's involvement in Kosovo was through the launch of the EULEX mission by the CSDP in 2008 that aimed at assisting the Kosovo authorities in establishing sustainable and independent rule of law institutions (European Union External Action, 2008). In contrast, NATO's KFOR mission was a more military based operation. In addition to the security versus defence axis, the EU and NATO present yet another differentiating feature which is external versus internal. While NATO has the mission of protecting its allies from external attacks and threats, the EU has the capacity and range to act in internal affairs, which is exceptionally helpful when the case of cyberspace is introduced. The EU has the unique ability to act both externally, through the CSDP, and internally through the European Commission and Home Affairs as an internal actor (Tardy & Lindstrom, 2019).

### 3.2 EU-NATO Cooperation in Cyberspace

Cyberspace presents EU and NATO with the opportunity to cooperate in a domain that currently lacks the rigid international laws of the physical world and international regulatory

bodies through the United Nations. Therefore, their cooperation in this space is even more important *because it lacks international regulatory structures.* However, many of the same challenges to cooperation that present themselves in traditional domains apply in cyberspace. Mainly, their lack of shared situational awareness and information sharing, their uneven levels of preparedness, and cyber resilience (Lété & Pernik, 2017). EU-NATO cooperation in cyberspace is an extension of their close alliance in traditional domains.

As complementary partners in this space, the EU and NATO signed a Technical Arrangement on Cyber Defence in February 2016 between NATO's Computer Incident Response Capability (NCIRC) and the EU's Computer Emergency Response Team (CERT). The Technical Arrangement strengthens cyber defence cooperation through information sharing, joint training, research and exercises (NATO, 2019). However, as this text will later discuss, one of the challenges that faces this cooperation is the lack of information sharing and situational awareness in cyberspace.

The most pivotal steps towards cyber cooperation were through two signed Joint Declarations, one in 2016 and the other in 2018. The 2016 Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of NATO, saw both the EU and NATO listing expanding cooperation "on cyber security and defence including in the context of our missions and operations, exercises and on education and training" as an "urgent need", and cooperation in this area as a strategic priority (NATO & European Union, 2016). EU-NATO cooperation in cyber security and defence included fostering cyber defence research and technological innovation cooperation by strengthening cooperation between the EU, NATO, and the NATO Cooperative Cyber Defence Centre of Excellence to explore innovation in the area of cyber defence (NATO, 2016). However, how can the Joint Declaration continue given EU and NATO's different approaches to combating cyber threats? Vendela Rupp argues that it can continue if the EU follows the decisions made by NATO, meaning it will have to continue to develop its capabilities that compliment those of the Alliance or risk falling behind (Rupp, 2019). In 2017, a common set of new proposals on the implantation of the Joint Declaration was added to advance exchange between staffs' relevant good practices concerning the cyber aspects and implications of crisis management and response, in addition to operational aspects of cyber defence including analysis of threats and malware information, with the objective of improving

joint understanding of the field and finding potential synergies (NATO & European Union, 2017). The 2018 Joint Declaration reaffirmed cooperation commitment on responding to cyber-attacks among other crises, and emphasized that EU-NATO cooperation was essential (NATO & European Union, 2018).

### 3.3 Obstacles Facing EU-NATO Cooperation

As previously illustrated, EU-NATO cooperation in cyberspace is both mutually beneficial and necessary. While they both separately approach cyberspace differently, with the EU taking a holistic approach and NATO approaching it strictly from an external defence approach, they both face similar threats to their institutions and their Member States. There are three main obstacles that stand between NATO-EU cooperation: lack of situational awareness and information sharing, uneven levels of preparedness and cyber resilience, lack of joint cyber exercises, training, and education (Lété & Pernik, 2017).

The lack of situational awareness that exists in cyberspace stems from the ambiguous nature of this new domain. EU and NATO cooperation faces a perception challenge. States conceptualize, respond to and interact with this new space differently. This can be difficult when a shared response is required in cases of defence and security. However, while NATO member states and EU member states are part of each respective agreement, it is evident that member states do not share situational awareness in this space with one another. A 2016 Comparative study of the provisions of national cyber security strategies of EU and NATO member states illustrates that regardless of their shared goals of cyber resilience, member states have different cyber security strategies and norms than the institutions they are aligned with (Štitilis et al., 2016).

The EU approach to cyberspace is enshrined with the belief that the EU's core values apply in this new domain as they have in traditional domains. The EU's focus on protecting fundamental rights, freedom of expression, personal data and privacy, illustrate a holistic approach to cyberspace, ensuring both the protection of the state, but also the protection of the individual from external actors and potential state infringements on these fundamental rights. An extension of this holistic approach is through the EU's focus on ensuring that all EU citizens have access to this new space. When perceptualizing this space, the EU's internet policy and governance is a priority based approach that emphasizes a strategy that is democratic, efficient, and multi-stakeholder

governance structured (European Commission, 2014). Finally, as previously mentioned, the EU's strategy has a shared responsibility approach to security. This comprehensive approach to this space is in line with the EU's institutional identity. Alternatively, NATO does not clearly identify cyber security principles in their documents. The main concepts are principles of prevention, detection, resilience, recovery and defence. NATO recognizes international law such as humanitarian law and UN Charter to apply in cyberspace, but it does not go further in specifying rights that are particularly specific to operating in cyberspace such as privacy and freedom of expression (NATO, 2014b). Furthermore, while this thesis is not focusing on EU-United States, cooperation, their different approaches to this space is worth noting. George Christou states that EU's conception of cyber defence is grounded in a security as resilience logic- to self-protect which is in a premise that in opposition to the US who operates within the logic of cyber offence and an aim to enhance cyber weapons in order to ensure it is well equipped "for fighting the cyber enemy" (Christou, 2016, p. 180).

Information sharing between NATO and the EU is crucial in detecting threats early. However, due to the various levels of governance, this can become increasingly complicated. Hypothetically, if a state such as Canada who is a member of NATO, but not the EU, detects a cyber-attack, it would first share this information with its internal governance systems such as the Canadian National Defence. Then, this information is triaged to NATO commands, and NATO commands shares this information with the EU, where this information would trickle down to EU states to check for the specific vulnerability in their system. The speed of which information shared is one challenge, but a greater challenge is whether states decide to share this information. For states, there is a reluctance to share threat intelligence, technical information about cyber incidents, and sharing information on their vulnerabilities and preparedness (Lété & Pernik, 2017). EU and NATO member state information on cyber capabilities are voluntary, which means that EU and NATO do not have a clear picture of their respective members' capabilities in cyberspace and in extension, their ability to respond and defend against specific cyber threats. As previously mentioned, information sharing is critical in ensuring a joint response. However, there is currently no immediate channels for sharing classified information between the EU and NATO (Lété & Pernik, 2017).

The third challenge that the EU and NATO face in cyberspace is that of unequal levels of preparedness in cyber capabilities and resilience. As it stands, the recommendations made by NATO and the EU to their respective member states are largely non-binding. This disconnect results in an environment in which member states' cyber capabilities are "not interoperable, not complementary, or are not coordinated" in a way that national efforts reinforce common EU or NATO cyber objectives (Lété, 2017, p. 31). This creates a gap between member states' civilian and military cyber capabilities and detection abilities. The fourth challenge is the lack of joint cyber exercises, training and education. The EU and NATO have held one military joint exercise in 2003 which did not include cyber capabilities. The joint trainings that was planned for 2007, 2010, and 2014 did not come to fruition. While the EU and NATO hold exercises and training with their member states, a joint exercise in this field has yet to take place.

# 4. Theoretical Framework

The field of cyberspace and particularly the study of EU-NATO cooperation in cyberspace can benefit from critical analysis. While IR traditional theoretical models can be helpful when analyzing the international relations dimension of EU-NATO cooperation, they often lack a critical engagement with the material. What we end up with is theoretical frameworks that try to fit cyberspace, and even more so EU-NATO relations in cyberspace, into pre-existing boxes, thus failing to acknowledge the complexities of the space itself. Therefore, this thesis uses Critical Security Studies (CSS), with a sub-section of Critical Military Studies, and Science and Technology Studies (STS), to analyze cyberspace and the impact the complexities within this domain have on the pre-existing relationship between the EU and NATO.

## 4.1 Critical Security Studies

The decision to equip this thesis with CSS is due to this theoretical tradition's ability to provide insight where other traditional theoretical frameworks would come up short. It is important to clarify that CSS is more of an orientation than a strict theoretical label (Peoples & Vaughan-Williams, 2014). This elasticity allows us to analyze this field as a question rather than a given solution. Where this theoretical framework is best utilized within this thesis is in its engagement with well understood boundaries and the concept of security as a derivative concept. Within CSS, Critical Military Studies will be used as it problematizes the idea that a clear line can be drawn between what is "military" and what is "civilian". This understanding of blurred lines is especially useful when analyzing cyberspace because unlike traditional domains such as land, air, and sea, it is a man-made domain. Therefore, our ideas and perceptions of this space are not separate from the space itself, in fact they are part of what shapes this domain into what it is.

### 4.1.1 Origins of Critical Theory

CSS finds its origins in peace studies that aimed to develop new ways of thinking about the Cold War environment and the threat of nuclear war. The emergence of CSS is connected to a wider development of a 'critical turn' in international studies (Peoples & Vaughan-Williams, 2014, p. 30). In the 1980s, the international relations theorist Robert Cox argued that in the future, world politics would be divided into two categories: "problem-solving theory" and "critical theory" (Cox, 1981). He describes problem-solving theory as one that takes the world as it is with the existing social and power relations and dynamics, along with the institutions that are in place to organize

them. Critical theory, on the other hand, questions how the current order came to be. It does this by not taking institutions, social and power dynamics for granted but questions their origins, how they came to be the way that they are and whether they might be in the process of changing. Unlike problem-solving theory, it does not accept the parameters, but questions them. It seeks to place the issue, or the part being studied, into a larger construction to understand the processes of change. Due to its focus on the processes of change, its critical theory has to continuously adjust its concepts to the changing object it seeks to understand and explain (Cox, 1981, p. 130).

### 4.1.2 The Pillars of Critical Security Studies

As mentioned above, CSS is in some ways a response to the traditional approach to security studies. Therefore, its core ideas and concepts reflect this. Peoples & Vaughan-Williams explain that there are three core ideas that underpin CSS. The first is understanding security as a "derivative concept", the second is broadening the security agenda past the military realm, and the third is that the individual is seen as the "referent object" of security (Peoples & Vaughan-Williams, 2014, pp. 33–35). The first argues that our understanding of security is derivative, which means that our understanding of security comes from the way we perceive the world and the way we think politics works. What is perceived as the most important features of politics will therefore influence what we think of threats, what needs to be protected, and therefore how we define security (Peoples & Vaughan-Williams, 2014). When analyzing cyberspace and cybersecurity, this can be complicated as cyberspace is a relatively new domain in comparison to traditional domains. Therefore, the precedents that we choose to base our knowledge of this new domain on are vital for how we perceive this space. Whether that is space, maritime, land or air, shapes our conception of cyberspace. What we base cyberspace and cybersecurity conceptualizations on have real world consequences, and CSS allows us to analyze these consequences.

The second pillar within CSS is the argument that the security agenda must be broadened. At the heart of this argument is the belief that while military force is an important component, it is not the only area of potential threat. Barry Buzan (1991) argues that security analysts should consider five different sectors: the military, the environment, the economic, the political and the societal. CSS broadens the security agenda to study threats that are presented in these sectors (Buzan, 1991, p. 432). Broadening security has the unique ability to detect emerging threats, such as the once presented through cyberspace. This aspect of CSS is crucial in the study of EU-NATO

cooperation within cyberspace, as cyber threats and cyber defence have increasingly come under the umbrella of security.

The third pillar within CSS is that the individual is seen as the "referent object" of security. Wyn Jones (1999) argues that while Buzan's argument for broadening security is in the right direction, its state centric approach is problematic. Instead, Jones argues that military, environment, economic, political and societal threats affect people. States are simply human communities, and therefore, the ultimate referent of security should be human beings that make up the state, not the state itself. CSS argue that security should be perceived in relation to human beings – not an abstract idea of a state (Peoples & Vaughan-Williams, 2014, p. 35). This pillar sheds light on how cyber security is perceived by the EU versus NATO and what their position as the referent object.

Aside from the traditional understanding of CSS, Andrew W. Neal boldly states that a constant in critical security studies, is *neophilia* – a love for what is new (Salter et al., 2019). This love does not merely stem from enthusiasm but of an obligation to critically engage with the implications of new security problematizations and technologies. By critically engaging with cyberspace and how NATO and the EU choose to impose security and defence governance structures, this thesis can shed light on the framework in which this domain was securitized and the various policy decisions this instigated. As Neal points out, the alternative theoretical frameworks of traditional disciplines, such as traditional international relations theories, are inadequate to fully conceptualize the new. While there are academics who argue that traditional international relation models can help explain cyberspace, I would argue that the rigid lines they draw between war and peace, military and civilian, and the like impede their ability to fully comprehend, in Salter's words, "a space that is everywhere and nowhere" (Salter et al., 2019, p. 32). By equipping this thesis with a critical security studies lens, we can grasp the "in-between" that Debbie Lisle describes as "not a happy place of resolution and satisfied contentment: it is instead a difficult and demanding terrain of inquiry that scholars must fight hard to keep open, pluralistic, and hospitable to new ideas" (Lisle, 2016, p. 418).

Therefore, this thesis will not aim to push the nature of cyberspace into a clean-cut box. Rather, it will explore the movement and complexities of the subject matter while keeping in mind that new ideas are possible. Stefan Elbe (Salter et al., 2019), explains that critical security studies'

conceptualization of security is that of relational phenomenon rather than a static concept. This understanding will allow this thesis to examine *how* and *if* the concept of security and cybersecurity changes based on its relational interactions. Elbe uses the work of Karen Barad and her agential realism to understand how security as a relational phenomenon provides us with the ability to analyze how and why it constantly emerges out of the world while simultaneously feeding back into the world. Therefore, questioning the establishment of boundaries that separate what is and what isn't security, is one of its key contributions (Salter et al., 2019). However, this cannot be done by simply identifying the boundaries between what is security and what is not, but rather it must examine how the differences around security are within themselves continuously "made and remade, stabilized and destabilized, as well as their materializing effects and constitutive exclusions" (Salter et al., 2019, p. 13). Through this lens, we do not take concepts such as "security", "defence", "cyberspace", "cyber threats" or "cyberwarfare" for granted, we critically engage with them to find how and why they are securitized and the consequences of this decision.

### 4.1.3 Critical Military Studies

Critical military studies is an emerging academic field closely related to CSS that helps analyze the grey areas that cyberspace presents. Highlighting how the line between what is "inside" the military sphere and what is "outside" the military sphere is not static, and how there is a constant state of movement between the two. This theoretical framework's main strength comes from its focus on the grey areas, the "in-between", to shed light on the tensions in place. The "in-between" spaces in this thesis will be the key areas of focus. The in-between areas of civilian and military are particularly wide when analyzing cyberspace. Through this theoretical lens, "nothing is taken for granted as natural or inevitable, but the ongoing processes of construction, constitution, and contestation are explored", thus prioritizing "how military power operates, how it has come to work in the ways it does, and what its limits might be" (Basham et al., 2015, p. 2). Academic debates persist on whether CMS and CSS are, or should be, two distinct fields, or rather if they are part of the same epistemological traditional. For an overview, see the special issue of *Security Dialogue* edited by Stavrianakis and Stern (Stavrianakis & Stern, 2017).

This framework is crucial in analyzing this thesis as it will be exploring how the EU and NATO operate cooperatively in this domain, how they have both individually come to operate in the space, and how this domain may limit their individual actions in this space, but more specifically their

ability to cooperate with one another. Being critical about military power by being "sceptically curious" about its character, how it is represented, and its application and effect, lends itself well to the cyber domain. This application of the theory will speak to the decision to militarize cyberspace, and how this decision is represented by each individual organization.

Due to critical military studies' flexible nature, partially stemming from its interdisciplinary influence, it can fill in academic gaps, providing opportunities to address the security and defence field through an unrestrictive approach. As diverse as this field can be, it is united in its "shared desire to question how military institutions, practices, processes, and geographies are an outcome of social practices and political contestation" (Basham et al., 2015, p. 2). Critical military studies has been used to question military decisions that have previously been taken for granted as illustrated by Enole (2014), who looks at how militaries are created by using a critical feminist approach to military recruitment, along the way asking key questions like how narrow perceptions of "manliness" are used to recruit potential members, or how military recruiters interact with the mothers, girlfriends, and wives of potential enlistees. Much like Enloe's work, this thesis will take a critical approach to how various actors such as the EU, NATO, and private sector actors interact with this new domain and with one another in this space. Critical military studies are able to provide a more nuanced insight to these developments, both in the environment they create and the impact it has on pre-existing dynamics. It will provide a critical perspective on the environmental boundaries such as the militarization of cyberspace, but it will also provide a lens through which we may view EU-NATO cooperation and relation in cyberspace in the face of these complexities.

### 4.1.4 Gaps in Critical Security Studies

There are two main gaps within CSS in relation to answering the thesis question of "how can we understand EU-NATO cooperation in cyberspace with regards to cybersecurity and defence?". The first gap is a theoretical gap that CSS faces, that is, its lack of focus on one of its main pillars, namely the politics of security in which it asks "what security does politically" (Browning & McDonald, 2013, p. 236). Some authors argue that CSS currently lacks a nuanced and contextual understanding of security dynamics and practices in relation to social, historical, and political contexts (Browning & McDonald, 2013, p. 237). This thesis aims to bring the political context into the forefront when examining security and power dynamics between the EU and

NATO. This will be done by exploring what cyber security does politically to EU-NATO relations and cooperation, with the question becoming: under threat from a new domain, how will these two institutions interact with one another and what are the pollical consequences of their interactions and cooperation?

Some exceptions notwithstanding, especially regarding the analysis on the securitization of cyberspace, there is a vital gap within the cyber security and defence literature, that largely do not engage with the material from a critical perspective (Conway, 2008; Dunn Cavelty, 2008, 2013; Hansen & Nissenbaum, 2009; Lawson, 2013). Currently, the academic conversations are focused more so on the "problem-solving" side rather than the critical theory side. The critical lens that this thesis will take will aim to analyze the parameters within this space not as a given but as lines to be questioned and will place EU-NATO cyber security and defence cooperation within a larger political context to understand how this new domain impacts the process of change between these two institutions and their approach to security and defence.

### 4.1.5 CSS Components Used in Final Thesis Framework

Now that CSS as a theoretical framework and its gaps have been examined, I outline how CSS will be applied into this thesis. This thesis utilizes CSS's account for change in studying how the discourse on cyber security and defence has progressed and transformed through time, along with how cooperation between the EU and NATO has changed in the cyber domain. Accounting for change is vital, as the first pillar of CSS is that our understanding of security is derivative, meaning that our understanding of cyber security comes from the way we perceive the domain and the way we think politics works in this new realm. Therefore, accounting for how security in the cyber domain was perceived and how this has changed over time to what it is today, will shed light on why this change came about, and the political consequences of this shift. CSS's view on knowledge as constructed implies that how the EU and NATO perceive cyber security and defence and the cyberspace itself impacts what this space becomes overall. This is especially the case in cyberspace, a man-made realm that can shift based on the decisions made by key actors. In addition, CSS's agenda of broadening security is at the core of this analysis as security has expanded to include cyber security, Therefore, analyzing how cyber became a security issue will shed light on the change in perception and the institutional response to this broadening. As such, this thesis will utilize CSS's account for change as a key theoretical starting point when examining

both the discourses regarding security and defence within cyberspace by the EU and NATO and EU-NATO relations within the cyber domain.

CSS's critical approach to boundaries is a key component of this thesis, not simply examining what is security and what is not, but in examining how the differences around security are within themselves constantly created, recreated, stabilized and disrupted, and the political impact of this cycle. Within the framework of the cyber domain, the concept of security has expanded to include the cyber sphere and cyber threats as legitimate threats. This acts as a disruption to the security system, which had previously included four domains: land, air, space, and sea. However, now it includes a new domain that is man-made and malleable. This disruption also comes in the form of the dual-use nature of the cyber domain. It is a domain that citizens of use every day with little to no barriers of entry. As the dependency of civilians on this domain increases, so too do the vulnerabilities. Therefore, part of the disruption is in the effort of managing a space that potentially inflicts harm, but that must also be used daily by civilians, in addition to its inherently malleable nature which can shift based on the ways in which actors choose to behave. Thus, how key actors work together to stabilize this disturbance will determine what the domain will be. Therefore, by analyzing the political context through critically examining how we can understand EU-NATO cooperation in cyberspace with regards to cybersecurity and defence, we examine how the security system was disturbed and how political actors are working to stabilize it. This brings us to one of CSS's key question, which is "security for whom?", CSS views the individual as the referent object. Through our analysis we will explore whether this is the approach that the EU and NATO take when securing this space.

