Strategic cybersecurity partnership: Investigating the rationale behind the *EU-NATO Joint Declarations*

Thesis Dissertation

Christian Ørding Olsen – 05th September 1987

Hand-in Date: 3rd August 2020

Number of strokes: 191.842

Supervisor: Prof. Danita Catherine Burke

Abstract

The traditional structures of intergovernmental organizations such as the EU and NATO are challenged by rapidly changing environment in cyberspace. Through an analysis of *how* developments in cyberspace have affected the development of *EU-NATO Joint Declarations* (henceforth referred to as *Joint Declarations*), this thesis discusses the question of *why* such declarations were perceived as the next rational step for both organizations in making cyberspace more secure. Cyberspace is a realm that transcends the state borders, which are some of the most well-known denominators within the physical world. Moreover, it is an environment that is currently ungoverned, and which provides states and non-state actors alike with a range of possibilities to engage in threatening, malicious behavior. Concerningly, most of such behavior cannot be attributed to specific actors due to the characteristics of cyberspace enabling actors to mask their identity. This, combined with the fact that cyber threats are themselves becoming increasingly sophisticated and complex, poses a tremendous, contemporary challenge for states as well as international organizations such as the EU and NATO.

This thesis examines the rationale behind the EU and NATO's strategic cyber partnership, as initiated with the signing of the two *Joint Declarations*. In doing so, this thesis analyzes and compares selected EU and NATO cyber strategies that provide an understanding of the organizations' conceptualizations of cyberspace, perceptions of the cyber threat landscape, and cyber deterrence approach. A subsequent discussion on the rationale behind the *Joint Declarations* is presented building on the analysis of the *Joint Declarations*.

The findings suggest that, despite having similar values and goals and, to a certain degree, conceptualizations and perceptions in cyberspace, the EU and NATO's partnership has yet to come to fruition. Nevertheless, as no state or organization can counter all threats in cyberspace by itself, alliances and strategic partnerships might prove essential to ensure one's own safety in cyberspace.

Table of Content

Table of Figures

1. Introduction

Modern society's dependency on the Internet is rapidly growing, which in turn provides malicious cyber actors with more targeting opportunities. Thus, the increased use of cyberspace gives rise to increased vulnerability, evident in the 2007 cyber-attack in Estonia or the massive damages caused by the 'NotPetya' attack in 2017, which caused millions in damages (European Parliament 2019, 1). Given the accessibility, almost anybody, be they individuals, professional criminals, states, or non-state actors, could become a malicious actor in cyberspace. Cyber threats are not only increasing in volume but also in sophistication and potential damage. In a response to this evolving threat landscape, states and non-state actors alike are developing offensive cyber capabilities in a pursuit of geopolitical, enrichment or disruptive goals (Ibid, 1-2). This causes states to become uncertain regarding others' motives, capabilities, responses, and general behavior in cyberspace, which ultimately can cause international tensions to rise. This uncertainty contributes to an accelerated arms race and increases the cyber security dilemma among states (Nyemann 2018, 4). States and organizations are therefore urgently trying to find a way of mitigating the threats stemming from cyberspace.

For the Members of the EU and NATO, the Internet has become increasingly important for economic growth, freedom, and democracy. Concurrently, the threats stemming from cyberspace have become a problem, as they have proven not only to carry the potential of damaging the Members' economy but also their democratic foundation. As a result, both organizations have implemented several strategies in an attempt to mitigate and deter threats and threat actors in cyberspace. However, in cyberspace, no single state or organization can counter the entire cyber threat landscape alone and in 2016 the EU and NATO agreed on an unprecedented cyber partnership. Yet, very little research has been conducted on the organizations' compatibility and rationale behind the partnership.

The EU-NATO partnership is examined in this thesis through a two-fold research question. Firstly, the thesis sets out to analyze *how* developments in cyberspace have affected the development of the *Joint Declarations* regarding a joint approach to cybersecurity, defence and deterrence. This part is further divided into three steps in order to identify and analyze the cyberspace conceptualization, cyber threat landscape and cyber defence approach of the EU and NATO. This step is pertinent to analyze, as it provides an insight into the organizations' compatibility and thus their potential for a fulfilling their goals as stated in the *Joint Declarations.* This is followed by a comparative analysis of the two organizations understandings. This comparative analysis provides the foundation for the second part of the thesis, which seeks to analyze and discuss the rationale of *why* the *Joint Declarations* were seen as the next rational step in making in cyberspace more secure.

This subject adds to a small amount of research conducted on the rationale behind cyber partnerships. Thus, this thesis is contributing to an area, which is increasingly becoming more crucial given states and organizations' increasing dependency on the Internet and the services it provides. All the while cyber threats and actors are becoming more complex and dangerous.

To fully appreciate the analysis, this thesis begins with a conceptualization of cyberspace. Since the theories used in the thesis' analysis, e.g. deterrence and defence, differs greatly from their physical world counterparts, it is necessary to define the arena in which they function. See more in the section below.

To facilitate the thesis' analysis, a time frame from 2009 until present is applied. This prevents an uneven data collection, which could cause a skewering of the comparative analysis and ultimately an incorrect basis for the discussion. The time frame was selected since both organizations in close succession acknowledged that cyber threats were rapidly increasing in numbers and sophistication. In addition, by allowing the time frame to run until 2020, it includes the most recent progress report on the implementation of the *Joint Declarations.*

2. Literature review

This chapter explores how cyber deterrence has evolved from initially being a rough copy of Cold War nuclear deterrence where the goal was absolute deterrence, meaning that even one attack by the enemy would have proven devastating, into a stand-alone strategy which has been the focus of both academics and policy makers in recent years. Even though the nuclear deterrence approach might still be applicable for certain high-level strategic attacks, the nature of cyberspace necessitates a more comprehensive and tailored strategy due to the diversity of actors, threats and motivations involved (Burton 2018, 14; Iasiello 2013; Valeriano and Maness 2015).

Additionally, this chapter furthermore examines how the cybersecurity dilemma inadvertently causes states or organizations to feel threatened and thus increase their defensive capabilities, when they perceive their own security as inferior to others (Nyemann 2018, 12). This dynamic is amplified in cyberspace, as states are able to do more preparation undetected (Buchanan 2016, 48-49). This is based on the notion that defensive initiatives can easily be mistaken as escalatory capabilities if detected (Nyemann 2018, 12-13; Bendiek and Metzger 2015, 561).

The focus on cyber deterrence and the challenges stemming from cyberspace gained traction after the 2007 cyberattack in Estonia (Goodman 2010, 102; Valeriano and Maness 2015; Burton 2015, 310; Lété and Pernik 2017, 2). This is exemplified in the American 'Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee' in which 'cyber threats' were mentioned for the first time (McConnell 2008). By then, cyber deterrence had already been a focus point in NATO for several years, as they in 2002 during the Prague Summit placed cyber defense on their political agenda. (NATO 2019). The EU on the other hand, first began to pay serious attention to the challenges stemming from cyberspace in 2009 (European Commission 2009).

Authors such as Buchanan (2016) connects a central element in international relations theory, the security dilemma, to cyberspace, and shows how the particular characteristics of the digital domain largely influences the dilemma. The cybersecurity dilemma is both a vital concern of modern statecraft and a means of accessibly understanding the essential components of cyber operations (Buchanan 2016). Slayton (2017) adds to Buchanan's notion, and states that interactions based on fears of others' capabilities possibly increases the likelihood of conflict, and thus the cybersecurity dilemma (Slayton 2017, 72). Nyemann (2018) agrees to Slayton's notion, and claims that the development of cyber capabilities can trigger the security dilemma, as cyber defense is more difficult to prepare than cyber offense. Relatedly, the strengthening of one's own cyber defense includes organizational integration of offensive capabilities, which subsequently can cause an intensification of the security dilemma, as it becomes difficult to distinguish defensive from offensive capabilities (Nyemann 2018, 12).

The cyber incidents in Estonia in 2007 highlighted states' and organizations' need to develop their ability to prevent, detect, defend against and recover from cyberattacks. Moreover, the cyber incident caused a spike in cyber deterrence attention (NATO 2011, 1). For the EU and NATO, the incident caused a shift towards the threat emanating from states, state-sponsored groups and non-state actors in cyberspace (Burton 2015, Lungescu 2014; Lété and Pernik 2017), which is evident in the strategies the two organizations implemented in the years to come.

The importance of the cyber arena is underscored by Burton (2018, 3) who argues that if no progress is made on deterring malicious activity online, the costs and consequences of cyber-attacks will continue to grow and continue to cause instability within the international system.

Academics and policy makers have long agreed on the necessity to create a viable state-level cyber deterrence strategy, however as pointed out by Goodman (2010), this is not without its challenges (also see Bendiek 2015; Brantley 2018; Taddeo 2018). As pointed out by Schulze (2019, 2), existing in a multipolar world order[1] means that cyber deterrence often involves asymmetric opponents. Moreover, cyber capabilities are easily proliferated, which means that cyber deterrence are prone to failure (Ibid, 2; Bendiek and Metzger 2015, 558; Lewis 2013, 3), as seen in Saudi Arabia during the cyberattack on Saudi Aramco in 2012, in Ukraine 2017 during the 'NotPetya' cyberattack which exploited a security backdoor[2] in an Ukrainian tax preparation program to target the country's critical infrastructure (Tolga 2018). Craig and Valeriano add that a challenging aspect of cyber deterrence is, the lack of ability for states to physically demonstrate retaliatory capacity to cyber weapons. Moreover, they state that because cyber weapons[3] does not having the same destructive capacity as nuclear weapons, such weapons must be used repeatedly and with great effect to achieve a sufficient deterrent effect. Furthermore, attribution in cyberspace can prove difficult, causing uncertainty as to whom one should retaliate against. Based on these arguments, the policy implications are, according to Craig and Valeriano, that deterring aggression through cyber means is

[1] Characterized by more than two centers of power or interest

[2] Security backdoor refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access on a computer system, network, or software application (Malwarebytes 2020, 1).

[3] Cyber weapons refer to malicious code or exploitation of vulnerabilities in cyber networks or systems through various techniques intended to cause damage (Goychayey et al. 2017, 15)

an unworkable policy in practice (Craig and Valeriano 2018, 94). Adding to the complexity of this policy issue, other studies have found that a deterrence strategy which is effective against one potential adversary, may not deter another (Mazarr 2018, 8).

While authors like Craig and Valeriano (2018) and Mazarr (2018) focus on challenges regarding policy options for cyber deterrence at a state level, scholars such as Nye (2017), Brantley (2018), and Lynn (2010), argue that while cyber deterrence may face challenges, failure is not a given. Goychayev et al. (2017), Iasiello (2014), and Tolga (2018) argue that the main concepts from nuclear deterrence, deterrence by punishment and deterrence by denial, are not directly transferable to cyberspace, but could work by adding some elements relevant to cyberspace (Goychayev et al. 2017, 51; Iasiello 2014, 67; Tolga 2018, 18). Denning (2016) and Ryan (2017), suggests that by employing active defensive measures, for example 'hack back' (Ryan 2017, 333; Denning 2016, 2) and by establishing international norms regulating state behavior in cyberspace, deterrence in cyberspace is achievable (Ibid, 3; Taddeo 2018, 6; Goychayev et al. 2017, 49).

The characteristics of cyberspace is one of the reasons for cyber deterrence evolving slowly. There is no "one size fits all" for deterrence, and requirements for effective cyber deterrence vary greatly, given the variety of actors and threats in cyberspace (Brantley 2018, 44). These create a need to address their unique characteristics, i.e. goals, interests, strengths, strategies, and vulnerabilities, more often than in classical deterrence theory. There appears to be a consensus among most scholars that deterrence by punishment and the pitfalls in this approach makes for an ineffective policy concept that contains too many risks to the state, which are exemplified in the challenges of attribution, escalation, and credibility associated with the strategy (Libicki 2009; Bendiek and Metzger 2015; Schulze 2019). Libicki (2009), Bendiek and Metzger (2015), and Schulze (2019) argue, that the lack of correct attribution affects the strategy's legitimacy and the threat of punishment ultimately lack a certain strategic gravitas, as a central question arises; who should be threatened with punishment? Schulze (2019) further argues that threat of punishments must be credible insofar that if an attacker does not believe the defender, firstly, is technically capable of causing precisely measured costs with digital means or, secondly, lacks the political will to resolve or endure the risk of escalation, deterrence by punishment will fail (Schulze 2019, 5). The problems associated with creating strategies founded on deterrence by punishment have created a preference in many quarters for cyber deterrence by denial. This is reflected in the massive investment in defensive cyber security measures throughout the developed world, and this approach has been a central part of NATO's emerging cyber security strategy (Burton 2018, 9). The challenges of deterrence by denial to be an achievable approach in cyberspace has also been discussed by, amongst others, Burton (2018) and Mazarr (2018). The approach is a largely passive strategy that does little to address the actions and motivations of the attacker. The political need to be proactive in responding to threats in cyberspace runs counter to deterrence by denial approaches (Burton 2018, 9). Nonetheless, studies suggest that denial strategies are inherently more reliable than punishment strategies (Mazarr 2018; Iasiello 2014; Goychayev et al. 2017).

Studies by scholars such as Tor (2017) and Burton (2018) have thus examined classic deterrence approaches as well as challenges to incorporating such strategies within in a cyber context. These studies have discussed how deterrence strategies potentially could be adjusted to be a better fit for a cyber context and thus accommodating some of the challenges outlined in the other studies above. Amongst those are Tor (2017, 1) who argues that a slow and unpromisingly development of cyber deterrence as a strategic tool in both theory and practice is mostly due to the ill-fitting theoretical framework and underlining assumptions it borrows from the absolute-nuclear-deterrence context (Tor 2017, 1). Tor is not alone with this claim, as Burton (2018) states that since cyber deterrence has been relying on central arguments from the binary Cold War conceptions of deterrence, state-centric conceptions of cyber security is likely to prove ineffective. Burton notes that a tailored approach that recognizes the role of a diverse range of deterring actors and deterrable threats and which includes legal, social, normative and technological approaches to deterrence, could yield greater benefits. (Burton 2018, 27-28). Relationally, Burton and Tor argue that it is essential to accept that cyber deterrence is non-absolute, and its aim should instead be to postpone and limit actors and threats (Ibid, 14; Tor 2017, 93). Others, such as Tropeano (2019) and Taddeo (2018) argue that cyber deterrence may be unsuited as a stand-along strategy, and that it should be incorporated into an overall deterrent strategy (Tropeano 2019, 1; Taddeo 2018, 3-4).

As will be elaborated upon in the analysis, following the 2007 Estonia cyber incident the EU and NATO began implementing cyber strategies in an attempt to mitigate the contemporary cyber threat landscape. These show a clear interrelationship between the EU and NATO’s approach to cybersecurity and cyber deterrence, as they both embody a high level of cyber resilience and a combination of deterrence by denial and punishment.

3. Theory

In this thesis, I chose a theoretical framework that combines two classic schools of thought within International Relations (IR) to shed light on different dynamics of my research question. Firstly, to analyze the context of the cyber threat landscape organizations face, I draw on scholars from realism. Thereafter, to explore some of the dynamics between organizations engaging in partnerships, such as the *Joint Declarations*, as a response to threats from cyberspace, I include scholars from the field of liberalism.

Initially, it is essential to this thesis to define what cyberspace is. Moreover, it is relevant to examine the concepts *cyber* deterrence and *cyber*security dilemma as these concepts differ in cyberspace than in the physical world. Cyberspace can be described as consisting of three layers (Brantley 2018, 39-40; Royal Danish Defense College 2019, 7-8):

- The physical network layer is comprised by geographical components and the physical network components, for example network equipment, computers, and wired and wireless connections. In other words, it is a medium for data to travel through.
- The logical network layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network. For example, documents, files, firmware, operating systems, and programs. The logical network layer cannot work without the physical network layer, as digital information and commands are transmitted and stored at the physical network layer.
- The cyber-persona layer is a higher level of abstraction of the logical network layer. Through the logical network layer, it allows for development of a digital representation of an individual or entity identity in cyberspace for example, email addresses, user IDs, social media accounts, IP and MAC addresses. It is worth noting that a cyber-persona may be used by several physical individuals or entities. Conversely, one individual or entity may have several cyber-personas.

Because of the nature of cyberspace – i.e. the physical, logical, and cyber-persona layers - the conceptualization of cyber deterrence fundamentally differs from the conceptualization of deterrence in the physical domains of land, sea, and air. Deterrence in the physical domain might include physical and cognitive aspects analogous to the cyber-persona and physical network layers, however, the logical layer is wholly absent. The cyber-persona layer also diverges significantly from personas within the physical domain as individuals and states have the capacity to alter their attributes, thus making attribution of cyberattacks difficult (Brantley 2018, 40-41).

Additionally, I acknowledge that when analyzing the two organizations, they are simplified into analytically constructed (ideal type) actors. This means that I analyze them as such while recognizing that they operate empirically in a more complex manner due to the many interests and actors involved with their work.

3.1. Realism

Within International Relations (IR), realism is a school of thought that encompasses many multifaceted studies and scholars. In general, what is central to realist theories are their so-called 'pragmatic' approach to international relations, describing the world 'as it is, not as it ought to be' (Jørgensen 2018, 88). In the following, the elements of the theory of realism, which are deemed relevant to this thesis, are examined. Initially, by drawing on Morgenthau (1948), who is hailed as one of the founders of realism theory (Morgenthau 1948, 90), relevant concepts in the international system are examined. In addition, elements from the seminal work of Waltz (1979) on structural realism, the notion of the international system's anarchical state and defensive realism, is added to Morgenthau's theory (Waltz 1979, 89; Wivel 2002, 433). Furthermore, Mearsheimer's work, *The Tragedy of Great Power Politics* (2001), will be drawn upon as it adds yet another element, more specifically regarding offensive realism. Lastly, to incorporate scholars that interpret and apply elements from realist theory to cyberspace, I draw on studies by Craig and Valeriano (2018).

The notion of the international system as dominated by states is shared by some of the most prominent scholars within realism i.e. Morgenthau (1948, 13) and Waltz (1979, 102). According to Morgenthau and Waltz, the international arena can be seen as a competitive and hostile stage where power is the main currency (Ibid 102, Morgenthau 1948, 13). The concept of power is therefore at the very heart of their analysis of international politics. However, Morgenthau and Waltz differentiate on the roots of international conflict and war. Morgenthau claims that these roots are based on the imperfect human nature (Morgenthau 1948, 4-9), whereas Waltz (1979) as well as Mearsheimer (2001) claim that the roots of international conflict and war are anchored in the anarchical state of the international system (Waltz 1979, 102; Mearsheimer 2001, 30). According to Waltz, the anarchical structure of the international system, being the lack of a legitimate monopoly of violence, is what differentiates politics between states in the international system and state's internal politics. Since there is no centralized actor to protect states from each other, a lack of a legitimate monopoly of violence will occur, prompting states to focus on their own security and essentially survival. This, in turn, causes international relations to become defined by state power (Waltz 1979, 102-104; Wivel 2002, 433). The anarchical characteristic of the international system additionally means that the occurrence of violence is unavoidable. States exist in constant fear of attack, as Waltz (1979) states: "Because some states may at any time use force, all states must be prepared to do so […]" (Waltz 1979, 102). When combining the anarchical characteristic of the international system with state's goal of survival, two main state behavior characteristics can be deduced. First, every state will manage their own defence, as it is necessary for their survival. No state will entrust another with the functions central to their survival. Nonetheless, states are willing to cooperate to the extent, they gain from it and avoid risking their own security. Second, states will attempt to counter-balance the strongest power either through an arms race or through the creation of alliances or a combination of the two (Wivel 2002, 434).

Waltz' notion of defensive realism stems from his notion of the anarchical nature of the international system, which encourages states to undertake defensive and balanced policies. States are not inherently aggressive since "The first concern of states in not to maximize power but to maintain their positions in the system.". Accordingly, the international system induces balancing and not bandwagoning, as the latter would entail creating a world hegemony (Waltz 1979, 126). In other words, defensive realists assert that states, which strive to attain hegemony in the international system will be counterbalanced by other states seeking to maintain the status quo. Therefore, conflicts arise as an accidental consequence when states seek to survive in the anarchical system. As they increase their own security, they will decrease other's security, creating what Herz (1950) and Jervis (1978) refer to as a security dilemma. Offensive realists, such as Mearsheimer, on the other hand, argue that there are no status quo powers in the international system, except for the occasional hegemon that wants to maintain its position, since the desire for power does not go away (Mearsheimer 2001, 3). Moreover, the anarchical state of the international system, encourages states to look for opportunities, to alter the balance of power at the expense of others, which eventually will influence the security dilemma (Ibid, 30). Ultimately, the goal is not to create a status quo system, but to become the hegemon in it (Ibid, 21).

Based on the current cyberspace environment, I argue that with no international governing body or police force, cyberspace is well captured within a realist conceptualization of an anarchical system. In cyberspace, every state stands alone, or with its allies, whom it can never fully trust, and therefore tries to build up its offensive and defensive cyber capabilities while fearing that every breakthrough made by another state poses a direct threat to their security. Craig and Valeriano (2018) add that because realism is mostly concerned with issues of national security and power, realism would appear to be the natural international relations perspective for understanding cyber conflict. Furthermore, realism remains a relevant framework for this thesis in identifying important security-related issues in the cyber domain and can provide useful insights about some enduring characteristics of international relations and stability (Craig and Valeriano 2018, 94-95), for example the security dilemma.