Finally, CSS's view of security as a relational phenomenon rather than a static one is used to analyze the power dynamics between the EU and NATO. EU and NATO power dynamics have been analyzed by many scholars, mostly from an international relations perspective (Angelov, 2019; Duke, 2008; Flockhart, 2011; Ojanen, 2006; Touzovskaia, 2006). However, CSS presents us with a new lens to view this relationship, one that seeks to examine how they view and interact with security in this domain in relation to one another. The power dynamics, discussed earlier, play a major role in understanding who leads this cooperation, who sets the agenda in the domain, and if they both have differing views on the cyber domain, including whose views are dominant. This is particularly important as this domain is currently in the process of establishing international

norms. Therefore, the way in which power is distributed determines whose views on security in cyber space and interests are protected.

In addition to the points above which are used from CSS to develop this thesis framework, CMS questions what is viewed as an area with military jurisdiction and the areas outside. In studying cyberspace, this barrier is fluid and can be argued to be non-existent. CMS's focus on this is used when examining the cyber domain, but more importantly when examining the cooperation and relationship between NATO and the EU. As pointed out in the literature review, NATO is a military alliance whereas the EU is a governance experiment. Analyzing this mostly civilian and military alliance cooperation requires us to examine what is inside the military and what is outside, what is within the realm of defence and what is not and more importantly question why that is. By critically engaging with the parameters between military and civilian both in relation to the EU and NATO cooperation and the nature of the cyber domain, the thesis aims to find the grey areas, the in-between areas, and how and why they are processed.

The final theoretical framework incorporates CMS's focus on militarization as a result of social and political environments. Basham et al (2015) explains that CMS is united in a desire to question how military practices, processes and geographies are outcomes of social and political practices. Through CMS we examine how and why the militarization cyberspace by the EU and NATO is a result of their social and political practices and how these practices shape their perception of cyberspace and security within it.

### 4.2 Science and Technology Studies

Science and Technology Studies (STS) is an interdisciplinary field that explores the "institutions, practices, meanings, and outcomes of science and technology and their multiple entanglements with the worlds people inhabit, their lives and their values" (Felt et al., 2016, p. 1). STS focuses on the impact of science and technology on societies and seeks to explore how societal shifts occur as new science and technologies are introduced. Additionally, it seeks to understand how science and technology are linked to military power. Historically, state funding of both science and technology have often been in the pursuit of finding new and innovative ways of acquiring resources, and this been done through acquiring advanced military power over opponents. STS studies not only how science and technology impact and shift society, but also how social life and the power dynamics at play shape science and technology.

Through an STS lens, technologies that we create, such as cybertechnologies and the cyberspace itself, are viewed as the products of human labor. They are considered a part of a historical tradition, investment, choices and designs. Therefore, as we approach this domain, we do it from the understanding that cyber domain did not *have* to look like it does, it was a product of choices made based on societal dynamics. STS asserts that, as humans, we create science and technologies in our own image, reflecting our current societal and power dynamics, our identities and our current surroundings; therefore we import our beliefs and wishes into these technological systems that then feedback, impacting the way we live our lives and how we understand our world. From this perspective, studying cyberspace is not simply studying the domain or the cyber artifact itself, but examining the surroundings that produced the technology.

STS as a theoretical framework does not shy away from examining the moral economies that guide scientific and technological research and development, and how it impacts social arrangement. As a result, careful attention is paid to the boundaries that are set between what constitutes science and non-science (Felt et al., 2016, p. 2). It takes a critical approach to how where, when and how people produce science and technology and its impact on society as a whole. Asking questions like "why do societies make science and technology - and, along the way, themselves - in one way as opposed to another?" (Felt et al., 2016, p. 2).

At the heart of STS is the argument that technoscience practices are methods that shape and reproduce the social world. At its core, STS asks how science and technology shape our world and in return our world shapes them and how we might intervene in these processes (Law, 2016). As argued by Wiebe E. Bijker, paying attention to technology in political studies is vital as it reveals aspects of politics that have not previously been left unnoticed and unstudied (Bijker, 2006). STS analyzes the effects of how technologies are governed, theorized and used in practice. Seeing as one of the main components of this thesis is technology in the form of cybertechnologies and the creation and governance of cyberspace itself, it is vital that we equip the research with theory that can examine the technological side of the thesis with nuance. This is the strength of an STS theoretical approach, it will help in not only shedding light on cyberspace and its technologies, but more importantly on what this reveals about the political aspect of EU-NATO interaction and cooperation in the space that has previously gone unnoticed.

### 4.2.1 Origins of STS

It can be argued that the STS originated as a reaction to the idea that science is different and special because of its scientific method. The general consensus in the 1960's and 1970's was that the scientific method was able to collect accurate data, then generate logical generalizations based on the data collected and test those generalizations to form accurate knowledge (Felt et al., 2016, p. 32). It was argued that as long as people adopted the scientific method, accurate knowledge would grow (Law, 2016). Law explains that as a response to Nazi and Soviet political interference, philosophers believed that prejudice disfigured how scientists observe phenomena, which erodes their logical reasoning, and undermines their objectivity as scientists (Law, 2016, p. 33). STS originated in this environment. Law reiterates Jonathan Slack's (1972) argument that while theoretically the scientific method was useful, in practice scientific methods are not applied in a vacuum, they are practiced in a class or gendered society, and cannot escape social powers. This means that scientific knowledge is inherently both ideological and social. Therefore, science, along with the knowledge it attains, its methods and practices, are disciplinary cultures. As such, "scientific knowledge is shaped in interaction between the world on the one hand and the culture of science and its methods on the other" (Law, 2016, p. 33).

### 4.2.2 STS's Approach to Studying Technology

This thesis defines technology as "the embodiment of societal knowledge" (Cavelty, 2018, p. 22). STS illustrates that different understandings of technologies can show us different facets of cybersecurity and cyberspace. Bijker (2006) states that technology and politics are two sides of the same coin, and that to answer "why" or "how" they influence one another, require us to study them contextually. Thus, this thesis intertwines STS with CSS to develop a theoretical framework that will analyze co-production, the premise being that "the way in which we know and represent the world are inseparable from the way in which we choose to live in it" (Jasanoff, 2004b, p. 2). This thesis critically analyzes how EU-NATO cooperation and perception of this space, molds cyberspace and cybersecurity and defence into what it is today and vise versa, how cyberspace and cybersecurity has changed EU and NATO's perceptions of security and their cooperation.

To do this, we must first comprehend how technology is understood. Bijker (2006) breaks down how technology is understood into three layers. The first layer refers to technology as a physical object or artefact. Cavelty builds on this layer and states that within this layer technology

is seen as static and apolitical (Cavelty, 2018). Bijker's second layer includes human activities such as the designing, making, and handling of the technology itself. The third layer is the one that takes technology back to its Greek origins *techne* and *logos*. *Techno* means art, skill, craft, or the way, manner, or means by which a thing is gained. *Logos* means word, the utterance by which inward thought is expressed; a saying or an expression. Therefore, this third perspective is "about what people know as well as about what they do with" technology (Bijker, 2006, p. 2). Through this lens we see that the study of technologies can examine what power relations can be in practice as they shape and coordinate the behaviour of social actors (Cavelty, 2018). In the context of this thesis, the power relations examined are mainly be between NATO and the EU, as well as private actors in the context of private-public partnerships in protection of critical infrastructures.

We cannot study cybersecurity issues without connecting it to societal and political dynamics as both cyberspace and cybersecurity and defence are shaped by digital technologies and their use and misuse. As technological realities and social and political practices are interlinked, both feed into one another. STS provides a strong theoretical foundation on how to make this connection to reveal areas of study that have previously been overlooked as they have been viewed from traditional theoretical frameworks that have not adequately focused the conversation on the technology and its impact on society. An STS theoretical framework asks questions on how new sociotechnical arrangements are created, deliberated, and stabilized. It seeks to answer what happens when a domain such as cyber is contested, changed or reshaped. Finally, STS always asks who benefits from specific configurations of science and technology, and the insights that are gained from this theoretical framework strive to bring the knowledge to work in ways that can improve the outcomes for people and the planet (Felt et al., 2016, p. 2).

At its core STS tries to understand two critical technological questions. The first is "how do people shape the development of new technologies?" The second is "how, in turn, does the development of technological networks, systems, or infrastructures shape, impact, and (re)-configure the human condition?" (Fouché, 2016, p. 495). By critically examining this cycle of influence, Fouché (2016) analyzes how human efforts in creating technologies both physically and conceptually, continuously puts society in a position to "rethink, reassess, and re-examine" the evolving relationship among themselves and with interconnected complex "sociotechnical arrangements" (Fouché, 2016, p. 495). This thesis aims to use this theoretical approach of critical

engagement to rethink, reassess and re-examine the relationship between the EU and NATO and their individual relationships with cyberspace, specifically its security and defence dimensions. However, aside from the influence cycle that will be examined, STS provides an insightful look into knowledge and security which is helpful when examining the security component of this thesis.

Within STS, the concept of "co-production" is the idea that "the way in which we know and represent the world (both nature and society) are inseparable from the ways in which we choose to live in it" (Jasanoff, 2004a, p. 38). Within this framework, knowledge and its material embodiments, in this case cyberspace and cyber technologies, are simultaneously products of social work and are an integral part of social life. Technology, in this case cyberspace and cyber technologies, "both embed and are embedded in social practices, identities, norms, conventions, discourses, instruments and institutions" (Jasanoff, 2004b, p. 3). As such, "co-production" is a critique of the realist ideology that separates the domains of nature, facts, objectivity, reason, and policy from culture, values, subjectivity, emotion and politics. Within this thesis, co-production provides a framework that can examine how cyberspace and cybersecurity are incorporated into the workings of the EU and NATO, and in reverse how NATO and the EU influence the making and use of cyberspace. Particularly, this lens will be used when analyzing the values and frameworks the EU and NATO export into cyberspace, how this shapes the domain, and how this, in turn, impacts the EU and NATO.

Within this frame, the STS security approach provides three common strengths as outlined by Kathleen M. Vogel et al (2016). The first is that it provides a counter-narrative on security in comparison to traditional understandings and approaches found in other disciplines. The second, is that through an STS security interface we can innovate and adapt methods, tools, frameworks, and ideas to emerging security concerns. The third is its ability to contextualize how these concerns can be understood in terms of a broader historical and discursive context. Finally, its ability to contribute to the critique policy response equipped with an in-depth understanding gathered from the points listed above. As outlined by Kathleen M. Vogel et al (2016), the areas of study within security and STS is in the realm of "imagining security: the scope, boundaries, and discourse of security" in which we question "how do societies define, imagine, frame, scope, and otherwise

know “security” as a field of human activity and how do these knowledges of security shape and get shaped by the security enterprise?” (Vogel et al., 2016, p. 974).

This STS security component will be intertwined with the CSS as they both critically examine what security is and how it is developed. Seeing as cyberspace has been increasingly securitized, it is important that this is examined through a critical lens. Critically examining the securitization of this domain is important because as states invoke “security” to justify state action, when this term is applied to a domain, security is then taken as a public good to which the state has the responsibility to defend. Vogel et al cite Valverde (2001) explaining that when an issue or a domain is securitized, when it is placed under the umbrella of “security”, we know that this “enables and conceals a diverse array of governing practices, budgetary practices, political and legal practices and social and cultural values and habits” (Vogel et al., 2016, p. 974). Therefore, how a domain is framed, gives insight not only to how it is perceived, but also how this perception influences power dynamics and the freedom states have in monitoring and operationalizing it.

### 4.2.3 Gaps in STS

As a relatively new theoretical framework, there are two main gaps that this thesis addresses. First, as a new framework, this thesis expands on the areas that STS can be utilized in. By analyzing cyberspace, cyber security, and political impact of emerging domain and threats. The second gap in STS is its lack of intersection with security studies aside from surveillance technologies and implications (Binder, 2016). This thesis addresses this gap by intersecting STS with CSS in studying cyberspace, the concept of cyber security, and the impact of emerging domains and threats on institutional relationships and cooperation – the political context. By incorporating STS and security, this thesis creates a more comprehensive understanding of security aspects within STS.

### 4.2.4 STS Components Used in Thesis Framework

When analyzing EU-NATO security and defence cooperation in cyberspace, it is vital that this thesis utilizes a theoretical framework that intertwines the impact of technology into its analysis. By incorporating an STS framework, the thesis fills a gap in the field in which technology is studied in a vacuum without societal and political dimensions. Much like the CSS approach fills in the gap of studying security within a political context, STS helps us fill in the gap of studying technology within a political and societal context. The STS framework is particularly useful with

the discourse analysis method of this thesis, by critically engaging with the use of language to analyze how the way in which the EU and NATO represent cyberspace, how cybersecurity is connected to their practices, and ultimately how this space is created. By using both CSS and STS to examine this thesis, it is able to critically engage with the grey areas while analyzing how these spaces shape the EU and NATO, their cooperation, and what the implications of cyberspace cooperation reveal about their relationship.

As previously outlined by Vogel et al (2016), STS provides three main strengths that assists this analysis. First, in its counter-narrative which engages critically with what security means in cyberspace, and more specifically the boundaries around security as established by the EU and NATO and the political impact of the security threats in this technological domain. The second is in STS's ability to handle emerging security concern. The cyber domain and the security concerns in this field present a disruption to the global security system. By increasing the domains in which states must defend against threats, the cyber domain is especially disruptive due to the dual-use nature, the increasing amount of vulnerability due to societal dependence, and the lack of international norms and regulations in the domain. Therefore, this thesis incorporates the impact of disruptive technologies and the emerging threats they present when analyzing the impact of these disturbances on EU-NATO relations and cooperation. Third, the thesis utilizes STS's approach in understanding these security concerns by placing them in a broader historical and discursive context. Finally, the concept of "co-production" will pillar the STS framework within this thesis, as it operates on the premise that the way in which NATO and the EU know and represent the world and the security environment are inseparable from the way in which they act in the domain. With an STS framework, this thesis aims to provide a comprehensive examination of the cyber domain and the conceptualization of cybersecurity, one which is not conducted in a vacuum, but rather based on emerging technological studies in relation to the political context of two key international actors.

### 4.3 Theoretical Framework: Combining CSS and STS

Now that both CSS and STS have been analyzed, and the points that will be used from each theoretical framework in relation to this thesis have been outlined, this section presents the combined theoretical framework used in this thesis.

The thesis takes from STS and CSS their constructivist tradition, understanding that how security, cyberspace, and cyber security and defence are imagined has political and societal consequences. By being critical, this thesis will focus on the socially constructed nature of security and ask fundamental questions about whose security is advanced, the threats identified, and where security discourses come from. This is contrary to the traditional approaches to security which focuses on threat and use of force by and between states in world politics. Critical approaches point to the normative preferences that are inherent in these choices and the political implications of these decisions (Browning & McDonald, 2013, p. 238).

CSS's broadening of security to include areas that would otherwise not be considered a security matter under traditionalist, realist, frameworks will allow for the study of emerging technologies and the security threats they present. From STS the use of language in discourse in relation to this technological domain will be analyzed and placed into a political context. STS equips this thesis with "co-production", which does not aim to provide deterministic causal explanations of the ways in which science and technology influence society, or vice versa, but provides a lens to systematically think about the processes of "sense-making" through which NATO and the EU come to grips with the world in which technology, in this case cyberspace and cyber technologies, have become permanent fixtures (Jasanoff, 2004a, p. 38). As constructions, they are malleable to change. Therefore, this CSS's accounting for change will be used to examine how the EU and NATO view cyber security and defence and their cooperation with one another in this domain. CSS's accounting for change coupled with STS's study on disruptive technologies intertwines when analyzing the political and conceptual impact the emergence of a new domain has, especially one that has an inherent dual-use nature and the dependency of civilians on the domain. Taking from CMS, the thesis employs a critical approach to boundaries that exist in the security filed, such as civilian versus military, not only in the context of the dual use of this domain, but also in the cooperation between a military alliance (NATO) and a governance institution (EU). CMS provides us with a lens to view how the social and political practices of these institutions have resulted in the militarization of this domain. Additionally, the power dynamics in this relationship will reveal who sets the agenda in this domain, and whether there are tensions between how NATO and the EU conceptualize this space and the threats it presents. From intertwining CSS and STS, we will critically analyze these boundaries around how security and security cooperation

is created or perceived to be created by the EU and NATO, disrupted through the emergence of cyber threats, stabilized and re-stabilized again.

**Thesis Theoretical Framework:**

| **Concept** | **Theorical tradition** | **Definition** |
|---|---|---|
| Security as a derivative concept | Critical Security Studies (CSS) | The idea that the way we think about security comes from the way we think the world works more broadly (Peoples & Vaughan-Williams, 2014, p. 4) |
| The study of the "in-between" | Critical Military Studies (CMS) | The study of the area in between civilian and military, between peace and war. (Basham et al 2015) |
| Co-production | Science Technology Studies (STS) | The premise that the way in which we know and represent the world are inseparable from the way in which we choose to live in it (Jasanoff, 2004, p. 2) |

# 5. Methodology

The research question this thesis aims to answer is "how can we understand EU-NATO cooperation in cyberspace with regards to cybersecurity and defence?". In order to answer this question, one must analyze the discourse that both organizations have regarding cyberspace, cyber security, and cyber cooperation with one another. Analyzing their discourse is vital because discourse maintains regularity in social relationships and produces the preconditions to actions that will be taken (Dunn & Neumann, 2016, p. 4). It restricts how people categorize and think about the world by creating parameters that constitute what is thought of as possible, and what is thought of as the "natural thing" to do in a given situation. While discourse cannot be said to completely determine actions, as there will always be more than one possible outcome, what discourse analysis is able to provide us is the bandwidth of the possible outcomes. In the case of this thesis, it provides us with the bandwidth of possible ways in which the EU and NATO could conceptualize cyberspace, security within this domain, and the impact of emerging technologies such as cyber on their pre-existing relationship.

## 5.1 Discourse

Discourse can have varying definitions based on the context and the field of study it is utilized in. Therefore, it is important to clearly outline how this thesis defines discourse. Norman Fairclough (2003) views discourse as the ways of representing different aspects of the world, including processes, relations and the structures of the material world, the "mental world" of the thoughts and beliefs of the social world (Fairclough, 2003, p. 124). For Marianne Jørgensen and Louise Phillips (2002, p. 1), discourse is "a particular way of talking about and understanding the world (or an aspect of the world)". Fairclough (1992, p. 64) clarifies that discourse is "a practice not just of representing the world, but of signifying the world, constituting and constructing the world in meaning". Kevin C. Dunn and Iver B. Neumann (2016) build on Michel Foucault to define discourse "as systems of meaning-production that fix meaning, however temporarily, and enable us to make sense of the world and to act within it" (Dunn & Neumann, 2016, p. 2). Dunn and Neumann's definition highlights the inherent constructivist premise, that views discourse studies as open-ended and incomplete – as *emergent* (Dunn & Neumann, 2016, p. 3).

Thus, discourse with relation to this thesis is understood as collective ways in which meaning is generated in order to make sense of the world. Thus, the ways in which the EU and

NATO conceptualize cyberspace, cyber security and their relation to one another in order to make sense of a new domain of operation and their place within it. Within discourse, language is vital in that it does not merely explain the world, but rather produces it. *Therefore, by conducting discourse analysis on cyberspace and security within EU and NATO, this thesis attempts to capture how this happens – how these institutions produce this new domain and export security within it.*

### 5.2 Discourse Analysis

Discourse analysis is described as "the close study of language in use" (Taylor, 2001, p. 5). In relation to this thesis, it closely examines the discourse NATO and the EU use in relation to security as a derivative concept with regards to cybersecurity, the blurring of lines that occur with the introduction of cyberspace and cybersecurity, and finally how the they shape cyberspace and cybersecurity based on their ideas of the world. Discourse analysis questions the ways in which specific systems of meaning-production have been created, circulated, internalized, and/or resisted (Dunn & Neumann, 2016, p. 4). This method is especially suited for the study of emerging technologies and domains as this method is especially useful for illustrating the impact of language on discourses and practices of security, in our case, the practices of the EU and NATO in cyberspace (Mutlu & Salter, 2013). A key assumption of discourse analysis is that language is integral in the social world, in that it does not explain the world as much as it produces it (Dunn & Neumann, 2016, p. 2). Therefore, what the thesis aims to do with this method is to capture how this process occurs.

Discourse analysts use the term "representations" in order to not forget that meanings are socially reproduced (Dunn & Neumann, 2016, p. 5). Representations that are repeated over time become statements and practices which become institutionalized and "normalized" over time (Dunn & Neumann, 2016, p. 5). However, at closer examination, it becomes clear that there is a constant struggle between competing discourses to frame and define the categories and phenomena that constitute our world, such as the boundaries around what constitutes security, what constitutes a threat, the discourse that frames emerging technologies as threats, and the division between military and civilian domains. Therefore, as discourse analysts we examine these discourses to determine how they came about and in the context of this thesis, how this impacts the political context and more generally the implications this can potentially have on cyber governance and international norms in an emerging domain.