Despite providing useful analytical elements, realism does have its limitations. In the post-Cold War era, which has been influenced by a rapid technological development, the theoretical corner stones have proven insufficient in their explanations of war, foreign intervention, or the changing relations between states. In contract to classical realism, Waltz' notion of structural realism failed to take the coming of non-state actors into account. Although still relevant regarding core concepts of states interacting globally, I argue, realism would prove too simplistic to be used on its own to analyze the *Joint Declarations*. Whereas if used as part of a pluralistic approach, realism could provide key insights into the decision-making process of the EU-NATO agreement.

3.2. Liberalism

Liberalism is another school of thought within IR in which the role of international organizations and the decline in military force as a balance of power-tool is central, albeit with different assumptions compared to the realism. In the following, elements of the theory of liberalism, which are determined relevant to this thesis, are examined, such as Keohane and Martin's (1995) notion of liberal institutionalism and state interaction through organizations. In short, it represents a main argument that non-state actors (i.e. transnational organizations, social movements, and terrorists) have been equated to states in international relations. This will be elaborated below. Additionally, Keohane and Nye's (2012) concept of complex interdependence theory, on how international politics are transformed by interdependence will be drawn upon, as it can shed light on questions regarding how interaction between states and organizations may diminish the use of military force as a balance of power-tool. Lastly, Eriksson and Giocomello (2006) are included in the theoretical framework as their approach of applying liberal theory to the distinct sphere of cyberspace and are thus highly compatible with my further analysis.

In the following, arguments presented by scholars within the liberal school of thought, note that state interdependence and an increased multilevel cooperation could mitigate threats stemming from cyberspace. As stressed by Eriksson and Giocomello (2006), states alone are not able to counter the threats in cyberspace and must enter into cooperation with international institutions and organizations. The international institutions and organizations could in turn, potentially diminish security dilemmas originating from the interconnected and globalized world (Eriksson and Giocomello 2006, 230).

According to Jørgensen (2018), liberal theorists focus on state–society linkages and claim the existence of a close connection between domestic institutions and politics on the one hand and international politics on the other hand. Moreover, the increasing economic interdependence among states are said to reduce the likelihood of conflict and war (Jørgensen 2018, 67), which is in contrast to realist beliefs (Mearsheimer 2001; Waltz 1979). This is evident in the creation of the League of Nations, following the belief among analysts and policy-makers that a global international organization could prevent war better than the traditional balance of power politics. In other words, liberalism in general argues that the anarchical state of the international system can be modified and, to some extent, controlled through international institutions (Jørgensen 2018, 67-68). Overall, most scholars within liberalism agree with realists that states are the central actors within the international system. Nonetheless, liberals claim that states by no means are the only actors that play a significant role, as organizations and non-state actors become increasingly influential. Moreover, scholars within liberalism tend to highlight a positive outcome of interdependence and interconnectedness, rather than increased vulnerability and insecurity as is the case for most realists (Eriksson and Giocomello 2006; Keohane and Martin 1995).

A core path in the liberalist school of thought was developed in 1995, in which Keohane and Martin stated that a central element of liberal institutionalism is how international institutions have become the primary actor in international relations. They argue that institutions such as the EU and NATO are capable of facilitating cooperation in complex situations, especially those involving a large number of states (Keohane and Martin 1995, 45). Relationally, realists claim that states are reluctant to cooperate with one another as they fear that the others are gaining more than themselves. Liberal institutionalism takes on a different approach and argues that through the creation of institutions, fear of cheating in cooperation by other actors can be mitigated thereby helping to explain how cooperation can emerge. In addition, institutions can facilitate cooperation by helping settle distributional conflicts and by assuring states that gains are evenly divided over time, for example by disclosing information about the military expenditures and capacities of alliance members (Ibid, 45-

46). This in turn relates to security issues, as institutions can disclose specific information about military capabilities and thus calm potential emerging security dilemmas (Ibid, 43; Jørgensen 2018, 70-71).

Keohane and Nye (2012) add to the liberal school of thought, the notion of complex interdependency. Whereas dependence refers to a situation in which a state is being determined or significantly affected by external forces, interdependence refers to a situation of mutual dependence. Interdependence in international politics refers to situations characterized by reciprocal effects among states or actors within different states (Keohane and Nye 2012, 7). A central element of Keohane and Nye's argument is that in international politics' multiple channels connect society, which manifests itself through channels such as informal and formal governmental ties to transnational corporations and organizations (Ibid, 20). Put differently, the actors' activities are essential, as they are capable of influencing intergovernmental policies, ultimately ensures that they become aware of other actors' goals (Ibid, 21), which is why organizations such as the EU and NATO are central to analysis in the cyber context. Another central element is the decline of the use of military force as a balance of power-tool (Ibid, 9). According to Keohane and Nye, the use of military force is not exercised when complex interdependence prevails. A notion exists that between state in which there is a complex interdependence, the role of the military in resolving disputes is negated (Ibid, 22-23). Nevertheless, Keohane and Nye argue that even though military force could be irrelevant in resolving disagreements on economic issues, it could still retain some importance for alliances' political and military relations with a rival bloc (Ibid, 21).

The liberalist literature is not limited to interstate relations. For example, Eriksson and Giocomello (2006) who stress the importance of multilevel cooperation and public-private partnerships to mitigate cyberthreats and highlight that, "Government alone cannot secure cyberspace" (Eriksson and Giocomello 2006, 231). Likewise, governments have increasingly recognized that they alone cannot provide the growing number of public services needed by modern societies. This causes an increase in public-private partnership and privatization, which is evident in sectors such as health, education, transportation, and to a lesser extent, security (Ibid, 231). According to Eriksson and Giocomello, cyber threats are contemporary challenges due to the globalized world, which, they argue, weakens national security. The amount of powerful non-state actors is increasing, in part, because of the many possibilities that cyberspace provides, which can have both positive effects on integration and cooperation as well as negative effects in form of terrorism, transnational crime, and the destabilization of states (Ibid, 232). Ultimately, a security dilemma deriving from the interconnected and globalized world, could potentially be resolved through the creation of international institutions (Petallides 2012, 2-3). Though it might, especially from the outset, seem difficult to create an international organization composed of states and non-state actors alike all devoted to the maintenance of cybersecurity, it would undoubtedly, in theory, diminish the uncertainty and insecurity of cyberspace (Ibid 2-3). Petallides states that in theory, each member would reveal its capabilities thereby offering others the possibility to identify its cyber activities, ultimately fostering trust and security through transparency. However, this would also entail members to give up more information than they are likely to do in fear of weakening their position. Moreover, some states would probably avoid joining all together in order to be able to continue their already established cyber activities (Ibid, 2-3).

The complexity and challenges in cyberspace are highlighted by the ever more influential non-state actors and international interdependency. This ultimately highlights the importance of cooperation in cyberspace.

3.3. Cyber deterrence

Deterrence is not a modern nor a novel concept. Classical deterrence can be traced back to Thucydides during the Peloponnesian War and the threat of violence in response to adversary actions. However, the modern formulations of deterrence came about following World War II and the coming of the nuclear age (Brantley 2018, 32; Brodie 1958, 3). Deterrence theory is often divided into two sub-deterrence strategies (i) Deterrence by denial which seeks to make the adversary doubt it can achieve its goals, and (ii) Deterrence by punishment which seeks to make the adversary believe that achieving its goals is not worth the impending retaliation (Goychayev et al. 2017, 17-18; Nye 2017, 54). Two key components in both cyber deterrence strategies are signaling and communication. Because deterrence theory assumes that others receive and decode the deterrer’s signals although they might not always believe the messages conveyed. However, if the signals or communication is misunderstood, flawed conclusions about an adversary’s action or response can be made, which can cause deterrence to fail (Jervis 1979, 308; Goychayev et al. 2017, 19).

Since the Cold War, deterrence by punishment has been favoured over deterrence by denial given the capacity of the former to effectively protect against nuclear weapons. According to Thomas Schelling (1995), deterrence is about intentions. It is not just about estimating enemies’ intentions but also influencing them (Schelling 1995, 35). Schelling states that deterrence’s position in time is indefinite as the timing is up to the attacker and the deterring actor can wait forever (Ibid, 72). The objective of cyber deterrence is at its core, I argue, very similar to that of classical nuclear deterrence and conventional deterrence: to avoid being attacked. However, cyber deterrence differs greatly from classical nuclear deterrence and conventional deterrence both in the aspects of actors and means but also due to the different nature of cyberspace (Iasiello 2014, 54; Tolga 2018, 7; Craig and Valeriano 2018, 95).

In 2010, Knopf argued that deterrence in cyberspace reflects a change from a focus on relatively symmetrical situations of mutual deterrence to a greater concern with what have come to be called asymmetric threats (Knopf 2010, 1). Knopf stresses that this could include considerations of cyber deterrence (Ibid, 2). Knopf draws on earlier notions on deterrence, such as the role of assurances in making deterrence effective and the importance of integrating deterrence into a framework that includes other policy tools. However, contrary to its predecessors, cyber deterrence is driven by attempts to understand how deterrence operates in situations that appear different from the traditional interstate rivalries which were a key element in earlier deterrence theories.

Consequently, this necessitates a broader foundational work for the concept of deterrence, which still includes, but is not limited to, threats of military retaliation (Ibid, 2-3). Moreover, earlier theories did not allow any deterrence failures, as this could have meant total annihilation. Thus, the current security environment calls for a different approach. As Knopf argues, deterrence failures can still have terrible consequences for some people, but it does not impact a state’s ability to survive, meaning that one or more deterrence failures will therefore not undermine the value of deterrence (Ibid, 4). According to Buchanan (2014), the notion of absolute deterrence from the Cold War era is still alive and well today, given the nuclear deterrent many nations possess. However, if directly applied to cyber operations, it would only have little efficiency because of the diverse cyber threat landscape (Buchanan 2014, 132).

The sections below will examine the two main cyber deterrence strategies, by punishment and by denial, and how they can play a part of the EU and NATO’s visions of making cyberspace a more secure domain.

The central element in deterrence by punishment is to create disincentives against adversaries by threatening potential adversaries with harsh punishment for bad behavior, but implicitly promises to withhold any punishment if no attacks take place (Libicki 2009, 28; Tolga 2018, 7). In this sense, cyber deterrence by punishment is similar to nuclear deterrence by punishment, as both parties are mutually assured that in case of an attack, there will be an equal reaction from the victim (Tolga 2018,7). Consequently, according to Tolga (2018) deterrence by punishment seems to be a better approach given its better cost-benefit ratio (Tolga 2018, 7). Libicki (2009) supports this notion, stating that the attraction of deterrence by punishment is that, if it works, it can reduce the cost of defending systems. There would be no need to spend money on making systems more secure, as the defender precludes the attacker's intention by threatening retaliation against successful attacks (Libicki 2009, 34).

A drawback associated with the punishment strategy is the need for a credible retaliatory response (Brodie 1958, 5-6). It is necessary for the deterring actor to convey their will and determination to act quickly, accurately, and severely to a cyberattack. Stating that cyberattacks will be met with a swift punishment but not delivering on the threat after an attack, will seriously damage the deterring actor's credibility (Tolga 2018, 8; Iasiello 2014, 57; Bendiek and Metzger 2015, 557). Accordingly, establishing credibility in cyberspace can be very difficult as it entails that the deterring actor demonstrates its will, ability, and determination to potential attackers. However, by doing they risk exposing too much about their cyberweapon, which can render them useless since adversaries can locate and close the potentially targeted vulnerability (Ibid, 558-559; Goychayev et al. 2017, 51). Consequently, authors such as Brantley (2018), Lynn (2010), and Nye (2017) argue that deterrence by punishment in cyberspace is possible, but not a reliable or credible option (Brantley 2018, 46; Lynn 2010, 99-100; Nye 2017, 55).

Deterrence by denial is, in contrast to deterrence by punishment, less conflict driven as it seeks to convince potential attackers that their effort will fail and be denied the benefits they seek to obtain (Iasiello 2014, 55; Tolga 2018, 7; Philbin 2013, 4). The denial strategy is thus based more on defensive measures by discouraging or frustrating attacks, i.e. through resilience and costly defenses (Brantley 2018, 48).

However, the denial strategy requires a large and focused commitment by the actor to secure systems and networks under its control. Consequently, the cost increases significantly given the breadth of this endeavor including the use of advanced security practices and the adoption of trusted hardware and software components (Ibid, 47; Iasiello 2014, 55-56). This is subsequently a downside of the denial strategy because cyber deterrence generally is viewed in a cost-benefit ratio. In order for the denial strategy to become successful, its goal must be to turn the cost-benefit ratio in favor of the defender. In other words, it must convince potential attackers that the benefit they obtain from the damage inflicted or data collected, will be less that than the efforts and resources used (Tolga 2018, 7; Bendiek and Metzger 2015, 561).

A common challenge with cyber deterrence is the issue of attribution. Because of the Internet's decentralized, dynamic and open architecture, attackers can easily hide their tracks by changing their Internet Protocol addresses or leveraging the tactics, techniques, and procedures developed by other actors, thereby making it difficult to identify who actually committed the attack (Davis et al. 2017, 10; Libicki 2009, 43-44; Goychayev et al. 2017, 51).

Authors such as Iasiello (2014) and Tolga (2018) are adamant in their opinion, that deterrence by denial has a better chance of succeeding, as it can make the task of an attacker more difficult and simultaneously lowering the benefits from the attack (Iasiello 2014, 67; Tolga 2018, 8). Nye (2017) supports this notion and states that deterrence by denial has regained some of its importance during the cyber era. Even though cyber defenses are known to be porous, by building resilience and the capacity to recover from attacks, good cyber defense can be established. Especially resilience is vital as it reduces an adversary's benefits of attacking. In addition, the cost of resilience can vary from expensive, by for example stockpiling industrial power generators, to inexpensive, by for example training military personal in celestial navigation in case of loss of global positioning systems (Nye 2017, 56). Additionally, Goychayev et al. (2017) state, that by building stronger and more defensible computer architecture, investing in cyber security education of the population, and building resilient systems would create a safer cyber environment (Goychayev et al. 2017, 68).

Glaser (2011), on the other hand, states that pure deterrence by denial strategies have limitations. Even if a potential attacker believes that its attack is unlikely to succeed, it may not be deterred if the costs of attacking are low enough (Glaser 2011, 2). Taddeo (2018) adds to the criticism of deterrence by denial by stating that it is guaranteed to be an ineffective strategy in cyberspace. Defence, Taddeo (Taddeo 2018, 3-4) claims, is too porous and because every system has security vulnerabilities, identifying and exploiting them is simply a matter of time, means, and determination. Put differently, this means that even the most advanced defence systems will be short-lived thus limiting their potential of defence to deter new attacks.

In a similar fashion, as the end of any war does not mark a permanent cessation of future hostilities, so to is the case for deterrence. In the emerging cyberage, states and organizations are subjected to attacks in new and sophisticated ways, which has the potential to alter the way of future conflicts. In this case, cyber deterrence will arguably play an important part.

In summation, cyber deterrence is relevant in answering the thesis' research question as it can contribute with an understanding of the complementarity between the EU and NATO in cyberspace as well as an understanding of how the EU and NATO intended to shape their mutually beneficial cyber deterrence posture with the signing of the *Joint Declarations*.

3.4. Cybersecurity dilemma

The term 'security dilemma' was introduced by Herz in the beginning of the 1950s as a fundamental element of international relations (Herz 1950, 161). An essential part of Herz' concept, is the notion that a security dilemma necessitates the making of a choice between killing and being killed (Ibid, 172; Mearsheimer 2001, 35-36). According to Nyemann (2018), the security dilemma has developed into a security paradox, as increasing one's own security through power accumulation forces others to seek the same power, ultimately causing insecurity among the actors. This foster continued efforts to accumulate power, potentially resulting in negative and irreversible spirals (Nyemann 2018, 8).

In 1978, Jervis claimed that the anarchy in the international system would encourage behavior that leaves all actors worse off (Jervis 1978, 167). States will therefore seek to counteract the state of anarchy through increased security (Ibid, 169-170). Glaser (2004) adds that in reality, the security dilemma is about inter-state communication. When a state tries to show resolve, power, and credibility, it will often be perceived as aggressive and threatening if their communication fails to convince other states of their intentions. On the other hand, if a state, through decreasing its arms buildup, tries to signal peaceful intentions, it might be perceived as weak or as one whose sphere of interest is up for negotiation (Glaser 2004, 46-48; Nyemann 2018, 8).

Accordingly, the severity of the security dilemma is determined by whether offensive capabilities are distinguishable from defensive ones, and whether the offense is more effective than the defense. Jervis notes that if states increased their transparency, meaning the ability of others to recognize what you are doing, cooperation would be more likely. Coupled with the ability to act on information given, transparency can produce a situation in which the security dilemma is effectively ruled out (Jervis 1985, 73).

When it comes to the cyber realm, to Slayton (2017), points out that the fears of being hacked and confidence about hacking others, have prompted a global increase in cyber capabilities investment, suggesting a cyber arms race. Since cyber operations are by default dynamic, as they are not restrained in time and space as conventional operations, they can blur the lines between espionage and the use of force, which causes a cybersecurity dilemma. Network intrusions undertaken for defensive purposes could be mistaken as preparation of the battlefield, creating an environment where escalation and the use of force could easily happen (Slayton 2017, 73). This dynamic is highlighted as cyberspace operates in a virtual world, without difference between proximity and remoteness. Additionally, since time and space are not applicable to cyberspace, anarchical tendencies flourish (Nyemann 2018, 10).

In addition, the buildup of offensive capabilities can be done covertly can cause a general increase of insecurity, as both sides fear what the other is doing (Ibid, 10). Even if this notion is erroneous, the fact that the prevalent belief is that cyberspace favors offensive capabilities will cause an increased fear of attack, ultimately encouraging an arms race. Moreover, interactions between fears and capabilities can possibly increase the likelihood of conflict (Slayton 2017, 72). Nyemann (2018) claims that the development of cyber capabilities can trigger the security dilemma, as cyber defense is more difficult to prepare than cyberattacks. Relatedly, the strengthening of one's own cyber defense includes organizational integration of offensive capabilities, which subsequently can cause an intensification of the security dilemma (Nyemann 2018, 12).

Buchanan (2016) adds to this notion, stating that in the traditional security dilemma, actions such as building capabilities or training operators will, if discovered, be seen as a potential threat. Basic security dilemma logic states that when a state increases its own sense of security in making itself more secure, it risks making other states fell less secure. At a basic level, cyber operations amplify this dynamic, since states are able to do more preparation undetected (Buchanan 2016, 48-49). Defensive initiatives can thus easily be understood as an escalation if the opponent detects them, as signaling one's true intention is difficult when you try to do it secretly (Nyemann 2018, 12-13; Bendiek and Metzger 2015, 561).

According to Libicki (2016), cybersecurity revolves around two scenarios. Firstly, the distinct possibility that one's own cybersecurity will, in and of itself, increase or decrease another state's cybersecurity. Secondly, that particular actions to increase one's own cybersecurity may increase or decrease another state's cybersecurity. Libicki further argues that most defensive activities in cyberspace are easily recognized as defensive for example measures such as diligent patch management and least privilege, multi-factor authentication, and intrusion detection systems (Libicki 2016, 134). Buchanan opposes Libicki's view, stating that a part of the deterring actor's defensive activity often entails leaving their own networks and intrude into the networks of other states. He states that sophisticated states can have genuinely defensive reasons to launch intrusions into the networks of other states, as this can enhance their own network defense efforts by uncovering future risks. While it is possible to conduct such operations covertly, adversaries who discover such an operation would possibly consider it a threat (Buchanan 2016, 73-74).

Based on the above, the cybersecurity dilemma happens as a state or organization takes steps to increase its own cybersecurity. This inadvertently causes other states or organizations to feel threatened, as they feel their own security is being decreased. In relation to this thesis, the cybersecurity dilemma is relevant as the EU and NATO by joining forces will increase their cybersecurity and their capabilities. This causes their adversaries to see two powerful organizations becoming even more powerful, making them anxious about their own cybersecurity forcing them to commit to establish new capabilities to counter the EU and NATO's.

In summation, the cybersecurity dilemma is relevant in answering the thesis' research question as it can contribute with an understanding of why it was seen as mutual beneficial for the EU and NATO to sign the *Joint Declarations* and what challenges they might face because of it.

3.5. Subconclusion

This thesis' the theoretical framework combines two classic IR theories, realism and liberalism, to shed light on different dynamics of the research question. Realism can facilitate an understanding of states and organizations' understanding of cyberspace and their actions in it. Moreover, realism can provide insight into the cyber threat landscape that states, and organizations face and how they mitigate it. Liberalism can explain the dynamics or interorganizational cooperation within cyberspace as a response to the growing cyber threat landscape. Moreover, liberalism can highlight the ways non-state actors and international interdependency affect the *Joint Declarations*.