Discourse analysis illustrates how options and possibilities of actions are established based on the processes and interactions within the social realm. This method is suited for interrogating how meanings are produced and attached to various social subjects and objects, and how this produces specific interpretations which create what is thought of as a bandwidth of possibilities. As with any parameter, it includes certain possibilities while simultaneously excluding others. The assumptions scholars of discourses make is that "discourses are the product of power by which hegemonic interpretations are seemingly naturalized and internalized but also resisted and contested, within the social realm" (Dunn & Neumann, 2016, p. 12). The EU and NATO are key actors in establishing international norms, whether that is in space or cyberspace. Therefore, how two powerful actors interact and conceptualize a new domain and technology, and how they draw the boundaries between security and insecurity within this space, along with the line between civilian and military, will have lasting impact on how other key actors behave and conceptualize this space.

Therefore, how the EU and NATO conceptualize cyberspace, the threats in this domain, cyber security, and their relationship with one another can be institutionalized and the concept of cybersecurity and cyber protection can be "normalized" over time. This thesis critically examines and questions how they are produced and naturalized and the impact this has on EU-NATO relations, and more generally, cyberspace and international norms within this emerging domain.

### 5.2.1 Why Discourse Analysis?

The decision to base this research project on a qualitative approach stemmed from my curiosity in understanding the phenomenon of emerging technologies and their impact on pre-existing political and security systems – in the case of this thesis, the impact of an emerging domain, such as cyberspace, and its impact on EU-NATO relations and the security and defence systems in place. Therefore, the decision to conduct a qualitative research study was determined by my interest in the how questions of this phenomenon. This thesis uses discourse analysis and expert interviews to answer, "how can we understand EU-NATO cooperation in cyberspace with regards to cybersecurity and defence?"

Seeing as cyberspace, cyber security, and cyber threats are relatively new, the study of language used will give it its meaning. It is within language that meaning-making and action-taking in the social realm are created and debated. With discourse analysis we are able to answer

how language constructs this meaning and what it regards as acceptable and actionable knowledge with regards to this domain and security within it. Thus, discourses are intimately linked to the production of knowledge, in that they both enable and constrain it. As this thesis seeks to understand the production of knowledge around emerging technologies and how they are enabled and constrained, this method is best suited for this task.

### 5.2.2 Discourse Analysis Approaches

There are various approaches to discourse analysis. In this section, I outline Critical Discourse Analysis (CDA) and Poststructuralist approaches to discourse analysis to illustrate how they will both contribute to this thesis. Both CDA and poststructuralist approach to discourse analysis share the theoretical background of constructivism, and in both of their approaches, language is central. Where these two methods diverge is in their view on discursive dimensions in the social world and the ability to measure causality.

In poststructuralism, there is no distinction made between the discursive and non-discursive dimensions, and it rejects the claim that discourse can have a measurable degree of causality. As Dunn and Neumann (2016, p. 39) state, for poststructuralist discourse analysts "everything can be studied as text- as phenomena linked together by a code". This does not mean that they view everything as text, but rather that gestures, monuments, films, and fashion can be read as text. This is due to the ontological position that nothing exists independent of language. This is not to say that poststructuralist reject a "real world" where objects exist independent of our knowledge, instead they argue that it is only through discursive meaning-making that these objects become known and knowable to us. Laclau and Mouffe (2001, p. 107) state that the relationship between language and concepts are determined not by nature but by social processes, with signs only gaining their meaning within wider discourse structures or "discursive realities". Therefore, poststructuralist analysis is mainly about mapping discursive structures/institutions to illustrate how they produce objects and subjects, how power relations are embedded and produced within discourse, and the way in which discourses are related to practice and materiality. Methodologically, poststructuralist discourse analysis shifts away from attempting to uncover "truths" and moves toward critically examining interpretations and the struggle for determining meaning (Dunn & Neumann, 2016, p. 40).

Critical Discourse Analysis operates on the premise that, unlike poststructuralists, there are two realms: the discursive and the extra discursive. The second premise is that discourse can have a measurable degree of causality, thus leading to empirical accuracy. Norman Fairclough, often referred to as the father of Critical Discourse Analysis, argues that "discursive practices are constrained by the fact that they inevitably take place within a constituted, material reality". Operating from this premise, there is a "reality" that does not depend upon what is known about it. For Critical Discourse Analysis, human agency exists within a dialectical relationship between discourse and social systems (Dunn & Neumann, 2016, pp. 35–36). This framing leads the way for Critical Discourse Analysis scholars to make empirical claims about discourses and causality as they believe that it is possible to measure how effectively a discourse is utilized by people.

As previously mentioned, there are significant similarities between CDA and poststructuralist approaches such as similar ethical and political considerations driving the researchers. Both are interested in uncovering issues relating to power and domination, and they both aim to expose dominant ideologies and opening up alternative spaces (Dunn & Neumann, 2016, p. 41). While this thesis does not strictly follow Fairclough's CDA approach, it utilizes a critical lens in questioning knowledge that has been taken for granted in the past to understand how they contribute through their preconditions of the actions taken by the EU and NATO, and employs this framework's focus on change. This thesis takes CDA's extra-discursive dimension but situates itself closer to a poststructuralist approach in that everything is discursive. Although I outline the differences in these two key approaches to discourse analysis, they are not mutually exclusive, meaning I can work across these approaches. This thesis combines different parts of both approaches in order to answer the research question, and while the ontological framework of this thesis is poststructuralist in that it will hold to the premise that everything is discursive, it takes from critical discourse analysis in its emphasis on change, practice and critical insight into the impact of discourse.

### 5.2.3 Discourse and Power

One of the key areas of study in this thesis is the role of power. Discourse analysis, especially one that leans towards a poststructuralist framework, gives analytical focus to the conceptualization of power. Jennifer Milliken (1999) states that "discourses are understood to work to define and to enable, and also to silence and to exclude, for example, by limiting and

restricting authorities and experts to some groups, but not to others, endorsing a certain common sense, but making other modes of categorizing and judging meaningless, impracticable, inadequate or otherwise disqualified" (Milliken, 1999, p. 229).

Through this process, discourses determine *subjects authorized to speak and to act*, such as defence experts and foreign policy officials. This creates the idea of legitimacy, whether that is of a state or expert official. In addition, discourses produces audiences/publics with "common sense" of various phenomena, and how experts and public officials should act as their representatives, for example, when securing the state (Milliken, 1999, p. 229). This creates a power dynamic in which discourse determines the experts who have authority to speak and act, but also audiences that expect them to act in accordance with the roles they are given. Security studies is especially impacted by this, as security as a field of expertise is heavily guarded. Especially in areas of security and defence, discourse's naturalizing power is largely unseen. This aspect of the power dimension is mostly related to the Private Public Partnerships (PPP) and the level of authority they are given by the EU and NATO. Through this discourse analysis, I narrow in on this power dynamic to examine the political impact of this interaction.

### 5.3 Representation and Practice within Discourse Analysis

This thesis looks at the political impact of emerging technologies. In the case of this project, is the scope is limited to the impact of the cyber domain, and therefore the representations that I interrogate are at the core of the practices and policies that the EU and NATO have put forward. As such, this section explores the role of representations and practice within the methodological approach of discourse analysis. As previously discussed, representations are created based on language, and therefore they are not neutral signifiers; they have political implications due to their role in enabling actors to "know" the object and to act upon what they "know" (Dunn & Neumann, 2016, p. 60). This is how they create the bandwidth of possible action, in our case in the form of policies.

In this thesis, "policies are understood as discursively produced directions for action"(Dunn & Neumann, 2016, p. 60). Discourse and practice can be compared by saying that while discourse is a system for the formation of statements, practices are "the socially recognized forms of activity, done on the basis of what members learn from others, and capable of being done well or badly, correctly or incorrectly" (Barnes, 2001, p. 19). Therefore, discourse and practice

are both preconditions to action and patterns of actions. Ann Swidler makes the argument that the reason why practices remain stable is not only due to habits, but more so because engaging one another forces actors to return to common structures (Swidler, 2005). The practice that I analyze is that of the relationship between the EU and NATO, to examine how emerging technologies – in the form of cyberspace and cyber security – has impacted practices. Dunn and Neumann (2016, p. 64-65) discuss how, as emerging practices are adopted, one of two things happen: either they are altered in order to fit into pre-existing practices, or, as the new practice is institutionalized, it also becomes naturalized. As a naturalized practice it produces ideas of the way things should be like. The emergence of cyberspace presents a new domain that can either be integrated into pre-existing understandings of domains by the EU and NATO, or it can be institutionalized in its own unique way. Additionally, the introduction of this domain can either create EU-NATO cooperation policies that are in line with previous practices, such as the cooperation efforts on land and sea, or it can be naturalized in a unique and novel way.

### 5.4 Strengths and Challenges of Discourse Analysis

The choice of conducting an interpretive research method such as discourse analysis carries strengths that adds to my research project, but also challenges that must be addressed. The key challenges that this method faces are with the test of reliability and validity as any interpretive method faces. The topic of security adds onto this challenge as security studies are hard to fully grasp due to their secretive nature. As a scholar, we can only access the material available to us. We are shut out of closed meetings, the languages used when the doors are closed. Therefore, this adds to the challenges a discourse analysis approach takes. We are left with materials that have been heavily produced by communication departments in both the EU and NATO. Therefore, this thesis is limited to a degree by its very topic in addition to the challenges faced due to the methods of discourse analysis. Along with these challenges, discourse analysis has strengths mainly in its potential for hypothesis generation.

#### 5.4.1 Reliability and Validity Within Discourse Analysis

Reliability and validity are key to scientific endeavor. Simply put, validity refers to whether the research is measuring what it has set out to measure (King et al., 1993, p. 25). A positivist research project can achieve this by clearly defining causal relationships. However, this is a challenge for an interpretive research method such as discourse analysis, as it is based on the

analyst's subjective interpretations of the data and not causal relationships. The challenge of validity lies at a much larger debate between positivist and constructivist ideas regarding objectivity.

The next challenge that discourse analysis, and by extension this thesis, faces is the test of reliability. A study is reliable when applying the same procedure in the same way will always produce the same results, in that another researcher is able to follow the same steps and come to the same conclusion (King et al., 1993, pp. 25–26). If they can replicate the study based on your data and methods, the study has passed its reliability test. However, discourse analysis is based on subjective interpretations of the data, and therefore reliability becomes a challenge. As there is no consensus within social constructivism and discourse analysis regarding which criteria to apply, we will be utilizing Potter's and Wetherell's (1987) criteria of coherence and fruitfulness.

This does not mean that discourse analysis is not a scientific method, or that this study is not firmly placed in the scientific method. Rather, that discourse analysts have produced new and fitting checks to ensure validity and reliability. Jonathan Potter suggests the methods that discourse analysts can use to assess reliability and validity of their analysis (Potter, 1996, pp. 138–139). One of these includes "Coherence", which refers to how discourse analysis builds on previous work conducted in the field, and therefore each new study is somewhat of a "check" upon the validity of earlier studies. However, as Jørgensen & Phillips (2001) illustrate, there is a debate within the field of discourse analysis regarding this point.

Jørgensen and Phillips (2002) present the criterion of *fruitfulness* which emphasizes the importance of the production of new knowledge and new types of thinking and action. This is directed towards whether or not the research has the ability to generate new scientific explanations of the phenomenon under study (Potter & Wetherell, 1987). This thesis aims to generate new knowledge by adding a political context to the field of CSS, CMS and STS. In addition, it aims to generate new knowledge on a previously understudied area of EU-NATO relations in the face of an emerging cyber domain. To this, Karen Tracy introduces the *helpful problem framing* criteria which focuses on the framing of the problem of a practice that would be helpful in fostering reflection on how to act. (Tracy, 1995, p. 210). The final criterion that this thesis works to abide by is Potter's "readers evaluation" which is perhaps the most important method for validity of the

analysis to be checked, by presenting the materials being analyzed in order to allow the reader to make their own evaluation of the analysis presented (Gill, 2000).

### 5.5 Expert Interview

Expert interviews are used in this thesis to color the discourse analysis. Interviews, unlike conversations, are a professional interaction based on careful questions and listening "for the purpose of obtaining thoroughly tested knowledge" (Kvale, 2007, p. 7). I have conducted semi-structured expert interviews. They have been conducted with the purpose of obtaining information from experts based on their experience and knowledge to help interpret EU-NATO cooperation in cyberspace. The questions were driven by the theoretical frameworks of this thesis in aiming to critically examine cybersecurity, EU-NATO cooperation in cyberspace, and the blurring of lines between civilian and military in this domain. The interviews were transcribed, and their analysis have been incorporated into the analysis chapter. However, I want to reiterate that these interviews will not serve as the main methodological approach, but rather an addition that will color the discourse analysis of the documents analyzed.

I had initially planned a trip to Brussels to interview EU and NATO officials for this thesis. However, due to the COVID-19 outbreaks I was unable to follow through with my initial plans. There were a couple of interviewees that had agreed to conduct interviews however, who stopped responding to emails. This was an invaluable experience on how field research can change with very little notice. Moving forward in my academic career, I will ensure that I plan for such events. Towards the end of the writing process between May and June, I was able to conduct 4 interviews with highly knowledgeable academics and practitioners who have worked on these issues. I followed the Norwegian Centre for Research Data's (NSD) procedures and privacy protocols and gained their approval for both my interview guide and information form sent out to interviewees. I conducted these interviews through both Microsoft Teams, Zoom and WhatsApp and ensured that the participants had full control of the level of privacy they were comfortable with.

### 5.6 Data Selection

This thesis sits at the intersection of technology, security, and international relations. Therefore, while the data selection must reflect this intersectionality, it must also be limited in scope as to produce viable analysis. Therefore, as my research question is focused on the EU and NATO, this provides a first step in narrowing our data and limiting it to these two institutions. The

second step that assists with narrowing down the source material is to limit the timeframe, which in our case is inherent in the topic that we are analyzing – cybersecurity (Neumann, 2008, p. 67). Cybersecurity is a relatively new field in comparison to traditional threats, and therefore the time period in which cyber is introduced to both NATO and the EU begins with 2002 for NATO and 2004 for the EU. Finally, this thesis limits its source material to official texts published by the EU and NATO, such as summits, policies, pledges, directives, official speeches, and frameworks. I do not want to limit the official data by narrowly focusing on a specific type of official data such as speeches, instead I have decided to tighten the scope by limiting the data to official texts from NATO, the EU, and official joint sources.

### 5.7 Overview of Data

In total, this thesis, analyzes 42 documents. From these documents 18 are NATO official documents, 20 EU documents, and 4 joint EU-NATO documents. The document spans a timeframe between 2002 to 2020. For the full list of documents please refer to Appendix 1.

### 5.8 Coding Procedure

Before outlining the coding procedure used in this thesis, it is important to note that "there is no single way to conduct discourse analysis" (Potter & Wetherell, 1987). Likewise, there is no single method for interpreting discourse, and the best approach to learning this method is by doing (Potter, 1996). Therefore, while I follow certain discourse analysis guidelines for coding and analysis, I recognize that there is no solidified method. While there are no strict procedures in place, a useful starting point is the suspension of belief in what is normally taken for granted in language use (Potter & Wetherell, 1987). Anthropologists call this "rendering strange what we take as given" (Toren, 1996, p. 104). This is done by shifting the focus of interest in the data away from the underlying social realities of the linguistic material towards the ways in which accounts are constructed and to the functions that they perform (Gill, 1996, p. 144).

The first step in this process is to determine the texts that will be used as data. The previous section outlined how this is done by both limiting the timeframe and limiting the data to official texts from NATO and the EU. While these texts might not illustrate the "commotion" or the rupture that this emerging domain presents at face value, it is important that the study does not privilege based on the loudest texts, because the absence of commotion does not mean that the discourse of cyber security and adapting to emerging domains is non-conflictual (Neumann, 2008, p. 66). There

is a risk that after the limitations of the data has been established that some relevant texts are not included. Therefore, this thesis has only allowed new material into the analysis if the new data in question cannot be classified under one of the main positions (Neumann, 2008, p. 70).

The second step of the process is to familiarize myself with the data. While there are no clear guidelines on how to guide these readings, I follow Dunn & Neumann's (2016) deconstruction method, in which the first read-through is more descriptive. Here, I can gain an introductory grasp on the space, and the second and third read-throughs are dialogical. In this case, I can challenge the data and to explore alternative possibilities that the text is closing off. After reading the texts several times, coding is determined by my research question and my theoretical framework, specifically the ideas of "security as a derivative concept", "the in-between" and "co-production". Therefore, in the second read-through I focus on areas in the texts that address these theoretical pillars such as: "cyber security", "security", "cooperation", "cyber threat", "cyber-attack", "cyber governance", "international norms", "dual-use", "civilian", "military", "partnership", "EU-NATO". In the NATO texts, I code for "EU" and "European Union", and in EU texts, I code for "NATO" and "North Atlantic Treaty Organization". To organize the large parts of the texts I use the data analysis software NVivo12.

### 5.9 Textual Mechanisms Used for Interpreting Discourses

Textual mechanisms are a guided method of denaturalizing naturalized and internalized representations within the data. In this section I outline the textual mechanisms that were used based on Dunn and Neumann's (2016) categorization.

#### 5.9.1 Presupposition and the Creation of Background Knowledge

The background knowledge that is taken as a given, natural or inherent, is a textual mechanism called presupposition. This is used in discourse to construct understandings about the existence of objects, subjects, and their relationship with one another. In the context of this thesis, both the relationship between the EU and NATO can be considered background knowledge, but also the relationship between both institutions and a new domain along with what the domain is. The strongest discourses are those that are accepted as "given truths", which forms a naturalized idea of "background knowledge" (Dunn & Neumann, 2016, p. 110). Therefore, my role as the discourse analyst is to expose which "natural facts" are being presented without question, and to highlight them and question them. By doing this, I open space for alternative constructions of

knowledge. For example, by questioning concepts that are presented as facts in the data, such as cyber threats or cyber security, I open a gateway for alternative representations within this space.

### 5.9.2 Predicate Analysis and the Creation of Subjects

In addition to presupposition textual mechanism, this thesis utilizes predication. Predicate analysis "examines the verbs, adverbs, and adjectives that are attached to nouns within specific texts" (Dunn & Neumann, 2016, p. 111). This approach helps the researcher understand how certain meanings and capabilities are established that then enables actors to understand and act in specific ways. How cyberspace, cybersecurity, and security are established, and how EU-NATO capabilities are established, informs the bandwidth of action taken by these key actors. Therefore, by utilizing presupposition textual mechanism, the researcher can see the impact of how linking certain qualities to a particular subject or object informs how they are represented. In this thesis, I analyze the qualities linked to cyberspace, cyber, cyber security, security, and dual use.

### 5.9.3 Intertextuality

Intertextuality refers to how each linguistic expression contains aspects from previous relations with other linguistic expressions (Dunn & Neumann, 2016, p. 46). This is done by identifying connections of, both explicit and implicit, texts and meanings through their references to other texts. Intertextuality is central to Fairclough's critical discourse analysis as it investigates *change*. Seeing as this is one of the key areas of focus in this analysis, this thesis will borrow this component of Critical Discourse Analysis into our analysis (Jørgensen & Phillips, 2002, p. 7). This operates on the premise that representations and meaning are consolidated over through either explicit or implicit references in other texts. Therefore, through analysis of intertextuality, this thesis aims to investigate both the reproduction of discourse where no new concepts and representations are introduced, but also discursive change through new combination of discourses (Jørgensen & Phillips, 2002, p. 7).

Now that I have outlined my methodological approach and the areas of focus in conducting the discourse analysis, the next chapter covers the analysis that I have conducted based information presented in this chapter. As a discourse analyst, I am seeking to interrogate representations, power dynamics, and practices that are taken as a given by analyzing how the statements in the official documents of NATO and the EU are constructed to create a bandwidth of possibilities in regards to cyberspace, cybersecurity, and EU-NATO cooperation. As discussed in my theory section, this

theory driven discourse analysis will analyze security as a derivative concept from CSS, the idea of the "in-between" from CMS, and co-production from STS.

# 6. Analysis

The analysis is organized into three main sections that coincide with the theoretical underpinning of this thesis, from CSS "security as a derivative concept"; from CMS the "blurring of lines"; and finally, from STS, the idea of "co-production". This section aims to provide theory driven discourse analysis that contributes to a critical engagement with how we can understand EU-NATO cooperation in cyberspace with regards to cybersecurity and defence. While expert interviews will be used in this section, they are only there to color the discourse analysis.

## 6.1 Security as a Derivative Concept

This framework operates on the premise that what is perceived as the most important features of politics will influence what we think of as threat and what needs to be protected. As mentioned above these are derivative of the way we think the world works (Peoples & Vaughan-Williams, 2014, p. 22). Therefore, the key areas of analysis within this framework will focus on this derivative concept within NATO and EU discourse on how the way they view security is derived from the way they see the security environment more broadly.