In addition, cyber deterrence and the cybersecurity dilemma can together provide an understanding of the complexity of challenges existing in cyberspace. Moreover, as theoretical tools they can provide insights into states' and organizations' rationale and actions in cyberspace, for example the *Joint Declarations*.

4. Research design

The following chapter outlines the research design in relation to the research question of the thesis. The chapter will additionally expand on the thesis' method, empirical timeframe, content of data collection including search terms, ontological and epistemological view, and lastly the analytical tools used for the subsequent analysis will be outlined.

This thesis sets out to analyze the following research question, which is divided into two parts, see Figure 1 below. Firstly, it sets out to analyze *how* developments in cyberspace have affected the development of *Joint Declarations* through two steps that identify and analyze how the EU and NATO each conceptualize cyberspace, perceive the cyber threat landscape and how their approach to cybersecurity have developed since 2010. Following the analysis of the EU and NATO, I compare the two organizations' conceptualization of cyberspace, the cyber threat landscape and cybersecurity. The comparison provides the basis for the analysis of the second part of the thesis' research question, which seeks to analyze and discuss *why* the *Joint Declarations* was seen as the next rational step for the EU and NATO in making cyberspace more secure. This part is supported by operationalizing the theories of liberalism, realism, deterrence, and the security dilemma to the findings from the comparison of the EU and NATO. Furthermore, it discusses the conceptualization of deterrence in the *Joint Declarations* and how it fits into the current deterrence paradigm.

Research design		
Part one	*How* developments in the cyberspace affected the development of *Joint Declarations*	
	Step 1 aim: Analysis of EU	Step 1 method: Document and textual analysis
	Step 2 aim: Analysis of NATO	Step 2 method: Document and textual analysis
	Step 3 aim: Comparative analysis of EU and NATO	Step 3 method: comparative analysis
Part two	*Why* the *Joint Declarations* was seen as the next rational step for the EU and NATO	

Figure 1 – Research design

The analysis examines the *Joint Declarations* from 2016 and 2018. Since the *Joint Declarations* is a relatively unique case of international cooperation within the field of cyberspace, this thesis' research method is a built around a qualitative single case study. A single case study enables the thesis to develop a detailed contextual analysis of data within this specific and narrow context. Drawing on Yin (1984), I understand case studies as a unique way of observing a *natural* phenomenon that can be seen within a set of data (Yin 1984). The methodological considerations associated with this choice are mostly concerned with the lack of generalization and application to other fields of research. However, in this case, as my intent is to achieve a contextual and in depth knowledge of the *Joint Declarations,* generalizing is neither a possibility nor an objective of the analysis in question.

It should be noted that NATO as early as 2002 placed cyber defense on their political agenda during the Prague Summit (NATO 2019). Nonetheless, in order to avoid an uneven data collection and thus risking skewering the comparative analysis, the thesis' time frame is set from 2009, as both the EU and NATO in close succession acknowledged that cyber threats were rapidly increasing in numbers and sophistication, up until 2020 as this includes the most recent progress report on the implementation of the *Joint Declarations.*

To embark on this analysis, I draw on secondary empirical material such as official political documents and statements by the EU and NATO including related expert opinions, scientific journals, and reports from IT companies, and non-governmental groups. The search was conducted on sites such as the EU's main website's in-site search engine, EUR-Lex (The European Union Law online library), the EU ISS (Institute for Security Studies), NATO's main website's in-site search engine, NATO's Multimedia Library, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Google Scholar, Microsoft Academic, and CORE. In addition, the University of Southern Denmark's online library was used as it provides access to academic work through databases such as Taylor & Francis Online, Oxford University Press, SAGE Journals, JSTOR, and Cambridge Journals.

The literature used in the analysis has been screened using specific search terms prior to selection, which are outlined below. The use of such search terms both brings structure to the collection of data and ensures that the data represents the key concepts of the research question. The search terms used in this thesis have thus been selected to support the research question and are semantically related, for example 'cyber deterrence' instead of 'IT deterrence', see the section below. For the same reason, certain search terms, for example ‘IT’, ‘Network’, and ‘Computer’ were not included, as this would have resulted in literature not relevant to the research question. Consequently, the prefix ‘cyber’ has been added to avoid a too wide search, and unintended irrelevant search results. For example, if the prefix had not been added to ‘deterrence’ this would have resulted in material focusing on non-cyber related deterrence strategies and challenges, and the process of finding relevant literature would have become extremely time consuming. It should be noted, that by adding the prefix ‘cyber’, there is a chance that some relevant texts may have been excluded. Nonetheless, when weighed up against the time consuming task of sorting relevant from irrelevant literature, this option seemed most appropriate.

4.1. Search terms

The following outlines each step, including which search terms, search engines and databases were used to collect literature for the subsequent analysis. It should be noted that since the thesis’ analysis is contingent on official versions of what is perceived as a threat and based on official framing of threats based on empirical documents and statements, I acknowledge that certain strategic aspects cannot be included, as they, due to their classified nature, are not disclosed to the public. The data collection and subsequent analysis are therefore affected by the level of openness and detail in the EU and NATO documents and statements.

In each of the first, second and third steps, a twofold search strategy was chosen aimed at obtaining secondary literature such as strategies, statements and reports made by the EU and NATO as well as commentary to these by academics, expert within the field, etc. Firstly, an exploratory search was conducted to gain an initial understanding of the scope of the issue. Secondly, based on the findings from the exploratory search, key words were developed. Thereafter, a systematic search using the key words was conducted.

This search strategy was conducted as an exploratory search to gain an initial understanding of the scope of the issue. Moreover, it facilitates a comparative analysis between documents and to create a similar base for the analysis.

The exploratory search for the first and second step were conducted using the following search terms, including an ‘EU’ and ‘NATO’ prefix respectively: ‘cyber security’, ‘cyber threats’, ‘cyber actors’, ‘cyber threat actors’, ‘cyber defense’, ‘cyber defense cooperation’, ‘cyber defense approach’, ‘cyber defense strategy’, ‘cyber security’, ‘cyber security cooperation’, ‘cyber security approach’, cyber security strategy’, ‘cyber deterrence’, ‘cyber deterrence strategy’.

The third step used slightly different search terms in order to explore the EU and NATO partnership: 'EU-NATO Joint Declaration', 'EU-NATO cyber security', 'EU-NATO cyber security cooperation', 'EU-NATO cyber defense cooperation', 'EU-NATO cyber cooperation', 'EU-NATO cyber security agreement', 'EU-NATO cyber defense agreement', 'EU-NATO cyber cooperation agreement', 'EU-NATO cyber deterrence'. The third step aims at examining whether or not the *Joint Declarations* conceptualizes threats and actors similarly or differently than the findings in the first two steps. The third step leads to the second part of the thesis, which seeks to analyze *why* the *Joint Declarations* was seen as the next rational step for the EU and NATO in making cyberspace more secure. This part will, through a comparative analysis of the findings in the second and third step, discuss the conceptualization of threats and actors in cyberspace as well as the concept of deterrence in the *Joint Declarations* and how it fits into the current deterrence paradigm.

4.2. Qualitative coding

To analyze the empirical textual data, I chose to qualitatively code the selected texts. This enables a breakdown, or 'fracture', of the data (Strauss, 1987, p. 29). Initially, the coded data is rearranged into categories that facilitate a comparison within - and between - these categories that form the basis for the analysis as a whole (Maxwell, 1996, p. 78-79). The coding throughout the three steps were conducted using abductive reasoning. The abductive approach is best understood as a dialectic combination of the deductive and inductive approaches (Beach and Pedersen 2013, 19). The abductive approach was chosen, as this focuses on discovering new concepts, ideas and explanations by finding surprising phenomena, data, or events that cannot be explained by pre-existing knowledge (Kennedy 2018, 52). The abductive approach differs from the deductive and inductive approach by not initially being aimed at developing theory but rather to focus on the context that triggered the event and does need not to follow a series of steps in a predetermined order. Through the abductive approach, I, as a researcher, aspired to continuously employ an analytical-selectivity mindset to examine how the data support existing theories or hypotheses as well as how the data may call for modifications in existing understandings. Moreover, this approach facilitated a constant move back and forth between data and theories thus enabling comparisons and interpretations in search for patterns (Ibid, 52). Ultimately, it enabled central themes and sub-themes to be identified in step two and three. The themes are: (i) Threat type and (ii) Threat actor. Each theme will include their own sub-themes, see Figure 2.

Threat type[4]	Threat actor
Malware	States
DDoS	State-sponsored groups
Ransomware	Terrorists
Espionage	Hackers
Cybercrime	Organized cybercriminals
Botnets	Hacktivists

Figure 2 – Threat type and actor

4.3. Ontology and Epistemology

While I draw on elements from both realism and liberalism for the analysis, the basic ontological and epistemological approach is based within the realm of critical realism, as it focuses on making sense of changes that can be observed in social entities, such as organizations, people and relationships (Easton 2010, 120; O'Mahoney and Vincent 2014, 7). Critical realism is thus seen as particularly applicable to making sense of changes that can be observed in interorganizational relationships or nets of connected organizations. This is because of the way critical realism interprets social phenomena by analyzing the associated events that take place as a result of the actors acting, whether they are human or non-human (Easton 2010, 120-123), such as that between the EU and NATO. Critical realism is thus well suited for case studies regarding organization and interorganizational relationships why I draw on critical realism in the analysis to answer the overall question, "what caused the events associated with the phenomenon to occur?" (Ibid, 123; O'Mahoney and Vincent 2014, 7).

Choosing to draw on critical realists means that I ascribe to an ontology that assumes that there exists a reality independent of observers (Ibid, 120; Sayer 2000, 2; O'Mahoney and Vincent 2014, 3-4). In this, I follow the argument that the causal forces, which researchers' study, from gravity to social structures must also exist as real ontological forces. Only by accepting this, it is possible to explain why and how processes around us work as they do (Ibid, 9; Maxwell 2011, 5; Milja 2007, 364-365). Following Aristotle's notion that "nothing comes from nothing", critical realists believe that events, processes, objects, and agents are shaped by pre-existing causal context. However, as critical realists believe that causes are often unobservable, they need to be uncovered through a deep ontological inquiry, which involves conceptualization of the nature of the unobservable structures

[4] Note: Not full list of threat type. See p. 37 for full list.

that lie beneath observable patterns. In relation, a perception of causal factors within critical realism often includes a variety of ontological factors, for example: material resources, social structures, social rules and norms, and discourses (Ibid, 365-366; Sayer 2000).

Epistemologically, in line with critical realisms acceptance of the world as socially constructed - to a certain extent, I acknowledge that I *interpret* rather than *construct* the world. Thus, this understanding also comes with an acknowledgement of how social phenomena are intrinsically meaningful and that meaning is not only externally descriptive of them, but also constitutive of them. Relationally, it must be noted that critical realists are aware that material constituents play a part too. Critical realists argue for a stratified rather than flat ontology, meaning that within critical realism, three overlapping domains of reality exist: the empirical, the actual and the real (Bhaskar 2008). I understand the empirical domain as where observations are made as well as experienced by observers. An 'actual' domain is hence both where events take place, and how they are experienced by actors herein. However, events that occur in the actual domain may not be observed at all or may be understood differently by the observers. Lastly, the 'real' domain is wherever the process of interpretation happens as events occur from mechanisms that operate in this domain. When ascribing to a such an understanding, inspired by critical realists, I view this domain as the most important. They recognize that knowledge obtained through research is, per default, fallible because it is unlikely to reveal any intricate social reality. This represents the criticality; for researchers to collect data that helps to distinguish other alternative explanations in order to understand the mechanisms of the real domain (Easton 2010, 123). Consequently, my analysis will take place in all three domains to explain how threats in cyberspace have been experienced by EU and NATO as observers but also how they have experienced the threats as actors. This subsequently leads to an analysis of how they have interpreted and acted on the threats.

4.4. Analytical tools

In order to answer the research question, the three separate but mutually dependent and supporting steps, need to be analyzed. This will be conducted using several analytical tools. Each of the steps relies on one or more of the analytical tools, which are presented in the following section.

4.4.1. Document analysis

In the thesis, document analysis is used to examine and interpret data from documents such as NATO Summit Declarations, EU strategies, the *Joint Declaration*, and academic journals (i.e. chapter 2).

Conducting document analysis on such literature, allows me to extract meaning, gain understanding, and develop an empirical understanding. Document analysis is well-suited as a qualitative research method as the essence of it revolves around creating detailed knowledge of a single phenomenon, in this thesis' case the reasons behind the *Joint Declaration*. For that same reason, it is suitable to qualitative single case studies (Bowen 2009, 27-29; 34). In addition, document analysis is an unobtrusive and nonreactive research method, meaning that it does not interfere with the subject being analyzed (Ibid, 38; Prior 2008, 231). Since document analysis does not conduct direct observations and interacting directly with the actors, researcher's personal biases are minimized, but it will arguably still occur.

I draw on Bowen's (2009) method in which he argues that document analysis can be used as a complement to other qualitative research methods as this facilitates a 'triangulation', meaning to combining methodologies in the study of same phenomenon. This ultimately means that I am provided with the ability to corroborate findings across data sets and thus reduce the impact of potential biases that can exist in a single study (Bowen 2009, 28-29). Additionally, through document analysis it is possible to recognize emerging themes within the data, which is relevant for this thesis, as this might provide insights as to why the two organizations decided to increase their cooperation in cyberspace. By conducting a careful analysis of the selected data and performing coding and category construction, based on the data's characteristics, I can uncover themes pertinent to the phenomenon at hand (Ibid, 32).

I also acknowledge the limitations of document analysis. One of these, Bowen refers to as an "incomplete collection of documents", suggests that a biased selectivity exists. If one relies solely on document analysis, this can potentially become a fallibility, as this method is dependent on availability and accessibility of data (Ibid, 32). The source richness can prove another pitfall of document analysis. As Bowen states, researchers must critically assess documents and be cautious about using them in their studies, as documents are not necessarily precise, accurate, or complete recordings of occurred events. Additionally, it is crucial that I as a researcher assess the document's authenticity, credibility, accuracy, and representativeness, along with a consideration of the original purpose of the document—the reason it was produced—and the target audience (Ibid, 33). Consequently, Bowen states that document analysis is not simply a matter of "lining up a series of excerpts from printed material to convey whatever idea comes to the researcher's mind.". Rather, it a full process of evaluating documents and thereby create empirical knowledge and understanding (Ibid, 34).

4.4.2. Textual analysis

Additionally, the thesis employs textual analysis, which, in a sense, lets the data "speak" for itself. This means that documents as those stated in the section above, will not be subject to and attributed a 'correct' interpretation. As a qualitative method, it is instead used to identify possible and most likely interpretations. Even though texts can have a semantic instability, meaning that they can have multiple and different meanings, it does not mean that readers are free to make a text mean whatever they wish. According to Lockyer (2008), a text's meaning originates in its codes, genre of the text, and its social, cultural, historical, and ideological context. Combining these will give a preferred understanding of the text. Accordingly, a key element of textual analysis is to examine the interconnections of meanings of the text, referring to the rhetorical context, specific textual characteristics, and any wider context of the text (Lockyer 2008, 865-866). Lacity and Janson (1994) add that by ensuring that the researcher is an outsider, meaning one who cannot interact with the originator of the text because the author's ideas are sufficiently expressed by the text, the researcher will interpret the text through semantics and not by personal biases and experiences (Lacity and Janson 1994, 138). Moreover, texts contain nonrandom variations, which implies that frequency is an indicant of importance. The more a phenomenon occurs, the more likely it is nonrandom and thereby important. Relationally, Lacity and Janson state that the text's understanding arises through the identification of nonrandom variation and in order to uncover these, researchers must construct a category system and code the data to test hypotheses about the relationships among variables of interest (Ibid, 139).

A potential challenge with textual analysis is the risk of 'cherry picking' in which one simply selects the examples that support one's research the best while ignoring poorer examples. It is often an unconscious action by the readers caused by his or her expectation of the text. This ultimately "forces" the reader to search for specific content supporting his or her expectations and can influence the reader into deselecting content not supporting one's expectations. If the reader solely relies on content that supports selected theories, the conclusion runs the risk of becoming faulty (Aarhus University n.d., 2-3).

4.4.3. Comparative analysis

The final analytical tool this thesis employs is comparative analysis. Comparative analysis can be done between different entities, such as individuals, groups, or organizations, or at different points in time. These entities or time periods are then analyzed to isolate prominent similarities and differences

(Mills 2008, 101). This is done in step 3 of this thesis, when the findings from step 1 and 2 are compared to each other. Moreover, I argue, that comparative analysis is a good fit to case study research, as it can be used to compare a particular case with that of a hypothetical frame of reference to highlight differences (Ibid, 101). Comparative analysis is particularly well-suited for this thesis, as it involves taking one entity or piece of data, such as a statement or a theme, and comparing it with others to identify similarities or differences. Subsequently, it is possible to develop a conceptual model of the possible relations between various entities (Ibid, 101-102).

According to Bowen (2009), by using analytic tools that are complimentary to each other a 'triangulation' becomes possible, in other words, to combine methodologies in the study of the same phenomenon. This ultimately provides me as the researcher with the ability to corroborate findings across data sets and thus reduce the impact of potential biases that can exist in a single study (Bowen 2009, 28-29).

5. Cyberspace in an EU security framework

With the aim of analyzing EU's cybersecurity and deterrence postures, the following chapter examines how the cyber threat landscape is described in strategies, statements, reports, and legislation by the EU, as well as relevant academic work (see appendix 1). The findings from this chapter will subsequently be used to elaborate on the research question and the reasons for the EU and NATO to enhance their cooperation with the signing of the *Joint Declarations.* While understanding how the EU perceives the current state of cyber threats, divided in threat types and threat actors, is useful to form a foundation of knowledge regarding which threats are viewed as urgent and how. This first step needs to be expanded in order to further analyze EU's cybersecurity and deterrence postures. Thus, this part of the analysis is followed by an examination of the EU's cybersecurity conceptualization and deterrence strategies by analyzing four EU cybersecurity strategies relevant to this thesis. This enables the thesis' analysis to further establish an understanding of how and the EU counters cyber threats strategically and on what basis. Finally, the findings and reflections from the first two parts of the analysis in this section are discussed in the context of the concept of the cybersecurity dilemma.

5.1. Cyberspace and the EU's cyber threat landscape

Cyberspace has changed the world immensely as interaction transcends physical borders, thus changing the landscape of politics. It has become a sphere of disruption, conflict and geopolitical rivalries (European Commission 2009, 3; European Commission 2018, 7; European Parliament 2019, 1). Cyberspace has become an integral element of the EU's economy and society (European

Commission 2009, 3; European Commission 2016, 10). However, this has not been without challenges, and it has come to a point where the EU's digital walls are constantly under attack from both states and non-state actors (Pawlak 2018, 103). Malicious activities against the networks of EU institutions and Member States seem to have become the new normal in which an example was the 2017 ransomware attack 'NotPetya' (Ibid, 104). On this background, scholars have noted that attacks of this type has made the EU aware that it is necessary to adapt to this new reality and take more proactive approaches to counter as well as prevent cyber threats (Tiirmaa-Klaar 2018, 23). Moreover, according to a European Court of Auditors' report from 2019, the financial impact of cyberattacks continues to grow, which has created a disparity between the cost of launching an attack and the cost of prevention, investigation and reparation. They state that, a DDoS[5] attack can cost as little as €15 to carry out, while the losses and reputational damages suffered are considerably higher (European Court of Auditors 2019, 9).

Combined with the EU's gradual development into a global diplomatic and security actor (see also section 7.3), this new threat landscape underlines the need for the EU to develop specific cybersecurity strategies and tools to protect both its institutions and Member States (Renard, Thomas and Barrinha 2018, 181; European Commission 2016, 10). Such measures must counter the technological vulnerabilities inherent in globalization and the common market, which the EU with its digitalized economy and increasingly open and interconnected society is ever more dependent on (European Commission 2009, 3; Gressel 2019, 2). Cybersecurity as a policy area is therefore paramount for the EU (European Parliament 2017, 25). Nonetheless, compared to traditional security, the threats in cyberspace are more difficult to counter. They are complicated due to the attributional issues, the lack of geographical boundaries, the speed of which technological developments takes place and the lower cost of tools to conduct attacks (European Commission 2009, 6).

According to the EU, the same norms, principles and rights that the EU upholds in the physical world is also applicable to cyberspace. The EU's cyber interests therefore seemingly follow its core values, such as freedom, democracy and the rule of law (European Union 2020, 1). An element of the EU's conceptualization of cybersecurity is thus the promotion of the EU's core values, such as peace and security, prosperity, democracy and a rules-based global order, to cyberspace. The EU's core values

[5] DDoS attacks particular internet sites, servers, or routers with more requests for data than sites can respond to or process. This effectively shuts down the site thereby preventing access or usage until the 'flooding' is stopped or the attackers separate (Valeriano and Maness 2014, 353-354).

are consequently guiding factors when the EU adopt cybersecurity policies (European External Action Service 2017, 13; ENISA 2017, 4; Giantas 2019, 9).