NATO's perception of the security environment in which they operate is one of constant change. This idea is a staple in the NATO documents analyzed, thus positioning the alliance as a necessity to "meet the grave new threats and profound security challenges" that are ever emerging (NATO, 2002). These "new threats" are presented as natural and a given. This is NATO's general perception of the security dynamic, which, as cyber becomes more prominent, includes the cyber domain. This idea of the world and more specifically the security environment in a constant state of evolution that presents new threats intersects with technology as illustrated in the *Strategic Concept: Active Engagement, Modern Defence*, in which this evolving threat and environment highlight the impact of technological trends such as laser weapons and electronic warfare on NATO's military planning and operations (NATO, 2010b, p. 12). Due to this perception of change being associated with security risk, NATO moves to "ensure that the Alliance is at the front edge in assessing the security impact of emerging technologies, and that military planning takes the potential threats into account" (NATO, 2010b, p. 15). Within these documents, there is emphasis on the threats that emerging technologies present rather than their contribution in assisting NATO's objectives.

NATO's conceptualization of the security environment carries over to its conceptualization of cyberspace. Throughout the documents up to 2011, cyber is not listed under the conversations on emerging technologies, but rather progressively given its own points and sections. However, this changes with the Secretary General's Annual Report 2011, in which "cyber attacks" are listed as one of the emerging threats that NATO faces by outlining the investments made in 2011 to ensure that NATO is capable of meeting these emerging security challenges, cyber attacks being one of them (Rasmussen, 2012). It places cyber as one of the engines shifting the security environment, thus partially responsible for triggering a response from NATO. Not a proactive approach, but a responsive one. Due to NATO's perception of the security environment, it does not view security as static, but as a changing idea that can incorporate emerging technologies as threats. Therefore, as emerging technologies enter spaces such as cyber, they are institutionalized as a security threat. This lens that NATO discourse presents sees the environment and technological advances as threats. Thus, the conceptualization of cyberspace is derivative of NATO's perception of the larger security environment and the world more broadly as an evolving environment that presents new threats to be faced. The interview conducted with James Shires further supports this analysis as he states that as a military organization, NATO sees its objective to protect its own networks first, share information and coordination between military organizations and only after that to enter the private sector as that is an "unknown and uncomfortable space to operate in" (Interview 1).

Through analyzing the EU documents, it is evident that its engagement within cyberspace varies from NATO's, and that this divergence is indicative of the EU's broader conceptualization of cyberspace. This may be due to the EU's governance role allowing it broader jurisdiction and its role as a governing body more generally than NATO's narrow mandate. Throughout the texts analyzed, the background discourse is based on the essential nature of cyberspace. The focus is initially communication networks and information systems, through "Regulation (EC) No 460/2004" establishing the European Network and Information Security Agency, later renamed European Union Agency for Cybersecurity (ENISA), which compares communication networks and information systems "as essential as electricity or water supply" (European Parliament and of the Council, 2004). This comparison clearly illustrates that for the EU, there is a clear dependence on these systems. Thus, this understanding that as a society's dependency grows, so too do their vulnerabilities. As such, this "increasing concern" to society is derived from the "mistakes and

attacks" and their consequence on "physical infrastructures which deliver service critical to the well-being of EU citizens" (European Parliament and of the Council, 2004).

The EU approaches operates on a different premise than NATO's. is especially well illustrated in the 2013 "Cybersecurity Strategy of the European Union", which states that over the past two decades the internet and "more broadly cyberspace" has impacted all parts of society (European Commission, 2013, p. 2). The document continues to list the ways the EU depend on information and communication technologies, listing "fundamental rights", "political and social inclusion" around the world, "[breaking] down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe". It continues to state that this space has provided "a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies - most strikingly during the Arab Spring" (European Commission, 2013, p. 2). This context that the EU builds is heavily influenced by values and the impact cyberspace has on these values. While it does acknowledge that "cybersecurity efforts in the EU also involve the cyber defence dimension", the text as a whole does not open with the perception of threat in the space, but rather the opportunities it has provided (European Commission, 2013, p. 11). This discourse is present throughout the EU documents, stating that the internet has "fostered innovation, growth, trade, democracy and Human Rights" (European Commission, 2014, p. 2). Through this discourse, cyberspace is framed as playing a critical role in society through economic and societal activities (European Parliament & The Council, 2016; The Council & European Parliament, 2019). As such, the conceptualization of cyberspace within the cyber domain is derivative of the way the EU views its role more broadly, not limited to threat detection, but rather as a governance body that views cyberspace's possible contributions to other areas and thus, the security impact it can potentially have.

The 2016 *Joint Declaration* between the EU and NATO illustrates that NATO's conceptualization of security and by extension the security dynamic has transferred over to their joint document that incorporates NATO's conceptualization of the security environment as evolving to present more threats. Stating that "the Euro-Atlantic community is facing unprecedented challenges emanating from the South and East. Our citizens demand that we use all ways and means available to address these challenges so as to enhance their security" (NATO &

European Union, 2016). This continues onto the 2018 *Joint Declaration on EU-NATO Cooperation* stating that "the multiple and evolving security challenges that our Member States and Allies face from the East and the South make our continued cooperation essential, including in responding to hybrid and cyber threats, in operations, and by helping our common partners" (NATO & European Union, 2018).

Shires ties the EU's and NATO's conceptualization of cybersecurity back to the institutions' origins in which NATO's conceptualization of cybersecurity and priority was impacted by the cyber attacks against Georgia and Estonia. This reemphasized for NATO "that cyber can be used as part of traditional antagonistic relationships even if they did not cause significant harm, they were still tied to existing tensions and conflicts" thus, marking the beginning of NATO's prioritization of cyber issues (Interview 1). Whereas the EU's broad conceptualization of the cyber domain is more economic and focused on the possibilities and opportunities for trade and commerce throughout the early 2000s. As such, Shires states that the EU's concerns would be focused on data protection, enabling businesses to trade confidently and consumers to go online and combat fraud and cybercrime "to make sure that rights of EU citizens are protected online and offline" (Interview 1). With regards to the conceptualization of cybersecurity, Shires believes that "cybersecurity continues to be redefined. There's no end to the definition, and the framing of disinformation and influence operations as a security issue is very important for the EU's development […] you continue to see redefinitions of security and cybersecurity even when it is embedded in the mainstream. For NATO, cybersecurity is not over the horizon challenge, it is something it has been doing for a long time. But just because it is there in the middle does not mean the content of the task or the mandate is static, it changes as priorities change and as different interest changes as well" (Interview 1). Paul Timmers states that the while NATO takes securitization of cyberspace as its primary dimension, the "EU over the last few years takes sovereignty as an ever more important dimension and it may become the primary dimension" (Interview 2). As such "[t]hese interests are definitely not necessarily the same but that does not mean that EU and NATO cannot meet each other. However, they do not have the same interest and that will become more explicit because of this conceptualization of where cyber security belongs, and their conceptualization of cyberspace" (Interview 2).

### 6.1.1 Referent Object

The analysis illustrates that NATO derives who is to be protected with regards to cyber threats based on a traditional state-centric and institutionalized world view of security. In this case, the initial reference to cyber threat is in relation to the protection of the state and this carries on throughout NATO discourse with a few exceptions such as the *Secretary General's Annual Report 2012*. In the 2006 Riga Summit, cyber is introduced as part of NATO's agenda to adapt its forces and to increase its capacity to address contemporary threats and challenges. Part of this is to "work to develop a NATO Network Enabled Capability to share information, data and intelligence reliably, securely and without delay in Alliance operations, while improving protection of our key information systems against cyber attack" (NATO, 2006). Thus, positioning information systems and areas of data and intelligence as the referent object. Åsne Kalland Aarstad argues that "NATO, like other military alliances, struggle with new security challenges because of the civilian nature of some of these new challenges. The fact that the biggest threat to cyber security may very well be stemming from private individuals or companies, it is difficult for a conservative military alliance that is driven by, not so much innovation but by rank tradition hierarchy, it is difficult to be on top of things" (Interview 4).

This perception carries onto the *Bucharest Summit Declaration* in which NATO is concerned with strengthening the alliance's information systems against cyber attacks by adopting a Policy on Cyber Defence. The text explains that the policy emphasizes the need for "NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack" (NATO, 2008). NATO's 2010 "Strategic Concept" expands the conceptualization of what is to be protected in the cyber domain stating cyber attacks are urgent phenomena that are "becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. (NATO, 2010b). There is one reference to the protection of individuals in the Secretary General's Report 2012 of the negative impact cutting defence spending will have on threats, such as the threats "cyber warfare" will pose to "our children and grandchildren" (Rasmussen, 2013).

NATO's understanding of what is to be protected expands over time to include economic and political institutions. The *Secretary General's Annual Report 2016* expands the concept of who and what needs cyber protection by including democratic systems. The report states, "Cyber threats and attacks are becoming more common, sophisticated, and damaging. These attacks can shut down infrastructure, undermine democratic systems, and affect military operations. In light of this changing security environment, cyber defence has become a key priority. It has evolved from being seen as a technical enabler to an operational domain in which NATO has to be able to act as effectively as on land, in the air or at sea" (Stoltenberg, 2017, p. 24). This is further elaborated in the *Secretary General's Annual Report 2017* in which Stoltenberg states "in today's world, cyber threats are becoming more widespread, sophisticated and damaging than ever before. In a worst-case scenario, a cyber attack could compromise a country's critical infrastructure, paralyse its government, undermine its democratic system or affect the operational effectiveness of its armed forces" (Stoltenberg, 2018b, p. 20).

The EU discourse on referent object in cyberspace illustrates that it views the protection of its values and citizens as the center of its role in cyberspace. From the first EU document analyzed, the security of communication networks and information systems, specifically their availability, is positioned as an "increasing concern" to society due to the possible problems such as "mistakes and attacks" that can impact "physical infrastructures which deliver service critical to the well-being of EU citizens" (European Parliament and of the Council, 2004). While the "physical infrastructure" is described as the potential target of an attack or a mistake, the focus is on how this will impact EU citizen being able to access critical services. Within the same document, the security breaches that have resulted in financial damages is discussed, but only in reference to its impact on "individuals, public administrators and businesses", thus bringing the focus back again to the individual (European Parliament and of the Council, 2004).

This position of who and what is to be protected is imbedded into ENISA's purpose as an agency "for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union (European Parliament and of the Council, 2004). This is further illustrated in the *Concerted Work Strategy and Practical Measures Against Cybercrime*, that lists "protecting Europeans" as one of the EU's main objectives (European Council, 2008). Within the "European Security Strategy", "Cyber Security" is listed as one of the "Global Challenges and Key Threats",

this section illustrates the EU's understanding of this field in relation to the EU's reliance on it. The document states that "[m]odern economies are heavily reliant on critical infrastructure including transport, communication and power supplies, but also the internet" (The Council, 2009, p. 13). While it cites the EU Strategy for a Secure Information Society, adopted in 2006 that strictly focuses on "internet-based crime", the security strategy continues on to establish that "attacks against private or government IT systems in EU Member States have given this a new dimension, as a potential new economic, political and military weapon" (The Council, 2009, pp. 13–14). As such, the EU acknowledges that this is not a one-dimensional threat. Therefore "more work is required in this area, to explore a comprehensive EU approach, raise awareness and enhance international co-operation" (The Council, 2009, p. 14). This line of discourse continues onto the "Shaping Europe's Digital Future- Council Conclusions", in which the document underlines "increased connectivity, while empowering digital services, can result in citizens, companies and governments being exposed to cyber threats and crimes that are increasing in number and sophistication" (The Council, 2020, p. 11). While the document addresses the threat to critical infrastructure and communications networks, it does not fail to include citizens.

In addition to its focus on EU citizen, "EU values" are positioned as objects in need of protection in cyberspace. This includes fundamental rights, democracy and the rule of law (European Commission, 2010, p. 4, 2013, p. 2). The EU discourse analysis illustrates that the EU's idea of security is derivative of what they perceive to be the most important features of their function as a governance body, that is the focus on protecting EU citizens and values. While other areas are discussed such as economics and infrastructure, the language brings them back to how they are important for the individual or EU values. Thus, illustrating a key distinction between EU and NATO.

The first *Joint Declaration* cites that "our citizens demand that we use all ways and means available to address these challenges so as to enhance their security" (NATO & European Union, 2016). With regards to cyber, the declaration does not focus on the individual but rather more broadly expanding "coordination on missions and operations, exercises and on education and training" (NATO & European Union, 2016). The "Statement" on the joint declaration states that "the overall goal of NATO and EU remains the same: maintain peace and stability and promote security for our citizens" but no other reference to the individual is made throughout the text

(NATO et al., 2016). The *Joint Declaration on EU-NATO Cooperation* opens with acknowledging that the EU-NATO cooperation has "improved the security of our citizens", and that the tools developed together has provided "greater security to citizens" (NATO & European Union, 2018). While the citizen is present in the joint documents, they do not directly connect them to the field of cybersecurity or defence.

### 6.1.2 EU and NATO Threat Perception in Cyberspace

The perception of cyber threat is derivative of NATO's perception of threats in traditional domains. This is evident through the language that is used to describe cyberspace and the security implication of its use. As previously mentioned, the first reference to cyber in the data is through "cyber attack" in the Prague Summit (NATO, 2002). This stood in contrast to early EU language, which was open to using cyber "incident" which encompasses a broader concept of what is potentially harmful in this domain. This use of "attack" continues on in the "Strategic Concept" in which the use of war is presented. Within this strategic concept, it focuses on the impact of technological trends using "electronic warfare" as positioned to have a "major global impact on NATO military planning and operations" (NATO, 2010b, p. 12). The vocabulary changes again in the *Secretary General's Annual Report 2012* that introduces "cyber warfare" into the discourse. Within the context of this report, "cyber warfare" is used as one of the "security challenges of the 21st century" that the alliance faces while its members are focused on fixing their economics, arguing that "while there is a price to pay for security, the cost of insecurity can be much higher", adding that "any decision to cut our defence spending will have an impact on the security of our children and grandchildren" (Rasmussen, 2013). The "Strategic Concept" mentions "foreign militaries, intelligence services, organized criminals, terrorist and/or extremist groups" as possible sources of cyber-attacks (NATO, 2010b, p. 11).

Shires argues that one of the main ways that cyber domain has influenced how NATO perceives security is "how NATO sees security revitalized" as it provides for NATO a greater reason for existence given the cybersecurity threats and cyber attacks by Russia (Interview 1). Therefore, while NATO faces issues with the cyber domain, "the overall theme is cybersecurity and Russia's offensive actions in cybersecurity [giving] NATO a new reason for existence" (Interview 1).

Unlike NATO, the EU's representation of the cyber threat is much broader, focusing on areas such as cybercrime, child pornography, cyber attacks, protection of personal data, privacy, critical infrastructure, and even mistakes. The concept of cyber defence enters discourse in 2013 through the "Cybersecurity Strategy of the European Union" in which language such as "cyber resilience" and "cyber defence" are at the core of the strategic priority (European Commission, 2013). The text states that "cyberspace should be protected from incidents, malicious activities and misuse" (European Commission, 2013). The EU recognizes that cyber threats can have multiple origins such as "criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes" (European Commission, 2013, p. 3). A key issue that the EU cyber discourse includes, that NATO's does not, is the possibility of government misuse of cyberspace for "surveillance and control" over its citizens. To counter this, the EU promotes freedom online and the assurance of respect of fundamental rights online. (European Commission, 2013, p. 3).

Furthermore, the EU highlights the "borderless" nature of cyberspace, which informs its perception of "large-scale cross border incidents and crises" (The Council & European Parliament, 2019). The *Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises* states that due to cybersecurity incidents unpredictability and its ability to cross borders, "cybersecurity incidents are often not contained with any specific geographical area and may occur simultaneously or spread instantly across many countries" (Commission, 2017, p. 2). The EU's holistic conceptualization of cyberspace translates to the way in which it perceives cyber threat and security, stating that "cyberattacks are on the increase and a connected economy and society that is more vulnerable to cyber threats and attacks requires stronger defences" (The Council & European Parliament, 2019). Through an understanding of the reliance the EU and its citizens have on this domain, the discourse captures a broader conceptualization of cyber threats, and thus, a broader view of cyber security and defence.

The Joint documents illustrate that NATO's conceptualizing of cyber threats are the most prevalent. The *2016 Joint Declaration* focuses on "cyber security and defence" with regards to institutional cooperation with missions and operations (NATO & European Union, 2016). The 2017 "common set of new proposals" discusses the "cyber aspects and implications of crisis management and response", focusing on the operational part of cyber defence (NATO & European

Union, 2017). The 2018 "Joint declaration" is in line with previous statements focusing on "cyber attacks" (NATO & European Union, 2018).

### 6.2 The "in-between"

Critical military studies provides this analysis with a lens that critically examines the preconceived notions of the lines between "civilian" versus "military", and "peace" versus "conflict". Within this thesis, it analyzes whether the introduction of cyberspace and cybersecurity is blurring these lines.

The civilian and military line is relatively intact within NATO discourse, which can be attributed to the predominately state-centric approach to security and defence within cyberspace. Where we see this grey area is in the role of the private sector as security providers and NATO's reliance on the private sector for assistance. Partnership with industry is seen as a key component of cyber security and defence within NATO discourse. This is institutionalized in the Wales Summit that established NATO Industry Cyber Partnership. Within this document, NATO outlines the critical role the private sector plays in meeting NATO and Allies Enhanced Cyber Defence Policy objectives. This also solidifies the private sector as a key actor in this domain. The discourse within the NATO Industry Cyber Partnership expands on the private sector's role in this domain by stating that "as the majority of networks are owned and operated by the private sector, its technological innovations and expertise are crucial for cyber defence" (NATO, 2014a). Additionally, the role of industry in NATO's approach to security and defence led to the Industry Malware Information Sharing Portal which "facilitates the sharing of unclassified technological cyber information between NATO and industry representatives" (Stoltenberg, 2017, p. 24).

In comparison, the EU's discourse on the role of the private sector illustrates that the EU is aware that they are not the central actor in cyberspace, therefore require insight and cooperation with the private sector and EU citizens. From the establishment of ENISA, EU discourse has clearly stated the important role the private sector plays, "[a]s electronic networks, to a large extent, are privately owned, the Agency should build on the input from and cooperation with the private sector" (European Parliament and of the Council, 2004). This carries into the "Cybersecurity Strategy" which clearly outlines that while governments have a "significant role in ensuring a free and safe cyberspace", the private sector provides the actors that operate a significant part of "cyberspace" (European Commission, 2013, p. 2). Additionally, the strategy illustrates that the

EU's perception of cyber threat carries over to this blurring of the line as they conceptualize that cyber "threats are multifaceted [therefore], synergies between civilian and military approaches in protecting critical cyber assets should be enhanced" (European Commission, 2013, p. 11). One of the key differences in the EU and NATO discourse on background is that the EU early on states that "any initiative aiming to be successful in this area has to recognise [the private sectors] leading role" (European Commission, 2013, p. 2). While NATO discourse shows that it perceives the private sector actors as partners, it does not admit to the same degree as the EU on how large a role they play.

Regardless, both the EU and NATO blur the line between traditional security providers such as the state by clearly demonstrating the necessity of civilian partnerships to achieve security within this domain both in the language used and in their practices. The interviews with both James Shires and Paul Timmers concurred with this analysis. Shires states that one of the main differences between EU and NATO cooperation within cyberspace as opposed to traditional domains is that "neither the EU nor NATO are key actors in this space as other traditional domains" (Interview 1). As such, "both of them have to look elsewhere to rely on private partners, big technology companies as both the EU and NATO realize their relative lack of confidence in this area" (Interview 1). Louise Marie Hurel adds to this, stating that "while we know that knowledge is not confined to a particular sector, we do understand that when it comes to engaging in this space there is no way that either NATO or the EU have the whole picture, and we never know if we can ever have the whole picture" (Interview 3). She points to the discourse of public-private partnerships and how it can be operationalized pointing to "how Microsoft has been engaging as a diplomatic actor, or trying to pose themselves as diplomatic actors, in the norms making space, the cybersecurity norms, at the international level and the contestation and tension that can occur (Interview 3).

Åsne Kalland Aarstad speaks on public-private partnerships stating, "in some kind of ways they can be self-explanatory, but actually it just clouds more than it reveals. Surfing on this "partnership" and "collaboration" is a good thing, sure. But when it concerns public money, the evolution of technologies, policies that may have severe public implications then obviously the need to have full transparency about the limits, use and regulation is very important and very often it is not" (Interview 4). She adds that the field of public-private partnership "is a field that people

can easily get intimidated by because people speak with such certainty about things that are absolutely uncertain, so the next time someone tells you "oh it's a public private partnership" it's important to ask who has ownership and regulations. You should never assume that those questions are actually answered, it is a field that is filled with jargon and anecdotes. But very often you will realize that there are clear limits of how much people actually know" (Interview 4).

Timmers points to a larger technological trend: whereas previously, military technology would make its way to civilian markets, this trend is now reversed. Technology is today moving from the market side to the military. He believes this trend "will firmly continue". Additionally, he points to the Computer Emergency Response Teams as one of the ways in which there is a blurring between military and civilian. In relation to the power dynamics between the EU and the private sector, Timmers states that while in the past the private sector could be seen as the sector in the driving seat, the general trend is now being reversed due to sovereignty concerns, "governments are starting to take back, to a degree, control from global industry" (Interview 2).

In addition to the blurring of lines between military and civilian through public-private partnerships. Unlike NATO, the EU allocates security responsibilities to its citizens as part of its cyber security and defence approach. The discourse analysis illustrates that for the EU, cybersecurity is a "common responsibility" (European Commission, 2013, p. 8). This does not only refer to private and public actors but the text specifically states that "individual citizens" have a shared responsibility to take action to protect themselves and "if necessary, ensure a coordinated response to strengthen cybersecurity" (European Commission, 2013, p. 4). This approach is not only used on cyber security but also in cyber defence. Under "Developing cyber defence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP)" of the strategy, the discourse on cyber defence is that "given that threats are multifaceted, synergies between civilian and military approaches in protecting critical cyber assets should be enhanced" (European Commission, 2013, p. 11). In the context of cyber defence, the cooperation is seen as vital, not just between the public and private sector but also with academia in the EU. This discourse is prevalent into 2020 as the EU reiterates that "cybersecurity is a shared responsibility of all players" and "stresses the importance of education EU citizens through appropriate digital skills programmes on mitigating cyber threats" (The Council, 2020, p. 14).

This conceptualization of cyberspace creates the parameters in which EU policies and practices operate. The EU discourse, unlike the NATO discourse, emphasizes the importance the "end user" plays in ensuring security of networks and information systems. Therefore, by raising awareness the EU hopes its citizenry becomes "empowered" to guard itself against these threats (European Commission, 2013, p. 8). This is showcased with ENISA's objective to "promote a high level of cybersecurity awareness, including cyber-hygiene and cyber-literacy among citizens, organisations and businesses" (The Council & European Parliament, 2019, p. 2). One of these efforts is through the ENISA's "European Cybersecurity Month" which aims to raise awareness of cybersecurity threats by promoting cybersecurity among citizens and organizations and providing citizens with "resources to protect themselves online, through education and sharing of good practices" (ENISA, 2013). The message is clear: for the EU, "cyber security is a shared responsibility!" (ENISA, 2013).

These practices are in line with the EU's understanding of cyberspace and cybersecurity as "Cybersecurity is not only an issue related to technology, but one where human behaviour is equally important. Therefore, 'cyber-hygiene', namely, simple, routine measures that, where implemented and carried out regularly by citizens, organisations and businesses, minimise their exposure to risks from cyber threats, should be strongly promoted" (The Council & European Parliament, 2019). As stated in the European Union Global Strategy "[c]ooperation and information-sharing between Member States, institutions, the private sector and civil society can foster a common cyber security culture, and raise preparedness for possible cyber disruptions and attacks" (EU High Representative for Foreign Affairs and Security Policy, 2016, p. 22).

Furthermore, it showcases that these practices are required due to the "interconnected and complex nature of cyberspace" which " requires joint efforts by governments, private sector, civil society, technical community, users and academia to address the challenges faced" (Council, 2018, p. 2). Through this framework, the EU focuses on providing civilians such as citizens, organizations and business the tools they need to defend themselves in this domain. This is done in two key ways. The first is by raising awareness of cybersecurity issues as discussed above through public awareness campaigns and investments in education. The second is to build trust through the European cybersecurity certification framework which establishes requirements for European cybersecurity certification that will be recognized and used in all Member States. Thus,

providing common requirements and evaluation criteria across sectors and markets (The Council & European Parliament, 2019). This equips the public by providing information in "a transparent manner on the level of security of ICT products, ICT services and ICT processes that stresses that even a high level of cybersecurity certification cannot guarantee that an ICT product, ICT service or ICT process is completely secure." (The Council & European Parliament, 2019).

### 6.2.1 Blurring the Line Between Internal and External Security

The EU discourse illustrates that in addition to the blurring of lines between EU citizens and security providers, there is a blurring more broadly within the EU between internal and external security. *The European Security Strategy* connects internal and external security stating "The post Cold War environment is one of increasingly open borders in which the internal and external aspects of security are indissolubly linked" (European Commission, 2013, p. 4). This continues onto the *European Agenda on Security* which emphasizes the need to bring "internal and external dimensions of security" together explaining that security is not "confined by borders of the EU". As such, "EU internal security and global security are mutually dependent and interlinked. The EU response must therefore be comprehensive and based on coherent set of actions combining the internal and external dimensions" (European Commission, 2015, p. 4). This discourse is prevalent in the *Global Strategy for the European Union's Foreign and Security Policy* as it restates "internal and external security are ever more intertwined: our security at home depends on peace beyond our borders" (EU High Representative for Foreign Affairs and Security Policy, 2016, p. 7). This borderless security discourse is in line with the EU's conceptualization of cybersecurity as a borderless security threat as previously analyzed. As such, it reinforces the blurring of the lines between the EU's internal and external security objectives.

### 6.2.2 EU-NATO Cooperation Blurring the Lines

On a broader level, EU-NATO cooperation discourse illustrates this blurring of lines between civilian and military through the increased cooperation between the two organizations. NATO, a military alliance, and the EU as a governance structure have become more intertwined than ever before. The analysis of this thesis focuses in on the impact of cyber in this process.

Within the NATO documents analyzed, EU-NATO cooperation and partnership has progressively increased. Starting with the Prague Summit in which the EU is positioned as a natural ally early on within this summit due to "common strategic interests" (NATO, 2002). The areas of

cooperation and assistance are listed as land, sea, and air. The creation of the NATO Response Force (NRF) is quickly followed by its relation to the EU's Headline Goal, stating that they "should be mutually reinforcing while respecting the autonomy of both organisations" (NATO, 2002). NATO discourse cites "shared common values" and "strategic interest" contributing their cooperation in the Western Balkans and the Berlin Plus agreement with regards to operation Althea which states that it is contributing to "peace and security" (NATO, 2006). The summit declaration states that NATO will continue to strive for improvements in the partnership to "achieve closer cooperation and greater efficiency, and avoid unnecessary duplication, in a spirit of transparency and respecting the autonomy of the two organisations. A stronger EU will further contribute to our common security" (NATO, 2006). This sentiment is reiterated in the Strategic Concept Active which describes the EU as "a unique and essential partner for NATO" as they share a majority of members and common values (NATO, 2010b, p. 28).

The cyber discourse and EU-NATO cooperation discourse intersect for NATO in the 2010 Lisbon Summit Declaration. It does so by building on an intertextually implicit idea that "cyber threats are rapidly increasing and evolving in sophistication". Therefore, "to address the security risks emanating from cyberspace, [NATO] will work closely with other actors, such as the UN and the EU, as agreed"(NATO, 2010a). This continues into the Secretary General's Annual Report 2014 in which "cyber defence" is listed as one of the areas that consultations have broadened to address common concerns such as "cyber defence", listing it along with the proliferation of weapons of mass destruction, counterterrorism, and energy security. This section of the report intertwines cyber discourse, EU-NATO cooperation discourse, and evolving security environment discourse. In this context, cyber defence is used as a key area that the EU and NATO will cooperate in, along with traditional threats such as weapons of mass destruction. Listing it along with these traditional threats elevates cyber defence and the threat that it represents. The NATO Wales Summit states that "strong partnerships play a key role in addressing cyber threats and risks". Therefore, NATO will "continue to engage actively on cyber issues with relevant partner nations" and "international organisations" (NATO, 2014b).

This discourse continues in NATO's *Cyber Defence Pledge* which states that it welcomes work with the EU on enhancing cyber security and links this to the broader resilience of the Euro-Atlantic region, supporting "further NATO-EU cyber defence co-operation" (NATO, 2016a). As

this is a short pledge, including the EU shows the importance of this cooperation in relation to cyber defence. Unlike other NATO documents, where the EU is part of the international organizations NATO points to such as the United Nations, the EU is the only other international actor mentioned in this pledge. Through discourse analysis of NATO documents, it is evident that cooperation with the EU has become a core part of NATO's cyber defence policy. This cooperation is not merely practical but has become part of NATO's story. The "Secretary General's Report" significantly contributes to this discourse by stating that "[i]n 2016, the long-standing strategic partnership between NATO and the European Union (EU) was taken to a new level. Both organisations face security challenges of a new depth and complexity, and neither has the tools to overcome those challenges alone. By cooperating more closely than ever, the EU and NATO are making a real difference to the welfare and security of the people they serve" (Stoltenberg, 2017, p. 77).

To add to this, the 2018 report provides a historical section on "NATO and European Integration" that other reports have not had. The section opens with "rising from the ashes of the Second World War, NATO and what is now the European Union were created with a crucial goal: preventing the horrors of another war in Europe" (Stoltenberg, 2019, p. 90). This unites the origin story of both the EU and NATO. It then moves to claim that NATO has been the "cornerstone of European Security", and due to this protection it has "helped the European Union achieve peace, prosperity and political cooperation" (Stoltenberg, 2019, p. 90). This is a representation of how NATO views its role in the success of the EU, and its importance to European security. This plays a role in the power dynamic between the two organization. The EU's history shows a reliance on NATO, and as they cooperate moving forward, this history builds the context of their practices.

The EU documents analyzed do not discuss NATO to the same extent as the NATO documents' discussions on the EU. Within the 2009 European Security Strategy, the EU urges a "renewal of the multilateral order" stating that "the EU and NATO must deepen their strategic partnership for better co-operation in crisis management" (The Council, 2009, p. 9). The 2013 Cybersecurity Strategy gives insight to the EU's perception of this blurring of the line between civilian and military approaches to protecting critical cyber assets as it explains that cyber threats are "multifaceted" and therefore require "synergies between civilian and military approaches" (European Commission, 2013, p. 11). From this standpoint, the cooperation with NATO is an

extension of the EU's conceptualization of the type of threat cyber presents and therefore, the joint approach to solving it by exploring the "possibilities on how the EU and NATO can complement their efforts to heighten the resilience of critical governmental, defence and other information infrastructures on which the members of both organisations depend" (European Commission, 2013, p. 11). In the 2016 Shared Vision, Common Action: A Stronger Europe, the EU states that it will deepen its partnership with NATO through coordinated defence capability development, parallel and synchronised exercises, and mutually reinforcing actions to build the capacities of our partners, counter hybrid and cyber threats, and promote maritime security" (EU High Representative for Foreign Affairs and Security Policy, 2016, p. 37).

The Joint Declarations made by the EU and NATO is a monumental step towards cooperation. The 2016 Joint Declaration between the EU and NATO reinforces this cooperation, the document stating that due to the "common challenges" they must "step-up" their efforts to work together by establishing "a new level of ambition" citing their "interconnected" security (NATO & European Union, 2016, p. 1). The document states that EU-NATO cooperation would lead to the mobilization of a "broad range of tools" that would respond to the challenges they face and ensure efficient use of resources. This is in line with previous discourse on EU-NATO cooperation working to avoid duplication. The Joint Declaration explains that "[a] stronger NATO and a stronger EU are mutually reinforcing" as it would provide security both in "Europe and beyond" and "[t]ogether they can better provide security in Europe and beyond" (NATO & European Union, 2016, p. 1). In order to ensure this joint security, the declaration states that there is an urgent need to "expand our coordination on cyber security and defence including in the context of our missions and operations, exercise and on education and training"(NATO & European Union, 2016, p. 1).

The "statement on the implementation of the Joint Declaration" includes an ANNEX which contains the "common set of proposals for the implementation of the Joint Declaration" that includes a wide range of areas of cooperation including, countering hybrid threats, operational cooperation including maritime issues, defence capabilities, defence research and industry, exercises, defence and security capacity-building and cyber security and defence (NATO et al., 2016). The document includes EU-NATO cooperation with regards to countering hybrid threats, mainly through situational awareness that includes cyber security The "cyber security and

defence" section outlines "with immediate effect, EU and NATO will exchange concepts on the integration of cyber defence aspects into planning and conduct of respective missions and operations to foster interoperability in cyber defence requirements and standards", and strengthen cyber cooperation training by harmonizing training requirements and opening training courses for "mutual staff participation" (NATO et al., 2016). Staff cooperation is given additional attention to strengthen their joint cooperation in cyber exercises through "reciprocal staff participation in respective exercises" which include both the Cyber Coalition and Cyber Europe (NATO et al., 2016).

In the "Common set of new proposals", within the cyber security and defence field, the focus is on the "exchange between staffs' relevant good practices concerning the cyber aspects and implications of crisis management and response". This includes operational aspects such as "analysis of threats and malware information" in order to improve the understanding, as well as operational aspects of cyber defence, such as analysis of threats and malware information, with a view to improving the understanding of and identifying potential synergies between the two organisations' approaches, including existing cyber security incident response teams. This discourse is intensified in the 2018 *Joint Declaration on EU-NATO Cooperation*. The document states that closer cooperation has "improved the security of our citizens and strengthened our transatlantic bond", and that the cooperation has "developed substantially, and is now unprecedented in its quality, scope, and vigour" (NATO & European Union, 2018). The document restates again that the EU and NATO share "the same values" "common challenges" and that their security is "interconnected" (NATO & European Union, 2018).

### 6.2.3 Blurring The Line Between Peace and Conflict

NATO states that "cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging", and that "[c]yber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack". This is used as evidence or to provide context to their decision that in the case of a cyber attack, the "invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis" (NATO, 2014b). This decision is in line with conceptualizing cyberspace as an extension of traditional domains. This approach utilizes a strategic use of ambiguity in cyberspace approach. This lack of accountability can be dangerous

as there are no clear lines of consequences in cases of attacks (Libicki, 2011). By not creating strict lines as to what cyber attack would trigger the invocation of Article 5, other states would not know what line to go under but rather must risk that any attack, no matter how small, can invoke this Article. While this debate continues, the invocation of Article 5 by NATO in reference to cyber attacks illustrates that they view this act as a serious transgression. This premise blurs the line between peace and conflict because NATO has through its report, such as the Secretary General's Annual Report 2015, reported that an average of 320 cyber incidents occurred per month which is a NATO wide 20% increase from 2014 (Stoltenberg, 2016, p. 23). Seeing as NATO does not report the severity of these incidents, it leaves the current security environment with a blurred line between peace, in which there are no attacks against NATO, and conflict.

### 6.3 Co-production

This section will analyze how the EU and NATO create this space through the values they export into the domain. As argued throughout this thesis, through an STS co-production framework, the way in which NATO and the EU know and represent the world is inseparable from the way in which they choose to act within it.

The NATO documents make intertextually explicit reference to the Washington Treaty. While this treaty is referenced throughout the documents analyzed, this thesis is analyzing the values exported into cyberspace. Therefore, will not consider general references to the Washington Treaty as part of this analysis. The 2014 Wales Summit "recognizes that international law, including international humanitarian law and the UN Charter, applies in cyberspace" (NATO, 2014b). It does not go into detail into how these laws are applicable in cyberspace. Along with this recognition, the Summit states that cyber attacks could lead to the invocation of Article 5, but that this decision is made "on a case-by-case basis" (NATO, 2014b).

NATO's *Cyber Defence Pledge* reiterates NATO's stance as it reaffirms the applicability of international law in cyberspace. It also acknowledges the work done to establish "voluntary norms of responsible state behaviour and confidence-building measures in cyberspace" (NATO, 2016a). However, it does not go into specifics as to what these norms are and which international organizations are working to develop them. The Warsaw Summit Communiqué builds on this as it is the first time that NATO recognizes cyberspace as a "domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea" (NATO, 2016b). NATO

believes that this will improve its ability to protect and conduct operation across the domain to "maintain our freedom of action and decision, in all circumstances"(NATO, 2016b). While cyber threats have been compared to traditional threats, the move to operationalize cyberspace as a domain of operation akin to traditional domains raises new questions such as the approach NATO will take in this new realm. The language is still that of a defensive approach and states that it will continue to "follow the principle of restraint and support maintaining international peace, security, and stability in cyberspace" (NATO, 2016b). This statement illustrates that while NATO aims to maintain peace and stability in cyberspace, it is possible to have war and instability within this domain. Thus, cyber peace is not inherent but requires intentional effort. This defensive approach to cyberspace is reiterated in NATO's continuing mission mandate, "which remains entirely defensive and is conducted in accordance with international law" (Stoltenberg, 2017, p. 24).

The concept of "sovereignty" is introduced into the discourse in the Brussels Summit, which reports that NATO "agreed how to integrate sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions, in the framework of strong political oversight" (NATO, 2018). In addition, it reaffirms NATO's commitment "support work to maintain international peace and security in cyberspace and to promote stability and reduce the risk of conflict, recognising that we all stand to benefit from a norms-based, predictable, and secure cyberspace" (NATO, 2018). In the 2019 Article, by NATO Secretary General, Jens Stoltenberg states that "[c]yberspace is the new battleground". Therefore, "making NATO cyber ready—well-resourced, well-trained, and well-equipped—is a top priority as we look towards the NATO summit in London in December and beyond" (NATO, 2019).

The *Secretary General's Annual Report* for 2019 has a section titled "Women in Cyber" that highlights the role of women in the field, stating that "women make defence force more effective" and that "women are also key players" in cyber defence as they bring in diverse new perspectives (Stoltenberg, 2020, p. 28). Organizing events that provide "opportunities to enhance understanding of the importance of gender diversity in the cyber domain" (Stoltenberg, 2020, p. 28). This allocation of space towards gender equality within a domain is not given to other sections such as hybrid threats, space, or arms control. Thus, illustrating that NATO's discourse on values expands to include gender equality within the cyber field.

The EU documents illustrate a more intentional approach to how the values exported into cyberspace will impact both the domain and its governance. From the establishment of ENISA, the agency is given the task of contributing to the EU's efforts to cooperate with third countries and international organizations "to promote a common global approach to network and information security issues, thereby contributing to the development of a culture of network and information security" (European Parliament and of the Council, 2004). This common goal, development of cultural approach to this space, illustrates that the EU is aware of the "norm setting" powers that it can have and the importance of international cooperation in this field as it has made it one of 11 tasks given to the agency.

This narrative of cyberspace evolved, and in 2013, the EU presented their first "Cyber Security Strategy of the European Union" which clarifies that EU principles such as fundamental rights and freedoms apply in cyberspace. One of the five core priorities is "establishing a coherent international cyberspace policy for the EU, and promoting core EU values" (Commission, 2013). It builds context around cyberspace, stating that over the past two decades, the internet and "more broadly cyberspace" has impacted all parts of society (European Commission, 2013, p. 2). From the EU documents analyzed so far, this is the first time "cyberspace" is used to refer to this domain, as previous texts have focused on the "internet". The introduction continues to list the ways we depend on information and communication technologies, listing "fundamental rights" as one of them. The EU clearly states its position on a "open and free cyberspace", stating that it has promoted "political and social inclusion" around the world, "broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe", and it continues to state that this space has provided "a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies - most strikingly during the Arab Spring" (European Commission, 2013, p. 2).

This context that the EU builds is heavily influenced by values and the impact of cyberspace on these values. It does not open with the perception of threat in the space, but rather the opportunities it has provided. The strategy reiterates the discourse that "EU's core values apply as much in the digital as in the physical world" This includes the laws and norms. The values discussed are "protecting fundamental rights, freedom of expression, [and] personal data privacy",

refereeing to the Charter of Fundamental Rights of the European Union. Under this principle, the EU discourse yet again combats the possibility of government misuse of data for the purpose of cyber security. The document states that "[a]ny information sharing for the purposes of cyber security, when personal data is at stake, should be compliant with EU data protection law and take full account of the individuals' rights in this field." (European Commission, 2013, p. 4). The second principle listed is "access for all". In this case, the discourse on cyber and security is not only linked directly to the values of the EU, but also the rights of EU citizens by stating, "the Internet's integrity and security must be guaranteed to allow safe access for all". This focus on individual citizens' responsibility is further enhanced in the EU's understanding that "raising awareness" is key to ensuring that cybersecurity is a "common responsibility" (European Commission, 2013, p. 8).

The "Cybersecurity Strategy" continues to expand on the principles to include "democratic and efficient multi-stakeholder governance". The key aspect that this section contributes to the discourse is the awareness the EU has of their lack of centrality in this space by acknowledging non-governmental actors within this space. Thus, its multi-stakeholder governance principle comes from a place of full public acknowledgement that within cyberspace, the EU is not a central actor and needs the support and cooperation of other actors in order to achieve governance goals (European Commission, 2013, p. 4). The final principle is "a shared responsibility to ensure security". Unlike the NATO discourse, the EU takes a collective approach to cyber security as analyzed earlier in this chapter (European Commission, 2013, p. 4). The EU's strategy goal is clear: to provide the highest possible freedom and security for the benefit of everyone. While this document does acknowledge that the Member States are the ones with the task of security challenges in cyberspace, the strategy helps in providing specific actions that can strengthen EU's overall performance.

The EU's "Internet Policy and Governance: Europe's role in shaping the future of Internet Governance" delivers a clear vision of how the EU conceptualizes this space and the values that it exports based on these conceptualizations. The document identifies that the Internet is "an essential part of life" and has fostered "innovation, growth, trade, democracy and human rights". However, "this economic potential needs to be further exploited ensuring that individuals can access the content, goods and services they want, and control which personal data they want to share or not",

highlighting the individual as the focus of the EU's internet governance vision, and adding that "an open and free Internet in which all rights and freedoms that people have offline also apply online facilitates social and democratic progress worldwide" (European Commission, 2014).