Moreover, as cyberspace is highly interconnected and interdependent with other infrastructures, cybersecurity and resilience must not be ensured purely by national or potentially uncoordinated approaches (European Commission 2009, 6). The EU conceded that without their assistance to its Member States in increasing their overall cybersecurity level, the Member States would either not raise their cybersecurity level sufficiently or risk that they acted individually or through bilateral or regional agreements. This would result in too different and uncoordinated agreements, ultimately proving insufficient (European Commission 2009, 14).

The EU therefore began implementing several initiatives, for example the policies *An Open, Safe and Secure Cyberspace* (European Commission 2013), *Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU* (European Commission 2017a), *Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union* (also known as the 'NIS') (European Parliament 2016) and lastly the *Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (*also known as the *Cyber Diplomacy Toolbox)* (Council of the European Union 2017). The two latter initiatives build on the progress previously made but also bring new focal points. Common for these are their aim at increasing cyber resilience of EU institutions and members states and building capabilities (European Commission 2009, 6; European Commission 2016, 10; European Commission 2018, 1; Pawlak 2018, 103) as well as decreasing the level of fragmentation of cybersecurity policies within the EU (European Commission 2016, 3; Carrapico and Barrinha 2017, 1260; Darmois and Schméder 2016, 12). However, it is worth noting that even though cybersecurity is a fundamental element of the EU, strengthening its resilience to deter threats is predominantly up to each member of the EU (European Commission 2009; European Commission 2018, 1; Pernik 2014, 1). The role of the EU and its institutions, such as the European Network and Information Security Agency (ENISA), is solely supportive in nature. Operational cyber defence, in practice and on paper, remains the purview of Member States, while ENISA raises awareness, supports policy development and facilitates capacity building at the EU and state level (Scheffer 2018, 38).

While it remains clear that the EU members are responsible for their own cybersecurity, the low level of cybersecurity in some Member States has the potential to increase the vulnerability of others and thus the EUs security level as a collective whole. Accordingly, the EU recognized that without common policies on cybersecurity, increasing the EU's overall cybersecurity level would be difficult (European Commission 2009, 7-8; European Commission 2017b, 12). The EU thus plays a critical role in creating the conditions for its members to improve and increase their capacities, for them to work together and generate trust (Council of the European Union 2014, 7; European Court of Auditors 2019, 20). Trust between Member States and of the EU level policies, equals better and more effective communication and implementation, which ultimately increases the EU and its Member States' cybersecurity (European Parliament 2017, 26). However, trust can be one of the biggest barriers to overcome and a lack thereof can lead to a lack of sharing information and a disengagement from the EU-level policies, which eventually can lead to a less effective cybersecurity and weak deterrence posture (Ibid, 26). Moreover, given the wide differences among the Member States in terms of capacity and engagement, the provision of sensitive national security information will remain voluntary (European Court of Auditors 2019, 20; Cirlig 2014, 8).

In order to increase the EU's internal cybersecurity, the EU has also envisioned a strong public-private partnership, as they believe that cooperation and information-sharing between Member States, EU institutions, the private sector and civil society can foster a common cybersecurity culture as well as increase resilience and deterrence (European External Action Service 2017, 22). According to the European Parliament (2017), cooperation with the private sector makes sense since they deliver, in whole or in part, many of the critical services which society depends on. Additionally, due to their expertise, the EU views cooperation with the private sector as valuable, as including them in amending and revising national strategies and regulations, can potentially lead to a reduced cybersecurity risks and better protection of critical infrastructures (European Parliament 2017, 28).

From the analysis above, it has become evident that parallel with the development of cyberspace into a global community transcending physical borders, costly attacks against the EU have become the new normal (European Commission 2009, 3; European Commission 2018, 7; European Parliament 2019, 1). For the EU, with its digitalized economy and interconnected societies, cyberspace has become an integral element of its existence (European Commission 2009, 3; European Commission 2016, 10), why it is crucial to counter the technological vulnerabilities inherent in globalization (European Commission 2009, 3; Gressel 2019, 2). Consequently, as the EU's is evolving into a global diplomatic and security actor the EU need to develop cybersecurity strategies and tools to protect its institutions and Member States (Renard, Thomas and Barrinha 2018, 181; Scheffer 2018, VI;

European Commission 2016, 10). This development, I argue, has arguably affected the EU's conceptualization of cyberspace. To further identify how these emerging challenges have affected the EU's understanding of threats in cyberspace – and how to accommodate those most efficiently – four relevant EU cybersecurity strategies are analyzed in the sections below.

5.1.1. Threats

In Figure 3 below it is depicted how the threats in cyberspace are perceived in EU strategies, statements, reports and legislation, as well as academic work on cyber threats towards the EU. These were selected based on the search terms (see section 4.1 on p. 26), thereby ensuring their relevance for shedding light on the EU's cybersecurity policies and cyber threat landscape conceptualizations. Moreover, these facilitate the later analysis of the EU's perception of a cybersecurity dilemma, which ultimately assists in answering the research question. The threat categories below are illustrated based on the number of times they were mentioned in the 30 articles selected for this analysis, see appendix 1. I acknowledge, that despite a specific threat type is mentioned more than another, it does not necessarily mean that it is more severe. It is, however, an indication of what it pertinent in the EU's public strategic documents and in academic work relating to cyber threats towards the EU.

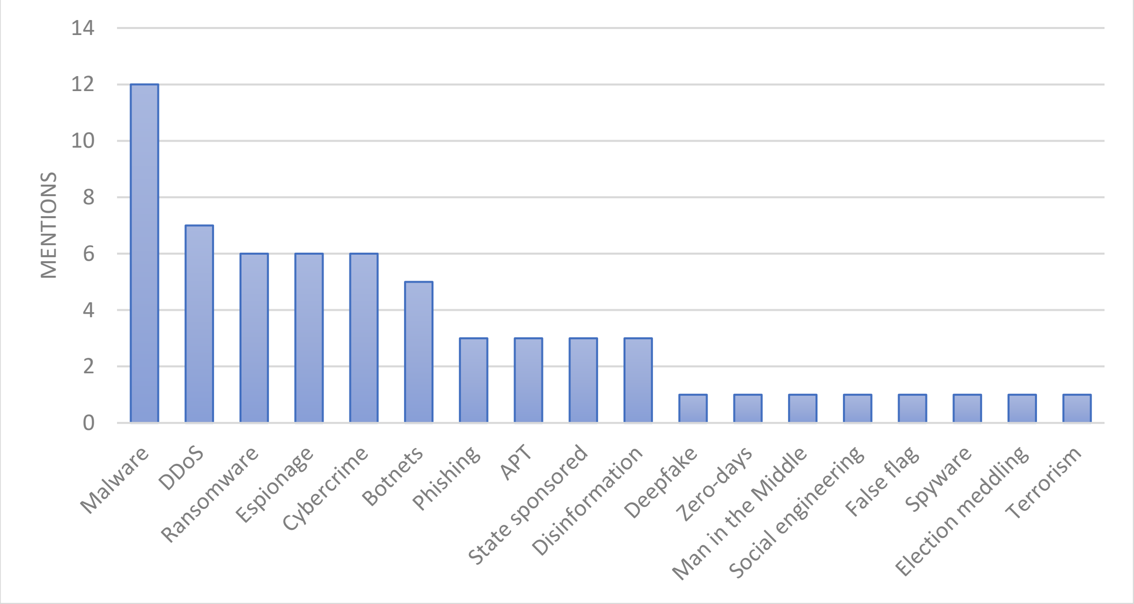

Figure 3 – Cyber threat types as perceived by the EU

A notable observation is the how the EU perceives 'espionage' and 'phishing'. The former is placed in the higher end while the latter in the lower end. A reason why 'espionage' receives as much focus as it does, might be because the illegality of espionage is not well established. According to the *Tallinn Manual 2.0 – On the International Law Applicable to Cyber Operations*, cyber espionage is not per se prohibited by international law (Schmitt 2017, 169). Furthermore, they recognized that cyber espionage operations can be challenging for a target state to distinguish from offensive cyber operations, since both entail system penetration by method such as malware. In addition, should the target state discover the malware, it may have difficulty to ascertain its precise function. Consequently, technical realities like this contribute to the risk that an act of cyber espionage will be misinterpreted as another type of activity, such as a cyber use of force (Ibid, 172-173). A possible reason for 'phishing' being placed in the low end, might stem from the EU's consideration that they possess a high level of 'cyber hygiene'. 'Cyber hygiene' is a fundamental principle relating to cybersecurity and refers to establishing simple routine measures to minimize the risks from cyber threats. According to a 2016 ENISA report, 'cyber hygiene' practices are well established in almost all EU Member States (ENISA 2016, 14).

5.1.2. Actors

In Figure 4 below it is depicted what the selected EU strategies, statements, reports and legislation, as well as academic work, perceive as actors towards the EU in cyberspace. The actors in Figure 4 are illustrated based on the number of times they were mentioned in the 30 articles, see appendix 1, selected for this analysis based on their relevance in answering who the EU and experts within the field perceive as the main actors, which forms the basis for further analysis. The actors are subsequently discussed in the context of the previously described concept of cybersecurity dilemma.

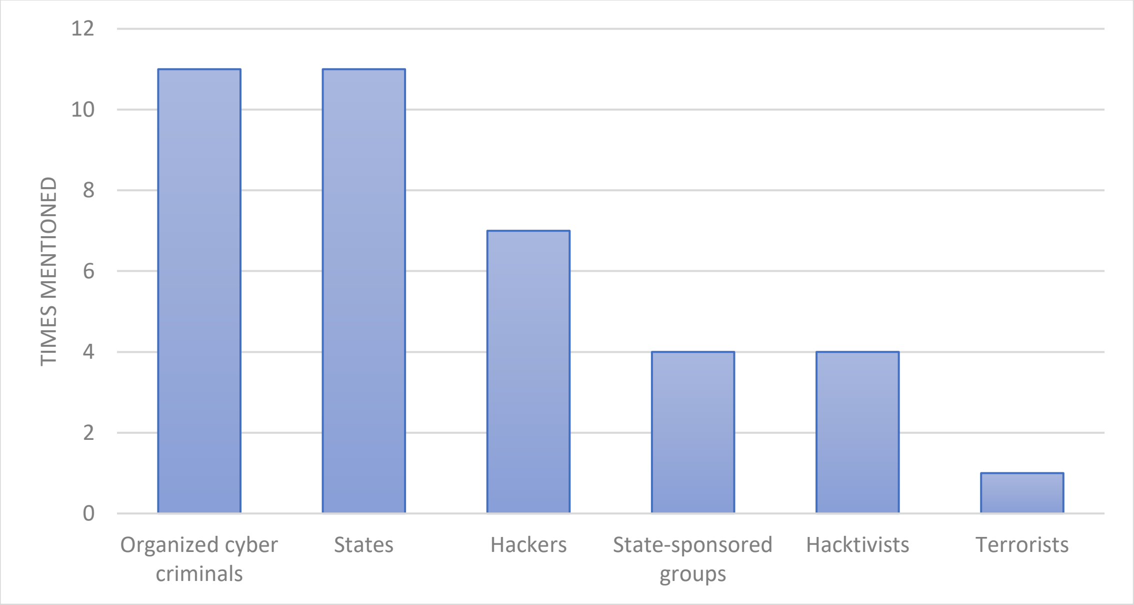

Figure 4 – Cyber threat actors as perceived by the EU

The EU's dual focus on organized cyber criminals stems from its first cyber strategy called *An Open, Safe and Secure Cyberspace*, which pointed out five overall strategic priorities, one of which was to drastically reduce cybercrime (European Commission 2013, 4). However, in past years, the EU's focus has shifted towards states, as evident in the EU's 2017 *Cyber Diplomacy Toolbox*, which was prompted by the EU's concern about the increased ability and willingness of states to undertake malicious cyber activities (Council of the European Union 2017, 3).