The EU's understanding of internet governance is a collective approach and refers to the "development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet" (European Commission, 2014). The document states that there are "conflicting visions of the future of the Internet and on how to strengthen its multi-stakeholder governance in a sustainable manner have intensified" while referencing how "large-scale surveillance programmes" and "fear of cybercrime" have hurt the trust in the Internet and fears the consequences this has on slowing down innovation and the growth of European internet companies and the possibility of fragmentation of the internet (European Commission, 2014).

The document "proposes a basis for a common European vision for Internet Governance", one that defends and promotes "fundamental rights and democratic values, and multi-stakeholder governance structures that are based on clear rules that respect those rights and values", " a single, un-fragmented network subject to the same laws and norms that apply in other areas of our day-to-day lives; and where individuals can benefit from their rights, and from judicial remedies when those rights are infringed", a clear understanding that "the Internet is built and maintained by a variety of stakeholders, as well as governments", with decisions made in this space based on "transparency, accountability and inclusiveness of all relevant stakeholders" (European Commission, 2014).

Based on these values that the EU promotes in cyberspace, it clearly states that "blocking, slowing down or discrimination of content, applications and services goes against the open nature of the Internet", thus making it clear that the EU's conceptualization of this domain is one that is inherently open. Any attempt to go against this is cited as hurting both economic growth and the "free flow of information" (European Commission, 2014). The document views the "Internet as a space of Civic responsibilities" and a driving force of "globalisation", acknowledging that internet protocols "can have significant public policy implications" and that their designs can impact "human rights such as users' data protection rights and security, their ability to access

diverse knowledge and information, and their freedom of expression online" (European Commission, 2014).

Discussing the establishment of Internet Governance, the document includes insight by "grassroots initiatives" as an "integral part of the Internet ecosystem", and states that "the implications of this evolution in norm setting in relation to the Internet requires an open public debate with all concerned". It proposes a workshop which will include European Internet Industry but also "international experts in law, ethics, social sciences, economics, international relations, and technology that will make recommendations to ensure coherence between existing normative frameworks and new forms of Internet-enabled norm-setting" (European Commission, 2014).

This focus on fundamental rights is carried onto the "Directive (EU) 2016/1148" that states that the Directive "respects the fundamental rights, and observes the principles, recognised by the *Charter of Fundamental Rights of the European Union*, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles" (European Parliament & The Council, 2016). These ideas are reiterated in the "Declaration by the High Representative on behalf of the EU on respect for the rule-based order in cyberspace" which reaffirms that the EU and its Members States "are firm promoters of an open, stable and secure cyberspace, respectful of human rights, fundamental freedoms and the rule of law. Cyberspace offers significant opportunities for social, political and economic development" (European Council, 2019b).

The EU conceptualizes upholding international law as applicable to cyberspace and its focus on respect for international law, and the United Nations Charter as "essential to maintaining peace and stability"(European Council, 2019a). Furthermore, through analyzing the EU's "Cyber Diplomacy Toolbox", the EU's values in this space guide its approach to settling international disputes in cyberspace through "peaceful means" and their diplomacy extends to cyberspace to promote security and stability in this domain through "increased international cooperation", "reducing the risk of misperception, escalation and conflict that may stem from ICT incidents" (Council of the European Union, 2017, p. 4). The joint documents do not include any reference to

the values either organization is instilling in cyberspace or reference to cyber governance structures.

# 7. Discussion

## 7.1 Diverging Conceptualizations

The analysis illustrated that cybersecurity is conceptualized differently by the EU and NATO, showing that ideas of technology and security are derivative and co-produced. In the case of cybersecurity it blurs the lines between pre-established boundaries around civilian and military, and peace and conflict. Using co-production as one of the frameworks demonstrated that cyberspace is shaped based on how actors choose to represent, and behave in, this domain. As such, their practices are reflective of that. While the EU takes a broader approach to cyberspace and what security means within this domain, NATO takes a much narrower approach to this domain seeing it predominately from a threat perspective. This transfers to who and what they believe is the referent object within cyberspace, and what and who is to be protected.

NATO focuses on the state, systems, and expands to include democratic and economic institutions. Alternatively, due to the EU's broad conceptualization of cyberspace, its documents illustrate that their referent object is the EU citizen, EU values, and economic stability. While it does discuss protection of systems, it focuses on it in reference to the impact it would have on the individual. In addition to their differences in perception of the security environment, more specifically cyberspace, and who and what is to be protected, has created the parameters of what a threat in this space can look like. For NATO, it views threats from a traditional perspective of "cyber attack" and then moves on to include "cyber warfare", whereas the EU has a much wider idea of what cyber threats are to include cybercrimes such as child pornography and fraud, protection of personal data, privacy, barriers to a free cyberspace, and traditional threats such as cyber attacks; cyber threats to critical infrastructure and its impact on democratic and economic institutions. This discourse analysis is in line with the insight Paul Timers provided, stating that the EU and NATO do not have the same interests and that it will become more explicit because of this conceptualization of where cybersecurity belongs, and the conceptualization of cyberspace.

How these actors view cyberspace, cybersecurity, and cyber threats has progressed and transformed through time. For NATO, early in the discourse, cyber threats are viewed in the forms of "attacks". Throughout the texts this threat perception changes based on external events. For example, the cyber attacks on Estonia and Georgia in 2007 and 2008 respectively, prioritized cyber issues for NATO. However, this introduction sets a reactive approach to how NATO views this

domain. This is evident through analyzing documents written during the time around the Estonia and Georgia attacks, which predominantly focus on protecting networks and the state against cyber-attacks. However, this expands in the Secretary General's Report of 2016 to include protecting democratic systems as a reaction to the 2016 US Presidential Election. Alternatively, the EU's conceptualization of cyberspace and its threats illustrate a movement from internal security concerns to include external security concerns.

This raises the question: how can we understand EU-NATO cooperation in cyberspace with regards to cybersecurity and defence? With regards to diverging conceptualizations, their cooperation in this domain provides them with an opportunity to benefit from the parameters of their counterpart. How each organization has decided to define cybersecurity and threats have set the parameters on their practices. Therefore, EU and NATO cooperation in cybersecurity brings together both capability, through NATO, and diplomatic capital, through the EU. Through cooperating with the EU, NATO gains a partner that takes on a cyber diplomacy role within cyber external security areas, providing NATO a diplomatic route to engage with cyber issues through the EU's cyber diplomacy toolbox. This is especially important for NATO as it has declared that a serious cyber attack can trigger Article 5, in which an attack against one ally is treated as an attack against all NATO allies (NATO, 2014b, 2019).

Therefore, cooperating with the EU in this domain provides NATO with diplomacy capabilities that can aid in deterring serious attacks by holding smaller ones diplomatically accountable. Cyber diplomacy is increasingly important in order to avoid a collective defence trigger. Through a diplomatic approach to cybersecurity attacks, the EU can step in to impose sanctions, impose restrictive measures such as sanctions, travel bans, arms embargos, and freezing of assets. This diplomatic approach can act as a de-escalation tool that warns off more serious attacks that could potentially trigger NATO's collective defence response. This is evident through the EU's cyber diplomacy toolbox in which "The EU reaffirms its commitment to the settlement of international disputes in cyberspace by peaceful means, and that all of the EU's diplomatic efforts should as a priority be aimed at promoting security and stability in the cyberspace through increased international cooperation, and at reducing the risk of misperception, escalation and conflict that may stem from ICT incidents" (Council of the European Union, 2017, p. 4).

Diverging conceptualization towards cybersecurity and cyberspace has given the EU the opportunity and space to take part in external security areas. Conducting discourse analysis on EU documents illustrates that the EU's conceptualization of cyberspace and security is focused on internal security and while this has changed to include external security, thus blurring those lines, the EU's discourse sets the parameters in such a way that their practices are diplomatic and regulatory. The joint documents illustrate that NATO's discourse is the dominant one, therefore allowing, or creating, room for the EU to participate in securitization conceptualization of cyberspace. As discussed in the literature review regarding the debate on whether or not the EU is a civilian power or not, this thesis has relied on K.E. Smith (2005) approach in which the thesis has aimed to analyze what the EU does in cyberspace rather than what the EU is. From its individual actions EU's powers in cyberspace are diplomatic as it does not possess offensive cyber technologies and for the most part, nation states are the ones responsible for attacks against their systems. This is an increasingly important role as cyberspace is a contested domain that requires diplomatic skill in order to prevent cyber conflicts and ensure stability (Barrinha & Renard, 2020, p. 1).

However, due to their close cooperation with NATO and the dominance of NATO's discourse in joint documents, blurs this perception, especially considering the NATO dominant discourse in joint documents. Therefore, an important implication to consider is whether the EU's cooperation with NATO will influence the way EU's cyber diplomacy aims are perceived by third parties. How will this impact the EU's role as a diplomatic actor when it is backed, through cooperation with NATO, with the might of the largest military alliance? These are important questions that can be explored in further research.

### 7.2 Conceptualization of Cybersecurity

The analysis has shown that the conceptualization of cyberspace and cybersecurity changes based on the actor and how they view the world and the security environment more broadly. In addition, through an STS lens, the point of discussion becomes "why do societies make science and technology - and, along the way, themselves - in one way as opposed to another?" (Felt et al., 2016, p. 2). It questions "how do people shape the development of new technologies?" and "how, in turn, does the development of technological networks, systems, or infrastructures shape, impact, and (re)-configure the human condition?" (Fouché, 2016, p. 495). By critically examining this

cycle of influence, Fouché (2016) analyzes how human efforts in creating technologies both physically and conceptually, continuously puts society in a position to "rethink, reassess, and re-examine" the evolving relationship among themselves and with interconnected complex "sociotechnical arrangements" (Fouché, 2016, p. 495).

The EU and NATO discourse illustrate that the concept of cyberspace and cybersecurity has changed over time. In the case of NATO, this has mainly been as a reaction to external events, such as cyber attacks against Estonia, which can be attributed to why NATO Cooperative Cyber Defence Centre of Excellence is in Estonia. In addition to the discourse of "cyber attack", the referent object changes to include democratic institutions in 2016 following Russian interreference in US Presidential elections. As such, the conceptualization of cyber technologies by NATO is derivative of its understanding of the larger security environment and the role it positions itself as playing and how this technology was used. What people have decided to do with this technology, for example election interference and conducting DoD attacks against a state, have catapulted this re-imagining of the referent object and the broadening of security within NATO. This reassessment of what security is would not have occurred otherwise. In this way, with regards to NATO discourse, this technology has triggered the alliance to "rethink, reassess, and re-examine" their conceptualization of security.

I would argue one further point as to why NATO conceptualizes cyberspace and cybersecurity in the way it has. From the analysis, NATO has progressively allocated more space to cyber threats within its discourse. However, the ideas that it presents about this domain are not objective but a choice. Its conceptualization of "cyber warfare" for example, which is introduced in the Secretary General's Annual Report 2012, positions this concept of "cyber warfare" as a given, using it as evidence as to why member states should continue to invest in NATO. However, from the literature review it is evident that "cyber warfare" is a highly contested concept. As some scholars argue that cyber war has become reality, other scholars believe that this concept is over-stated, and that while cyber has changed warfare in some capacity, cyber warfare is overstated. Therefore, NATO choosing to conceptualize cyber warfare as a threat states that it has chosen the side of the debate it is on despite evidence that cyber attacks in wartime have little or no impact on fighting (Kostyuk & Zhukov, 2019).

This decision to focus on cyber threats and cyber warfare to the extent that NATO has, I argue is a political decision as it revitalizes NATO's purpose as a security provider. Shires speaks on this, stating that cyber threats have given NATO "a far greater reason for existence" (Interview 1). Taking away the conceptualization of cyberspace as a threat and the fear of cyber warfare would leave NATO with fewer reasons for existing. However, as Russian aggression has taken to cyberspace, NATO's decision to side with the idea that cyber warfare is a threat is self-serving as it provides a revitalization of purpose. This can be seen in the discourse, as the first time "cyber warfare" is used is in relation to the importance of funding NATO despite economic turmoil. Therefore, there are political reasons as to how and why cyber threats, and more broadly, technologies, are conceptualized the way they are within NATO. To study cybersecurity without questioning how people shape the development of these new technologies, with a premise that these technologies did not have to be conceptualized this way, thus taking away the determinist lens, leaves us with room to critically engage with these decisions and understand that there is more to this process than just the technology.

The EU's decision to conceptualize cyberspace and cybersecurity the way it has, broadens its security impact on defence, but also the everyday life of EU citizens. This has shaped and impacted how the EU wants its citizens to act by trying to "configure" their approach to cyberspace through their daily interactions with cyberspace. In turn, their daily interactions have helped create the concept of cybersecurity based on the protection of their rights online as well as offline. This is part of the EU's exportation of values into the cyber domain, by taking the position that the "EU's core values apply as much in the digital as in the physical world". This value driven discourse is used as a premise in the EU's diplomacy toolbox that aims to resolve international cyberspace disputes by "peaceful means", and their diplomatic efforts are aimed at "promoting security and stability in the cyberspace through increased international cooperation, and at reducing the risk of misperception, escalation and conflict" (Council of the European Union, 2017, p. 5).

By exporting values into cyberspace, the EU can create room for itself to act as a political power in this domain. The EU's conceptualization of the "borderless nature of cyber threats" leads to the demand for a collective union level approach to "cross-border cyber incidents and crises" (European Parliament, 2019). As it views this threat as one that does not adhere to borders, but

cross borders, it is able to step in to coordinate collective responses, thus benefiting from this conceptualization of cyberspace both economically and diplomatically. It extends EU's power in cyberspace as a diplomatic power, in addition to its ability to influence member states cyber activities. As Shires states, the EU sees cybersecurity as an opportunity "to extend the Brussels effect in other areas where they become the main regulator in technology with regulations and institution design around the world" (Interview 1). As this thesis argues, one of the reasons for EU-NATO cooperation in cyberspace with regards to cybersecurity is due to the EU's diplomatic role in this space and its norm setting approach in cyberspace. Therefore, this conceptualization of the cyber domain by the EU provides it with added legitimacy in international relations through cyberspace governance.

The values and practices that cyber actors impose on cyberspace contributes to what the space becomes. As previously discussed, unlike physical domains, the cyber domain is malleable to change as it is a man-made space. As such, how we conceptualize it and the values we export into it, contribute to what the space becomes. Barrinha and Renard (2020) argue that "the rise of cyber diplomacy coincides with a growing contestation of the values, institutions, and power dynamics of the liberal-created cyberspace", and in this way, "cyber diplomacy is a practice that is always shifting between bridge-building dynamics and defence of long-held national (and regional) principles and interests" (Barrinha & Renard, 2020, p. 3). Cyberspace was conceived from a state of tension between the military and the scientific communities, who both integrated their values and visions into its development. The military's values in cyberspace regarded "survivability, flexibility, and high performance over commercial goals such as low cost, simplicity, or consumer appeal" (Franzese, 2009, p. 10). On the other hand, the scientific community integrated their values of "collegiality, decentralization of authority, and open exchange of information" into this domain (Franzese, 2009, p. 11). The struggle between these two developers is evident in cyberspace to this day, as a push and pull between varying states who take a range of approaches to this space, but also within each individual state.

Cyberspace reflects the kinetic world that is facing a post-liberal shift. Therefore, the values that both the EU and NATO hold in cyberspace are part of a larger project in attempting to reinforce the liberal order. NATO reaffirms the applicability of international law in cyberspace, including the UN Charter, international humanitarian law, and human rights law (NATO, 2014b, 2018). As

illustrated in the analysis, the EU discourse relies more heavily on liberal values such as "open and free cyberspace", seeing its role as "protecting fundamental rights, freedom of expression, personal data privacy", "access for all", and viewing this domain as one that has fostered "innovation, growth, trade, democracy and human rights", "open and free internet", "fundamental rights, democracy and the rule of law", "determined to keep cyberspace open, free, stable and secure where fundamental rights and rule of law fully apply", "open, free and secure Internet", and "multi-stakeholder model of governance" (Council of the European Union, 2017, p. 3; European Commission, 2010, p. 4, 2013, p. 2, 2013, p. 8, 2014, p. 2; The Council, 2020, p. 19). Thus, contributing to the cyber diplomatic role that EU seeks to play. As such, EU-NATO cooperation in cyberspace goes beyond shared membership and their efforts to avoid duplication. Their cooperation in this domain is part of their efforts to reinforce a liberal order in a domain that is currently challenging this liberal order.

### 7.3 The Implications of Blurring the Lines

The analysis illustrated that cybersecurity is blurring the lines between civilian and military in a few different ways. The first is through blurring the lines between who engaged and is perceived as a security provider. Both the EU and NATO have allocated security and defence responsibilities to the private sector, seeing as they both understand that the private sector is a key player in the domain. The EU has taken this a step further and acknowledged that without the private sector's involvement, it would not be able to provide a secure space for its citizens. This thesis's analysis is in line with Oldrich Burnes who argues that the EU's security discourse in cyberspace has progressed from traditional public provision towards one that centralizes the private sector (Burnes, 2018, p. 29). The EU documents illustrate a further blurring between internal and external security, and civilian and military by taking a collective approach to cyber security that includes EU citizens (the end users) as a key component of this framework. Finally, EU-NATO close cooperation acts as a blurring of lines between a military alliance and a governance structure. As discussed earlier, the joint documents illustrate that the military discourse is the dominant one when the two develop joint conceptualizations of security and cyberspace. This illustrates that cyberspace and cybersecurity is a driving force in blurring these lines. However, this raises concerns over the responsibility of the state as they are unable to protect their citizens without the help from the private sector.

This blurring is occurring in both ways, as traditionally military responsibilities are given to the private sector. This raises the implication of the militarization of civilians and politics. On the other hand, as Shires states that "the military now faces more risk from cyber threats because they engage in digital lives as citizens", as military personnel download apps and use smart phones (Interview 1). As such, the amount of information leakage from the military is far greater than it has been previously. Arguing that "just as you see the civilian side moving to blur the lines through intelligence production, you also see that the military is not as closed off as it once was, it is now more open, both to hostile actors and commercial companies. As such, the military is no longer as closed off in terms of what they are doing even as their functions are being taken and given to private companies" (Interview 1). This raises security concerns over the security of the military domain in addition to the concerns over the impact of militarization of civilians.

### 7.3.1 Military/Civilian Blurring

The analysis illustrates that both the EU and NATO rely on private sector actors not merely as followers of regulations or as defence contractors, but as partners in this field. The private sector is being incorporated into a security role out of necessity for its expertise, but the space it take up in cyberspace blur the lines between military and civilian. This grey area that exists between what has traditionally been perceived as the role of public actors versus private actors creates a liminal security environment. Åsne Kalland Aarstad states that this can be both a challenge and an opportunity, as "being unseen can both expand and contract an actor room for maneuver" (Å. K. Aarstad, 2016, p. 57). This can be seen from analyzing the documents which do not give insight into how these partnerships work. Aside from reference to the importance of cooperation and the general demand for further collaboration, the documents do not outline the exact role of the private sector which helps create this space for maneuvering depending on the issue faced.

The implications of this blurring of the line between private and public actors within cybersecurity reinforces the hybridity argument made by Anna Leander, in which she argues that "security can remain seen *and* unseen precisely because of its hybridity and that hybridity is core to the normalization, expansion and grip of hybrid security of the politics of security" (Leander, 2016, p. 143). This has led to the "hybrid security" of cyberspace in which its power derives from being elusive, seen and unseen, and therefore difficult to capture and resist. The analysis on both EU and NATO discourse, that the role of the private sector has increasingly become more

important and a critical part of ensuring cybersecurity, as Benjamin Farrand and Helena Carrapico (2018) reinforce, shows this growing role of the private sector, stating that "the private sector may not serve only to steer the ship; instead, it may determine its ultimate destination" (Carrapico & Farrand, 2018, p. 214). While this thesis does not aim to position itself as arguing for or against this blurring, it seeks to point to the area and critically examine the process. Throughout the analysis, what is clear is that both the EU and NATO are aware of their inability to maneuver this space alone, unlike the traditional security domain in which NATO can claim to be one of the key actors. Neither the EU nor NATO are key actors in cyberspace. Therefore, cooperation with each other is one of the ways in which they can combine their approaches and conceptualizations to build a better-rounded alliance that can tackle this space from multiple sides. As such, this blurring between military and civilian with regards to the EU and NATO private partnerships is due to both the EU's and NATO's inability to ensure cybersecurity on their own. This raises an important distinction between cyberspace and other domains and speaks to the larger question on the responsibility of the state. How safe and secure can EU and NATO citizens, networks, and infrastructure be if these institutions or even individual states are unable to guarantee their citizens full protection? As technology evolves, will this be a trend that continues forward with regards to securing new domains and technologies? If cyberspace is any indication of future domains and technologies, then we will continuously see the blurring of lines between civilian and military as the public actors, as analyzed in this thesis, a military alliance and a supranational and intergovernmental actor, will not be equipped to secure the security of their citizens in the face of emerging threats.

### 7.3.2 Militarizing Society

In the case of the EU discourse, the analysis illustrates that their framework on how to secure cyberspace is seen as a collective responsibility – which includes EU citizens. This move to blur the lines between military actors and civilian actors in cyberspace moves to militarize society with little critical attention being paid to this movement. As argued earlier, this is due to the liminal security environment cyberspace and cybersecurity presents. This has been illustrated in the analysis through the EU's emphasis on citizen engagement in cybersecurity, for example through ENISA's "European Cybersecurity Month". This responsibly that is allocated to the citizenry to be part of security practices and protection is part of the blurring of lines between military and civilians. As discussed in the theory chapter of this thesis, critical military studies

problematize the idea that a clear line can be drawn between what is military and civilian. This grey area that is especially evident in cybersecurity illustrates that civilians are expected to participate in protection. There are protection measures that individuals must take on land, air and sea. There they must follow protocol, such as wearing seat belts, being aware of safe exit points on airplanes, and wear life jackets. These protocols that are normally used on land, air and sea are framed to protect in case of accidents. However, with the cyber domain, the EU discourse is imposing a responsibility on its citizens to train in order to secure this domain against not only cyber accidents but cyber attacks. As previously mentioned, the EU discourse states that these threats can come from state, non-state, and state sponsored attacks. This is the major difference between the civilian/military divide in the cyber domain as opposed to traditional domains. The EU expects citizens to participate in what has traditionally been the role of the military – to protect against foreign threats. This is an important area that requires further research because, as Wibben explains, security is a practice that is "enacted in the everyday", and that "taking the everyday seriously" is vital, because it is within that space that the effects of security practices are felt (Salter et al., 2019, p. 12). These "everyday" cybersecurity practices need to be studied to fully comprehend the level of impact incorporating the public into the cybersecurity framework effects societies' conceptualization of cyberspace, cybersecurity and their role as security actors.

# 8. Findings and Conclusions

The aim of this thesis has been to answer how can we understand EU-NATO cooperation in cyberspace with regards to cybersecurity and defence? Through a critical theoretical framework composed of CSS, CMS, and STS, and careful discourse analysis, this thesis has illustrated that their cooperation goes beyond convenience. Furthermore, it has made clear the importance of critically engaging with international relations in cyberspace, and the need to ensure that the nature of the technologies that we study are incorporated into a political context.

## 8.1 Findings

The EU and NATO have diverging conceptualizations of cyberspace and security within this domain, and as such their practices vary. However, this is precisely one of the reasons why they cooperate. Through these diverging conceptualizations, both the EU and NATO can take advantage of their counterpart's role in this space. NATO is able to gain a political and diplomatic actor that can aid in cyber conflict de-escalation and deterrence through sanctions, and the EU is able to partner with a military alliance in cyberspace, and as such blur the lines between civilian and military goals, giving them room to maneuver security and defence areas that would otherwise go beyond their historic role. Thus, these diverging conceptualizations of cybersecurity and cyberspace present this partnership with the opportunity to benefit and participate in the parameters of their counterpart.

Through the discourse analysis it is evident that, unlike in the physical domain, neither the EU nor NATO are main actors in cyberspace – that role belongs to the private sector. This was illustrated in the discourse analysis with the emphasis on the need for private partnerships to ensure the security and defence of networks and citizens. This reliance on the private sector, and the minimal role each actor plays individually within this domain, provides further reasoning as to why the two organizations cooperate; they do so in order to combine their own individual forms of power to create a stronger alliance that can engage in this domain through various dimensions, but also with unique practices and perceptions.

Finally, cyberspace is presently in the process of establishing norms and order. As such, there are competing interests and visions for what this space ought to be, much like in the physical world. Through the values and norms that are exported into cyberspace, and the ideas of security presented in EU and NATO discourse, it is evident that both actors are prominent proponents of a

liberal order. As such, their cooperation in cyberspace and cybersecurity is one that reinforces a liberal order in this domain. While both the EU and NATO focus on this to varying degrees, they share this vision and thus their cooperation is an extension of liberal values.

### 8.2 Self- Reflection

This thesis has engaged with ideas of security, and as academics, our work helps shape what these ideas are. We are not separate from our analysis of the subject matter. Therefore, this presents us with an added layer of responsibility as we examine cyberspace and the various complexities it presents to security and defence. This is especially the case when it comes to security within cyberspace as an evolving domain that changes based on external actions. As discussed throughout this thesis, academic contributions, such as this thesis, can act as input on how this space is conceptualized and acted within. I critically engaged with these concepts, aiming to question the presumptions of how this domain is represented within EU and NATO discourse. However, in the process it is possible that my own work could contribute to these ideas in ways that could potentially exclude groups or ideas that I was unaware of. Therefore, I urge the reader to critically engage with the parameters created and ideas presented.

# Bibliography


Aarstad, A. K. (2015). Critical Approaches to European Foreign Policy. In *The SAGE Handbook of European Foreign Policy: Two Volume Set* (Vol. 1–2, pp. 121–136). SAGE Publications Ltd. https://doi.org/10.4135/9781473915190

Aarstad, Å. K. (2016). *Public/Private, Global/Local, and Land/Sea: International Relations and the Study of In-Betweenness*. Forlaget Politica and the Author.

Angelov, I. (2019). The Security Environment and the Challenges to the European Union and NATO in the field of Security. *Security & Future*, *3*(1), 17–21.

Bachmann, V. (2013). The EU's civilian/power dilemma. *Comparative European Politics*, *11*(4), 458–480.

Barnard-Wills, D., & Ashenden, D. (2012). Securing Virtual Space: Cyber War, Cyber Terror, and Risk. *Space and Culture*, *15*(2), 110–123. https://doi.org/10.1177/1206331211430016

Barnes, B. (2001). Practice as a Collective Action. In *The Practice Turn in Contemporary Theory* (pp. 19–27). Routledge.

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: The making of an international society in the digital age. *Global Affairs*, *3*(4–5), 353–364. https://doi.org/10.1080/23340460.2017.1414924

Barrinha, A., & Renard, T. (2020). Power and diplomacy in the post-liberal cyberspace. *International Affairs*, iiz274. https://doi.org/10.1093/ia/iiz274

Basham, V. M., Belkin, A., & Gifkins, J. (2015). What is Critical Military Studies? *Critical Military Studies, 1*(1), 1–2. https://doi.org/10.1080/23337486.2015.1006879

Betz, D. (2012). Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed: Journal of Strategic Studies: Vol 35, No 5. *Journal of Strategic Studies*, *35*(5), 689–711.

Betz, D., & Stevens, T. (n.d.). Power and cyberspace. *Adelphi Series*.

Bijker, W. E. (2006). Why and How Technology Matters. *The Oxford Handbook of Contextual Political Analysis*. https://doi.org/10.1093/oxfordhb/9780199270439.003.0037

Binder, C. (2016). Science, Technology and Security: Discovering intersections between STS and security studies. *EASST*. https://easst.net/article/science-technology-and-security-discovering-intersections-between-sts-and-security-studies/

Boyle, J. (1997). Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors Corporate Law Symposium: Intellectual Property Law for the Twenty-First Century. *University of Cincinnati Law Review*, *66*(1), 177–206.

Browning, C. S., & McDonald, M. (2013). The future of critical security studies: Ethics and the politics of security. *European Journal of International Relations*, *19*(2), 235–255. https://doi.org/10.1177/1354066111419538

Burnes, O. (2018). Contributions of Private Businesses to the Provision of Security in the EU: Beyond Public-Private Partnerships. In *Security Privatization: How Non-security-related Private Businesses Shape Security Governance* (pp. 23–50). Springer International Publishing.

Buzan, B. (1991). New Patterns of Global Security in the Twenty-First Century. *International Affairs (Royal Institute of International Affairs 1944-)*, *67*(3), 431–451. JSTOR. https://doi.org/10.2307/2621945

Camporini, V., Hartley, K., Maulny, J.-P., & Zandee, D. (2017). European Preference, Strategic Autonomy and European Defence Fund. *Armament Industry European Research Group, 22*.

Carr, M. (2015). Power Plays in Global Internet Governance. *Millennium*, *43*(2), 640–659. https://doi.org/10.1177/0305829814562655

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62. https://doi.org/10.1111/1468-2346.12504

Carrapico, H., & Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor? *JCMS: Journal of Common Market Studies*, *55*(6), 1254–1272. https://doi.org/10.1111/jcms.12575

Carrapico, H., & Farrand, B. (2018). Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism. In *Security Privatization: How Non-security-related Private Businesses Shape Security Governance* (pp. 197–217). Springer International Publishing.

Cavelty, M. D. (2018). Cybersecurity Research Meets Science and Technology Studies. *Politics and Governance*, *6*(2), 22–30. https://doi.org/10.17645/pag.v6i2.1385

Chaban, N., Elgstrom, O., & Holland, M. (2006). European Union as Others See It, The. *European Foreign Affairs Review*, *11*(2), 245–262.

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

Commission, E. (2017). *Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises*. Official Journal of the European Union.

Conway, M. (2008). Media, fear and the hyperreal: The construction of cyberterrorism as the ultimate threat to critical infrastructures. In *Securing 'the homeland': Critical infrastructure, risk and (in)security* (pp. 109–129). Routledge.

Council of the European Union. (2017). *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")—Adoption*. Consilium.

Council, G. S. of the. (2018). *Council Conclusions on malicious cyber activities*. Official Journal of the European Union.

Cox, R. (1981). *Social Forces, States and World Orders: Beyond International Relations Theory—Robert W. Cox, 1981*. https://journals-sagepub-com.ezproxy.uio.no/doi/abs/10.1177/03058298810100020501

Deibert, R. J., & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, *4*(1), 15–32. https://doi.org/10.1111/j.1749-5687.2009.00088.x

Demchak, C. C., & Dombrowski, P. (2011). Rise of a Cybered Westphalian Age. *Strategic Studies Quarterly*, *5*(1), 32–61. JSTOR.

Ducheine, P. (2016). Cyber warfare is taking place! *International Spectator*, *70*(6), 13.

Duke, S. (2008). The Future of EU–NATO Relations: A Case of Mutual Irrelevance Through Competition? *Journal of European Integration*, *30*(1), 27–43. https://doi.org/10.1080/07036330801959457

Duke, S. (2017). Europe's Harder Edges: Security and Defence | SpringerLink. In *Europe as a Stronger Global Actor*. Palgrave Macmillan. https://link-springer-com.ezproxy.uio.no/chapter/10.1057/978-1-349-94945-8_8

Dunn Cavelty, M. (2008). *Cyber-Security and Threat Politics: US efforts to secure the information age*. Routledge.

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, *15*(1), 105–122. https://doi.org/10.1111/misr.12023

Dunn Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701–715. https://doi.org/10.1007/s11948-014-9551-y

Dunn Cavelty, M. (2012). The militarisation of cyberspace: Why less may be better. *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1–13.

Dunn, K. C., & Neumann, I. B. (2016). *Undertaking Discourse Analysis for Social Research*. University of Michigan Press.

Ehrhart, H.-G. (2017). Postmodern warfare and the blurred boundaries between war and peace. *Defense & Security Analysis*, *33*(3), 263–275. https://doi.org/10.1080/14751798.2017.1351156

ENISA. (2013). *What is ECSM? —ECSM*. European Cyber Security Month. https://cybersecuritymonth.eu/about-ecsm/whats-ecsm

EU High Representative for Foreign Affairs and Security Policy. (2016). *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the EU's Foreign and Security Policy*.

European Commission. (2010). *Europe 2020: A strategy for smart, sustainable and inclusive growth*. European Commission.

European Commission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. European Commission.

European Commission. (2014). *Internet Policy and Governance Europe's Role in Shaping the Future of Internet Governance*. Official Journal of the European Union.

European Commission. (2015). *'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Agenda on Security*.

European Council. (2008). *Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime*. European Union.

European Council. (2019a). *Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States*. EUR-Lex.

European Council. (2019b). *Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace*. http://www.consilium.europa.eu/en/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/

European External Action Service. (2017). *Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy*. EU Publications.

European Parliament. (2019). *EU Cybersecurity Act*. Official Journal of the European Union.

European Parliament and of the Council. (2004). *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance)*. EUR-Lex.

European Parliament, & The Council. (2016). *Directive (EU) 2016/1148*. EUR-Lex. http://data.europa.eu/eli/dir/2016/1148/oj/eng

European Union External Action. (2008). *About EULEX - EULEX - European Union Rule of Law Mission in Kosovo*. https://www.eulex-kosovo.eu/?page=2,60

Fahey, E. (2014). The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security. *European Journal of Risk Regulation (EJRR)*, *5*(1), 46–60.

Fairclough, N. (2003). *Analysing Discourse: Textual analysis for social research*. Routledge.

Felt, U., Beck, S., Fouché, R., Miller, C. A., Smith-Doerr, L., Alac, M., Amir, S., Arribas-Ayllon, M., Balmer, B., & Barandiarán, J. (2016). *The Handbook of Science and Technology Studies*. MIT Press. http://ebookcentral.proquest.com/lib/oslo/detail.action?docID=5052910

Fiott, D. (2018). Strategic autonomy: Towards 'European sovereignty' in defence? *European Union Institute for Security Studies (EUISS)*, *12*, 1–8.

Fjærtoft, D., & Øverland, I. (2015). Financial Sanctions Impact Russian Oil, Equipment Export Ban's Effects Limited. *Oil & Gas Journal*, *113*(8), 66–72.

Fliegauf, M. T. (2016). In Cyber (Governance) We Trust. *Global Policy*, *7*(1), 79–82. https://doi.org/10.1111/1758-5899.12310

Flockhart, T. (2011). 'Me Tarzan – You Jane': The EU and NATO and the Reversal of Roles. *Perspectives on European Politics and Society*, *12*(3), 263–282. https://doi.org/10.1080/15705854.2011.596306

Fouché, R. (2016). Sociotechnological (Re-)configurations. In *The Handbook of Science and Technology Studies* (4th ed.).

Franzese, P. W. (2009). Sovereignty in Cyberspace: Can It Exist  Cyberlaw Edition. *Air Force Law Review*, *64*(1), 1–42.

Gill, R. (1996). Discourse analysis: Practical implementation. In *Handbook of Qualitative Research for Psychology and Methods for Social Sciences* (pp. 141–156).

Gill, R. (2000). Discourse Analysis. In M. Bauer & G. Gaskell (Eds.), *Qualitative Researching with Text, Image and Sound* (pp. 173–190). SAGE Publications Ltd. https://doi.org/10.4135/9781849209731.n10

Græger, N. (2017). Grasping the everyday and extraordinary in EU–NATO relations: The added value of practice approaches. *European Security*, *26*(3), 340–358. https://doi.org/10.1080/09662839.2017.1355304

Gray, C. S. (2013). *Making strategic sense of cyber power: Why the sky is not falling*. Strategic Studies Institute and U.S. Army War College Press.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175. JSTOR.

Howorth, J. (2005). The Euro-Atlantic Security Dilemma: France, Britain, and the ESDP. *Journal of Transatlantic Studies*, *3*(1), 39–54. https://doi.org/10.1080/14794010508656816

Howorth, J. (2017). EU–NATO cooperation: The key to Europe's security future. *European Security*, *26*(3), 454–459. https://doi.org/10.1080/09662839.2017.1352584

Howorth, J. (2018). Strategic autonomy and EU-NATO cooperation: Threat or opportunity for transatlantic defence relations? *Journal of European Integration*, *40*(5), 523–537. https://doi.org/10.1080/07036337.2018.1512268

Howorth, J. (2019). Strategic Autonomy and EU-NATO Cooperation: A Win-Win Approach. *L'Europe En Formation*, *389*(2), 85–103.

Jasanoff, S. (2004a). Ordering knowledge, ordering society. In *States of Knowledge: The co-production of science and social order* (pp. 13–45). Routledge.

Jasanoff, S. (2004b). The idiom of co-production. In *States of Knowledge: The co-production of science and social order* (pp. 1–12). Routledge.

Jørgensen, M., & Phillips, L. (2002). *Discourse Analysis as Theory and Method*. SAGE Publications Ltd. https://doi.org/10.4135/9781849208871

Joyner, C. C., & Lotrionte, C. (2001). Information Warfare as International Coercion: Elements of a Legal Framework. *European Journal of International Law*, *12*(5), 825–865. https://doi.org/10.1093/ejil/12.5.825

King, G., Keohane, R. O., & Verba, S. (1993). *Designing Social Inquiry: Scientific Inferences in Qualitative Research*. Princeton University Press.

Kostyuk, N., & Zhukov, Y. M. (2019). Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? *Journal of Conflict Resolution*, *63*(2), 317–347. https://doi.org/10.1177/0022002717737138

Kovács, L. (2018). Cyber Security Policy and Strategy in the European Union and Nato. *Land Forces Academy Review*, *23*(1). https://doi.org/10.2478/raft-2018-0002

Kvale, S. (2007). *Doing Interviews* (U. Flick, Ed.). SAGE Publications.

Lacroix, J., & Nicolaïdis, K. (2003). Order and Justice Beyond the Nation-State: Europe's Competing Paradigms. In R. Foot, J. L. Gaddis, & A. Hurrell (Eds.), *Order and Justice in International Relations* (pp. 125–154). Oxford University Press.

Law, J. (2016). STS as Method. In *The Handbook of Science and Technology Studies* (4th ed.).

Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics*, *10*(1), 86–103. https://doi.org/10.1080/19331681.2012.759059

Leander, A. (2016). Seen and unseen: Hybrid rule in international security. In *Hybrid Rule and State Formation: Public-Privte Power in the 21st Century* (pp. 143–159). Routledge.

Lété, B. (2017). Cooperation in cyberspace. In *The EU and NATO: The essential partners*. EU Institute for Security Studies.

Lété, B., & Pernik, P. (2017). *EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions*. 9.

Libicki, M. C. (2009). Operational Cyberwar. In *Operational Cyberwar from Cyberdeterrence and Cyberwar* (pp. 139–158). RAND Corporation. https://www-jstor-org.ezproxy.uio.no/stable/10.7249/mg877af.15?refreqid=excelsior%3A3f7738b16eba8ee9bc504066600935e6&seq=1#metadata_info_tab_contents

Libicki, M. C. (2011). The Strategic Uses of Ambiguity in Cyberspace. *Military and Strategic Affairs*, *3*(3), 8.

Lisle, D. (2016). Waiting for International Political Sociology: A Field Guide to Living In-Between. *International Political Sociology*, *10*(4), 417–433. https://doi.org/10.1093/ips/olw023

Lucarelli, S. (2007). European Union in the Eyes of Others: Towards Filling a Gap in the Literature, The. *European Foreign Affairs Review*, *12*(3), 249–270.

Lucarelli, S., & Fioramonti, L. (2010). *External Perceptions of the European Union as a Global Actor*. Routledge.

Lucas Jr, G. R. (2010). Postmodern War. *Journal of Military Ethics*, *9*(4), 289–298. https://doi.org/10.1080/15027570.2010.536399

Manners, I. (2002). Normative Power Europe: A Contradiction in Terms? *JCMS: Journal of Common Market Studies*, *40*(2), 235–258. https://doi.org/10.1111/1468-5965.00353

Martins, B. O. (2011). The EU, the Mirror and 'the Others.' *Journal of European Integration*, *33*(3), 341–347. https://doi.org/10.1080/07036337.2011.558702

Martins, B. O., & Küsters, C. (2019). Hidden Security: EU Public Research Funds and the Development of European Drones. *JCMS: Journal of Common Market Studies*, *57*(2), 278–297. https://doi.org/10.1111/jcms.12787

Mattice, L. (2014). Taming the "21st Century's Wild West" of Cyberspace? In *Conflict and Cooperation in Cyberspace: The Challenge to National Security* (pp. 9–12). Taylor & Francis.

McCarthy, D. R. (2018). Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order. *Politics and Governance*, *6*(2), 5–12. https://doi.org/10.17645/pag.v6i2.1335

McConnell, M. (2009). Cyberwar Is the New Atomic Age. *New Perspectives Quarterly*, *26*(3), 72–77. https://doi.org/10.1111/j.1540-5842.2009.01103.x

Mehmetcik, H. (2014). A New Way of Conducting War: Cyberwar, Is That Real? In J.-F. Kremer & B. Müller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 125–139). Springer. https://doi.org/10.1007/978-3-642-37481-4_8

Mihr, A. (2014). Good Cyber Governance: The Human Rights and Multi-Stakeholder Approach. *Georgetown Journal of International Affairs*, 24–34. JSTOR.

Milliken, J. (1999). The Study of Discourse in International Relations: A Critique of Research and Methods. *European Journal of International Relations*, *5*(2), 225–254. https://doi.org/10.1177/1354066199005002003

Mutlu, C. E., & Salter, M. B. (2013). The discursive turn. In *Research Methods in Critical Security Studies: An Introduction*. Routledge.

NATO. (1949). *The North Atlantic Treaty*.

NATO. (2002). *Prague Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Cou...* http://www.nato.int/cps/en/natohq/official_texts_19552.htm

NATO. (2006). *Riga Summit Declaration—Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga on 29 November 2006*. http://www.nato.int/cps/en/natohq/official_texts_37920.htm

NATO. (2008). *Bucharest Summit Declaration—Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008*. http://www.nato.int/cps/en/natohq/official_texts_8443.htm

NATO. (2010a). *Lisbon Summit Declaration*.

NATO. (2010b). *Strategic Concept 2010: Active Engagemen, Modern Defence*. http://www.nato.int/cps/en/natohq/topics_82705.htm

NATO. (2014a). NICP |. Retrieved November 20, 2019, from https://nicp.nato.int/

NATO. (2014b). *Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*. http://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO. (2016a). *Cyber Defence Pledge*. NATO. http://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO. (2016b). *Warsaw Summit Communiqué—Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016*. http://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO. (2018). *Brussels Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, 11-12 July 2018*. http://www.nato.int/cps/en/natohq/official_texts_156624.htm

NATO. (2019). *NATO will defend itself (Article by NATO Secretary General Jens Stoltenberg published in Prospect)*. NATO. http://www.nato.int/cps/en/natohq/news_168435.htm

NATO, European Council, & European Commission. (2016). *Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*. http://www.nato.int/cps/en/natohq/official_texts_138829.htm

NATO, & European Union. (2016). *Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*. http://www.nato.int/cps/en/natohq/official_texts_133163.htm

NATO, & European Union. (2017). *Common set of new proposals on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization*. http://www.nato.int/cps/en/natohq/official_texts_149522.htm

NATO, & European Union. (2018). *Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*. http://www.nato.int/cps/en/natohq/official_texts_156626.htm

Neumann, I. B. (2008). Discourse Analysis. In A. Klotz & D. Prakash (Eds.), *Qualitative Methods in International Relations: A Pluralist Guide* (pp. 61–77). Palgrave Macmillan.

Nye, J. (2010). *Cyber Power*. https://apps.dtic.mil/docs/citations/ADA522626

Nye, J. S. (2011). Nuclear Lessons for Cyber Security? On JSTOR. *Strategic Studies Quarterly*, *5*(4), 21.

Ojanen, H. (2006). The EU and Nato: Two Competing Models for a Common Defence Policy. *JCMS: Journal of Common Market Studies*, *44*(1), 57–76. https://doi.org/10.1111/j.1468-5965.2006.00614.x

Pace, M. (2007). The Construction of EU Normative Power*. *JCMS: Journal of Common Market Studies*, *45*(5), 1041–1064. https://doi.org/10.1111/j.1468-5965.2007.00759.x

Peoples, C., & Vaughan-Williams, N. (2014). *Critical Security Studies: An Introduction*. Routledge.

Pernik, P. (2014). Improving Cyber Security: NATO and the EU. *International Centre for Defence Studies*, 20.

Petr Hruza, & Cerny, J. (2017). Cyberwarfare. *International Conference KNOWLEDGE-BASED ORGANIZATION*, *23*(1), 155–160. https://doi.org/10.1515/kbo-2017-0024

Posen, B. R. (2004). ESDP and the structure of world power. *The International Spectator*, *39*(1), 5–17. https://doi.org/10.1080/03932720408457057

Potter, J. (1996). Discourse analysis and constructionist approaches: Theoretical background. In J. T. E. Richardson (Ed.), *Handbook of Qualitative Research Methods for Psychology and the Social Sciences* (pp. 125–156).

Potter, J., & Wetherell, M. (1987). *Discourse and Social Psychology: Beyond attitudes and behaviour*. SAGE Publications.

Rasmussen, A. F. (2012). *The Secretary General's Annual Report 2011* (pp. 1–17). NATO.

Rid, T. (2012a). Think Again: Cyberwar. *Foreign Policy*, *192*, 80–84.

Rid, T. (2012b). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Rugge, F. (2012). The case for NATO-EU cooperation in the protection of cyberspace. *2012 Third Worldwide Cybersecurity Summit (WCS)*, 1–10. https://doi.org/10.1109/WCS.2012.6780880

Rupp, V. (2019). *Fall in Line or Fall Behind? : Cooperation in cyberspace between the North Atlantic Treaty Organisation and the European Union.* http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-8357

Salter, M. B., Cohn, C., Neal, A. W., Wibben, A. T., Burgess, J. P., Elbe, S., Austin, J. L., Huysmans, J., Walker, R., Wæver, O., Williams, M. C., Gilbert, E., Frowd, P. M., Rosenow, D., Oliveira Martins, B., Jabri, V., Aradau, C., Leander, A., Bousquet, A., … Hansen, L. (2019). Horizon Scan: Critical security studies for the next 50 years. *Security Dialogue*, *50*(4_suppl), 9–37. https://doi.org/10.1177/0967010619862912

Schmitt, M. (2014). The law of cyber warfare: Quo vadis? - UiO : Universitetsbiblioteket. *Stanford Law & Policy  Review*, *25*(2), 269–300.

Schmitt, M. (2017). Sovereignty. In *Tallinn Manual 2,0 on the International Law Applicable to Cyber Operations* (2nd ed.). Cambridge University Press. http://doi.org.ezproxy.uio.no/10.1017/9781316822524.007

Shepherd, L. (2008). *Gender, violence and security: Discourse as practice*. Zed Books.

Simion, E. (2018). Nato-Eu Cooperation. *International Conference KNOWLEDGE-BASED ORGANIZATION*, *24*(1), 211–214. https://doi.org/10.1515/kbo-2018-0031

Siroli, G. P. (2018). Considerations on the Cyber Domain as the New Worldwide Battlefield. *The International Spectator*, *53*(2), 111–123. https://doi.org/10.1080/03932729.2018.1453583

Smith, H. (2019). Countering Hybrid Threats. In *The EU and NATO: The essential partners*. EU Institute for Security Studies.

Smith, K. E. (2005). Beyond the civilian power EU debate. *Politique Europeenne*, *n° 17*(3), 63–82.

Smith, S. J. (2011). EU–NATO cooperation: A case of institutional fatigue? *European Security*, *20*(2), 243–264. https://doi.org/10.1080/09662839.2011.557771

Stavrianakis, A., & Stern, M. (2017). Militarism and security: Dialogue, possibilities and limits: *Security Dialogue*. https://doi.org/10.1177/0967010617748528

Stevens, T. (2018). Global Cybersecurity: New Directions in Theory and Methods. *Politics and Governance*, *6*(2), 1–4. https://doi.org/10.17645/pag.v6i2.1569

Štitilis, D., Pakutinskas, P., & Malinauskaitė, I. (2016). EU and NATO cybersecurity strategies and national cyber security strategies: A comparative analysis. *Security Journal*, *30*. https://doi.org/10.1057/s41284-016-0083-9

Stoltenberg, J. (2016). *The Secretary General's Annual Report 2015* (pp. 1–124). NATO.

Stoltenberg, J. (2017). *The Secretary General's Annual Report 2016*. NATO.

Stoltenberg, J. (2018a). *Doorstep statement by NATO Secretary General Jens Stoltenberg prior to the European Union Foreign Affairs Council meeting*. NATO. http://www.nato.int/cps/en/natohq/opinions_160495.htm

Stoltenberg, J. (2018b). *The Secretary General's Annual Report 2017* (pp. 1–117). NATO.

Stoltenberg, J. (2019). *The Secretary General's Annual Report 2018* (pp. 1–132). NATO.

Stoltenberg, J. (2020). *The Secretary General's Annual Report 2019* (pp. 1–128). NATO.

Stone, J. (2013). Cyber War Will Take Place! *Journal of Strategic Studies*, *36*(1), 101–108. https://doi.org/10.1080/01402390.2012.730485

Swidler, A. (2005). What anchors cultural practices. In T. R. Schatzki, E. von Savigny, T. R. Schatzki, E. von Savigny, & K. K. Cetina (Eds.), *The Practice Turn in Contemporary Theory* (pp. 83–101). Routledge. https://doi.org/10.4324/9780203977453

Szewczyk, B. (2019). Operational cooperation. In *The EU and NATO: The essential partners*.

Tardy, T., & Lindstrom, G. (2019). The scope of EU- NATO cooperation. In *The EU and NATO: The Essential Partners*. EU Institute for Security Studies.

Taylor, S. (2001). Locating and Conducting Discourse Analytic Research. In *Discourse as Data: A Guide for Analysis*. Sage.

The Council. (2009). *European Security Strategy: A Secure Europe in a Better World*. European Communities.

The Council. (2020). *Shaping Europe's Digital Future- Council Conclusions*.

The Council, & European Parliament. (2019). *Regulation (EU) 2019/881*. Eur-Lex.

Toren, C. (1996). Ethnography: Theoretical background. In *The Handbook of Qualitative Research for Psychology and the Social Sciences* (pp. 102–112).

Touzovskaia, N. (2006). EU-NATO Relations: How Close to “Strategic Partnership”? *European Security*, *15*, 235–258.

Tracy, K. (1995). Action-Implicative Discourse Analysis. *Journal of Language and Social Psychology*, *14*(1–2), 195–215. https://doi.org/10.1177/0261927X95141011

Vogel, K. M., Balmer, B., Evans, S. W., Kroener, I., Matsumoto, M., & Rappert, B. (2016). Knowledge and Security. In *The Handbook of Science and Technology Studies* (4th ed.).

Warf, B. (2015). Cyberwar: A new frontier for political geography. *Political Geography*, *46*, 89–90. https://doi.org/10.1016/j.polgeo.2014.07.010

Yoran, A. (2010). *Cyberwar Or Not Cyberwar? And Why That Is The Question*. Forbes. https://www.forbes.com/sites/firewall/2010/03/25/cyberwar-or-not-cyberwar-and-why-that-is-the-question/#237a63ce269a

# Appendix

## Appendix I: Data Overview

### Overview of Data

| Institution | Year | Type | Title |
|---|---|---|---|
| NATO | 2002 | Summit Declaration | Prague Summit |
| NATO | 2006 | Summit Declaration | Riga Summit |
| NATO | 2008 | Summit Declaration | Bucharest Summit Declaration |
| NATO | 2010 | Strategic Concept/ Policy | Active Engagement, Modern Defence |
| NATO | 2010 | Summit Declaration | Lisbon Summit Declaration |
| NATO | 2012 | Summit Declaration | Chicago Summit Declaration |
| NATO | 2012 | Report | The Secretary General's Annual Report 2011 |
| NATO | 2013 | Report | The Secretary General's Annual Report 2012 |
| NATO | 2014 | Report | The Secretary General's Annual Report 2013 |
| NATO | 2014 | Summit Declaration/ Policy | NATO Cyber Defence Policy – NATO Summit in Wales |
| NATO | 2016 | Report | The Secretary General's Annual Report 2015 |
| NATO | 2016 | Summit | Warsaw Summit |
| NATO | 2016 | Pledge | Cyber Defence Pledge |
| NATO | 2017 | Report | The Secretary General's Annual Report 2016 |
| NATO | 2018 | Report | The Secretary General's Annual Report 2017 |
| NATO | 2018 | Summit Declaration | Brussels Summit Declaration |

| | | | |
|---|---|---|---|
| NATO | 2019 | Report | The Secretary General's Report 2018 |
| NATO | 2020 | Report | The Secretary General's Report 2019 |
| EU | 2004 | Regulation | Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance) |
| EU | 2004 | Website | European Agency for Cybersecurity (ENISA) "about us" |
| EU | 2008 | Council Conclusion | Council conclusions on a concerted work strategy and practical measures against cybercrime |
| EU | 2008 | Speech | Vice President Jacques Barrot Speech |
| EU | 2010 | Agenda | A Digital Agenda for Europe |
| EU | 2010 | Strategy | Europe 2020: A strategy for smart, sustainable and inclusive growth |
| EU | 2013 | Strategy | Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace |
| EU | 2014 | Policy | Internet Policy and Governance Europe's Role in Shaping the Future of Internet Governance |
| EU | 2014 | Campaign | European Cyber Security Month |
| EU | 2015 | Council Conclusion | Council Conclusions on Cyber Diplomacy |
| EU | 2016 | Directive | The Directive on Security of network and information systems (NIS Directive) Shaping Europe's digital future |
| EU | 2016 | Strategy | Shared Vision, Common Action: A Stronger Europe- A Global Strategy for the European Union's Foreign and Security Policy |
| EU | 2017 | Draft Implementation | Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - approval of the final text |

| | | | |
|---|---|---|---|
| EU | 2017 | Draft Conclusion | Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") - Adoption |
| EU | 2017 | Recommendation | Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises |
| EU | 2019 | Act | EU Cybersecurity Act |
| EU | 2019 | Council Decision | COUNCIL DECISION concerning restrictive measures against cyber-attacks threatening the Union or its Member States |
| EU | 2019 | Public Announcement | Cyber- attacks: Council is now able to impose sanctions |
| EU | 2019 | Framework | The EU cybersecurity certification framework/ Shaping Europe's digital future |
| EU | 2020 | Council Conclusion | Draft Council Conclusions on Shaping Europe's Digital Future |
| EU-NATO | 2016 | Joint Declaration | Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization |
| EU-NATO | 2016 | Statement | Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization |
| EU-NATO | 2017 | Proposal | Common set of new proposals on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization |
| EU-NATO | 2018 | Joint Declaration | Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization |

## Appendix II: Interviews

Interview 1: James Shires, Assistant Professor at the Institute for Security and Global Affairs, Leiden University, Associate Fellow with The Hague Program for Cyber Norms and a non-resident research fellow with the Cyber Project at the Belfer Center for Science and International Affairs, Harvard Kennedy School, working on issues relating to cybersecurity, governance, international relations and security (Teams 27/05/20)

Interview 2: Paul Timmers, Senior advisor at the European Policy Centre in Brussels and former Director of Digital Society, Trust, and Cybersecurity at the European Commission (EC), working on issues digital technologies, digital policy, European public policy (WhatsApp 10/06/20)

Interview 3: Louise Marie Hurel S. Dias, PhD Researcher at the Department of Media and Communication, London School of Economics, working on knowledge production, cybersecurity expertise and incident response (Teams 18, 06/20)

Interview 4: Åsne Kalland Aarstad, PhD in political science, with a thesis on international relations and the study of in-betweenness with expertise in public/private, global/local, and land/sea boundaries (Zoom 26/06/20)

## Appendix III: Consent/Information Form

### Are you interested in taking part in the research project "Brave New World: NATO, the EU and the New Age of Cyberspace"?

This is an inquiry about participation in a research project (MA thesis) where the main purpose is to analyze the security and defence dimensions of cyberspace and how EU and NATO are cooperating in this space to ensure a safe and collaborative environment. In this letter we will give you information about the purpose of the project and what your participation will involve.

### Purpose of the project

The purpose of this master's thesis project is to analyze the security and defence components of cyberspace and how EU and NATO are cooperating in this new domain. There is currently a major gap in academia in critically analyzing the cyber domain and EU-NATO relations within this new space. The research project seeks to answer "why are NATO and the EU cooperating in their response to cyber threats?" additionally, it asks "how are NATO and EU cooperating in their response to cyber threats" and "how has the threat of cyberattacks/ the arms race within cyber domain intensified the cooperation between the EU and NATO"?

### Who is responsible for the research project?

This project is part of a master's thesis conducted by Neven Ahmad at the University of Oslo. Additionally, this project has had the rare opportunity of collaborating with the Peace Research Institute Oslo (PRIO), as PRIO helps provide invaluable resources. Additionally, the thesis supervisor, Bruno Oliveira Martins, is a Senior Researcher with PRIO.

### Why are you being asked to participate?

You have been asked to participate due to your insight on either EU-NATO cooperation/relations or/and your expertise on cyberspace security and defence.

### What does participation involve for you?

If you chose to take part in the project, this will involve an hour semi-formal interview. The interview will ask questions along the lines of:

• In your expert opinion, how has the emergence of the cyber domain impacted EU-NATO relations?

• Why are the EU and NATO cooperating in their efforts in cyberspace, specifically in regard to security and defence?

• In your opinion, how do NATO and the EU conceptualize this new space and its securitization?
• Do you believe EU-NATO cooperation in this domain differ than those in traditional domains such as land and sea? If so, how?

• Is the cyber domain blurring the lines between the military sphere and the civilian sphere?

• What are some challenges that NATO and EU cooperation and relation face in relation to the dual-use aspect of this space?

• How has the perception of the cyber domain changed over time for NATO and the EU?

• As of today, is the concept of security being created, recreated or disturbed due to the emergence of cyberspace?

• How has the cyber domain influenced how EU and NATO perceive security?

Your answers to these questions will be recorded via a voice recorder.

**Participation is voluntary**

Participation in the project is voluntary. If you chose to participate, you can withdraw your consent at any time without giving a reason. All information about you will then be made anonymous. There will be no negative consequences for you if you chose not to participate or later decide to withdraw.

**Your personal privacy – how we will store and use your personal data**

We will only use your personal data for the purpose(s) specified in this information letter. We will process your personal data confidentially and in accordance with data protection legislation (the General Data Protection Regulation and Personal Data Act).

• In addition to the University of Oslo, the thesis advisor Bruno Oliveira Martins will have access to the information collected in the interviews.

• I will replace your name and contact details with a code. The list of names contact details and respective codes will be stored separately from the rest of the collected data, you will store the data on a research server, locked away and encrypted.

• This project will use Nvivo, a qualitative data analysis computer software that will help store and sort the interview

• In the final publication, your name and occupation will be published. However, if you do not feel comfortable with this, we can use a code and leave your name and occupation out and simply point to your expertise.

What will happen to your personal data at the end of the research project? The project is scheduled to end August 01, 2020. After this date, the personal data collected will be deleted.

**Your rights**

So long as you can be identified in the collected data, you have the right to:

- access the personal data that is being processed about you

- request that your personal data is deleted - request that incorrect personal data about you is corrected/rectified

- receive a copy of your personal data (data portability), and

- send a complaint to the Data Protection Officer or The Norwegian Data Protection Authority regarding the processing of your personal data

**What gives us the right to process your personal data?**

We will process your personal data based on your consent.

Based on an agreement with University of Oslo, NSD – The Norwegian Centre for Research Data AS has assessed that the processing of personal data in this project is in accordance with data protection legislation.

**Where can I find out more?**

If you have questions about the project, or want to exercise your rights, contact:

• Neven Ahmad- Project Leader

  o Email: nevenfa@student.sv.uio.no

  o Phone: +47 95 99 23 06

• Bruno Oliveira Martins- Thesis Advisor

  o Email brumar@prio.org

  o Phone: +47 40 03 77 85

• Roger Markgraf-Bye- Data Protection Officer

  o Email: personvernombud@uio.no

  o Phone: +47 90 82 28 26

• NSD – The Norwegian Centre for Research Data AS, by email:

(personverntjenester@nsd.no) or by telephone: +47 55 58 21 17.

Yours sincerely,

| | |
|---|---|
| Neven Ahmad | Bruno Oliveira Martins |
| (Student/Project Leader) | (Senior Researcher/Supervisor) |

---

---- Consent form  Consent can be given in writing (including electronically) or orally. NB! You must be able to document/demonstrate that you have given information and gained consent from project participants i.e. from the people whose personal data you will be processing (data subjects). As a rule, we recommend written information and written consent.  - For written consent on paper you can use this template - For written consent which is collected electronically, you must chose a procedure that will allow you to demonstrate that you have gained explicit consent (read more on our website) - If the context dictates that you should give oral information and gain oral consent (e.g. for research in oral cultures or with people who are illiterate) we recommend that you make a sound recording of the information and consent.

If a parent/guardian will give consent on behalf of their child or someone without the capacity to consent, you must adjust this information accordingly. Remember that the name of the participant must be included.

Adjust the checkboxes in accordance with participation in your project. It is possible to use bullet points instead of checkboxes. However, if you intend to process special categories of personal data (sensitive personal data) and/or one of the last four points in the list below is applicable to your project, we recommend that you use checkboxes. This because of the requirement of explicit consent.

I have received and understood information about the project [insert project title] and have been given the opportunity to ask questions. I give consent:

¨ to participate in (insert method, e.g. an interview)  ¨ to participate in (insert other methods, e.g. an online survey) – if applicable ¨ for my/my child's teacher to give information about me/my child to this project (include the type of information)– if applicable ¨ for my personal data to be processed outside the EU – if applicable ¨ for information about me/myself to be published in a way that I can be recognised (describe in more detail)– if applicable ¨ for my personal data to be stored after the end of the project for (insert purpose of storage e.g. follow-up studies) – if applicable

I give consent for my personal data to be processed until the end date of the project, approx. [insert date]

---

(Signed by participant, date)

**Appendix IV: Interview Guide**

- In your expert opinion, how has the emergence of the cyber domain impacted EU-NATO relations?
- Why are the EU and NATO cooperating in their efforts in cyberspace, specifically in regard to security and defence?
- In your opinion, how do NATO and the EU conceptualize this new space and its securitization? • Do you believe EU-NATO cooperation in this domain differ than those in traditional domains such as land and sea? If so, how?
- Is the cyber domain blurring the lines between the military sphere and the civilian sphere?
- What are some challenges that NATO and EU cooperation and relation face in relation to the dual-use aspect of this space?
- How has the perception of the cyber domain changed over time for NATO and the EU?
- As of today, is the concept of security being created, recreated or disturbed due to the emergence of cyberspace?
- How has the cyber domain influenced how EU and NATO perceive security?