5.2. EU cybersecurity strategies

In the preceding sections, the EU's perception of cyberspace and the cyber threat landscape has been examined. In the following section, four influential and important EU cybersecurity strategies will be analyzed. These were developed to counter the cyber threat landscape, to introduce the EU's core values, such as fundamental human rights, democracy and the rule of law to cyberspace (European Commission 2013, 2) and to ensure that the EU would continuously prosper from cyberspace (European Commission 2017a, 2).

The four strategies, the 2013 *An Open, Safe and Secure Cyberspace* (European Commission 2013), the 2016 *Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union* (also known as the *NIS Directive*) (European Parliament 2016), the 2017 *Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU* (European Commission 2017a) and lastly the 2017 *Cyber Diplomacy Toolbox* (Council of the European Union 2017), will be analyzed. Each of them represents pivotal strategy implementations for the EU. In short, they show that the EU's initial attitude in 2014 was predominantly defensive, whereas by 2019 the EU had become much less defensive, though not truly offensive. It furthermore shows that the EU's approach has transformed into a blend of soft and hard power, as it deploys security and defence instruments alongside development cooperation, diplomacy and sanctions (European Commission 2017b, 6). This combination of soft and hard power evokes questions of smart power.

Through the 2013 cybersecurity strategy, *An Open, Safe and Secure Cyberspace*, the EU began implementing incentives for creating cyber defence capabilities within the EU (Scheffer 2018, 34). In this strategy, the EU stresses the need to act now, as they underline the fact that the evolution of malicious tools has happened faster than the evolution of defensive tools, and that it is impossible to combat advanced offensive tools with outdated defensive tools (European Commission 2013, 9). The deterrence posture of the strategy is clearly shown, as it highlights the development of defensive cyber tools, such as increased resilience, detection, response and recovery (Ibid, 11). The strategy sets out five main strategic priorities for the EU in cyberspace; (i) achieving cyber resilience, (ii) reducing cybercrime, (iii) developing cyber defence policies and capabilities, (iv) develop the industrial and technological resources for cybersecurity and (v) to establish an international cyberspace policy aligned with core EU values (European Commission 2013, 4-5). The strategy clearly depicts that the EU relies on deterrence by denial, as it focuses on defensive capabilities such as resilience and recovery and not on offensive capabilities. Moreover, the EU state that it perceives that the rights and privileges enjoyed in the real world apply to cyberspace, "[…] the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace." (Ibid, 2). In relation, the strategy sets out a need for an increased cooperation with the private sector, as they "[…] owns and operates significant parts of cyberspace and so any initiative aiming to be successful in this area has to recognize its leading role.". To accomplish this, the EU views itself at an exalted level coordinating and planning while the EU Member States, and to a certain degree the private actors, are the ones dealing with security challenges in cyberspace (Ibid, 4-5). Additionally, the EU in the strategy envisioned a closer cooperation with NATO, arguing that the EU and NATO's protective approaches would not duplicate each other but rather compliment their efforts to heighten the overall cyber resilience level (Ibid, 11).

The *NIS Directive* adopted by the EU in 2016 was the first EU-wide cybersecurity legislation. It aimed at increasing cybersecurity capabilities across the EU Members States (European Parliament 2016; Tiirmaa-Klaar 2018, 18; Scheffer 2018, 39). It is important to notice, that since this is a Directive, it is binding on the Member States, which means that the EU ensures that its visions for increasing cooperation and cybersecurity must be followed by each Member State. It can thus be interpreted as the EU's minimum standards for its Member States regarding cybersecurity and as a cornerstone of the EU's cybersecurity (European Parliament 2016; European Commission 2018, 8; Giantas 2019, 18). Moreover, by establishing a 'Cooperation Group' consisting of Member States, ENISA and the European Commission, the directive aims at increasing EU- and national-level cooperation which ultimately should enhancing mutual trust and confidence (European Parliament 2016).

The 2017 strategy, *Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU* (European Commission 2017a), built on the foundation established in the 2013 strategy

(European Commission 2017a, 3). Accordingly, the 2017 strategy reiterates the cruciality of cybersecurity for the prosperity and security of the EU and its Members. Moreover, it states that cyberattacks are becoming more diverse in term of actors, means and goals (Ibid, 2). While the strategy sustains the focus on resilience as put forth in the 2013 strategy, it acknowledges that because of the continuously evolving and deepening threat landscape in cyberspace, the EU must do more to withstand and deter such attacks in the future (Ibid, 3). The strategy therefore proposes three new areas of increased focus: (i) building resilience to cyberattacks based on a collective and wide-ranging approach (Ibid, 3), (ii) creating effective cyber deterrence by putting in place credible measures to dissuade criminals and hostile states (Ibid, 12-13), (iii) strengthening international cooperation to promote global cyber stability (Ibid, 18).

Additionally, the strategy calls for an increased focus on streamlining policies (Ibid, 7), which has been, and continues to be, a challenge, as the lack of a coherent cybersecurity framework hinders the EU's ability to respond to and limit cyberattacks (European Parliament 2011, 29; Council of the European Union 2014, 6; European Commission 2017a, 3; European Court of Auditors 2019, 29). This challenge is most likely enhanced due to the complexity of the EU's operational setup (European Parliament 2017, 9; Christou 2014, 4), which arguably is enhanced due to the large number of actors dealing with cybersecurity within the EU, which according to ENISA amounts to 22[6].

In 2017, as the EU adopted the *Cyber Diplomacy Toolbox*, it shifted from its previous defensive posture to a more aggressive one, since a considerable element of the framework is the EU's attempt to signal willingness to punish malicious cyber activities (Moret and Pawlak 2017, 1), which can be interpreted as a shift from solely relying on deterrence by denial to a combination of both deterrence measures. According to the EU, the framework was adopted due to their "[…] concern about the increased ability and willingness of states and non-state actors to pursue their objectives by undertaking malicious cyber activities of varying in scope, scale, duration, intensity, complexity, sophistication and impact" (Council of the European Union 2017, 3; Moret and Pawlak 2017, 1). Prior to the EU adopting the framework, only the United States had used cyber sanctions, which was against North Korea in response to the country's alleged involvement in the cyberattack on Sony Pictures in 2014 (Ibid, 2). The use of sanctions as a strategy is nonetheless not new to the EU. According to Moret and Pawlak (2017), the EU's use of sanctions had trebled over the past decades as policymakers find it an attractive option at a time when diplomacy has reached its limits

[6] Also see https://www.enisa.europa.eu/cybersecurity-institutional-map/results

(Moret and Pawlak 2017, 2). Relationally, the EU cyber sanction framework is based on already established EU sanctions legal framework, meaning that even though the sanctions might be different, the mechanisms and decision processes behind them are not (Ibid, 2; Council of the European Union 2017, 5). However, two important elements were not mentioned in the framework: (i) the criteria for implementing cyber sanctions and (ii) which types of sanctions can actually be made. Without these, the framework arguably does not possess credibility and subsequent ability to deter potential adversaries from conducting malicious cyber activity. In the framework, the EU acknowledges its attempts to increase its own institutions and EU Member States' resilience through its previous frameworks but argues that these are not sufficient enough anymore (Council of the European Union 2017, 4; Council of the European Union 2018, 6). The EU states that it is necessary to implement restrictive measures that can be used to strengthen the EU's response to activities that harm its political, security and economic interests (Ibid, 6; European Commission 2018, 8; Council of the European Union 2017, 4-5). Put in other words, the EU recognized the need to rely on deterrence by denial and punishment along with soft and hard power tools.

The first substantial addition to the *Cyber Diplomacy Toolbox* came in 2019 when the EU adopted the *Council Decision Concerning Restrictive Measures Against Cyber-attacks Threatening the Union or its Member States* which provided much needed criteria and sanctions guidelines missing in the 2017 framework. The Council Decision set forth a two-step assessment process to determine if a cyberattack causes sufficient damage to the EU or its Member States to commence the process of implementing cyber sanctions (Council of the European Union 2019, 4). Firstly, a cyberattack must constitute an external threat to critical infrastructure, which are essential for Member States', for example areas of defence, governance and the function of institutions, including those used for elections or the voting process. Additionally, it applies to services necessary for the maintenance of essential social and/or economic activities, for example energy, health, banking and financial market (Ibid, 7), which are similar areas of interest as in the *NIS Directive* (European Parliament 2016). Relationally, external threats refer to any carried out or which use infrastructure outside the EU. But it also includes attacks, which are carried out with the support, at the direction or under control of any natural or legal person, entity or body operating outside the Union (Council of the European Union 2019, 6). Secondly, an attack must be assessed based on its scope, scale, impact and severity of disruption caused to economic and societal activities. This will include the number of persons, entities, bodies and Member States affected, as well as the amount of economic loss caused and, relationally, the amount of economic benefit, data, or commercial sensitive data, gained or accessed by the perpetrator (Ibid, 9-10). If these criteria are fulfilled, the EU can impose two types of sanctions: (i) asset freeze, in which all funds and economic resources belonging to, owned, held or controlled by the sanctioned persons, entities, bodies can be withheld (Ibid, 13) and/or (ii) an entry and transit travel ban (Ibid, 10). Accordingly, both measures target the "natural or legal persons, entities or bodies that are responsible, provide financial, technical, or material support, or are otherwise involved in the cyberattacks" (Ibid, 10-13).

Ultimately, the *Cyber Diplomacy Toolbox* and the 2019 addition both follow the shift in the EU's perception of cyberspace towards a more offensive interpretation of cyberspace and with it the activities the EU can and should conduct within this realm. In 2014, the EU acknowledged in their first *EU Cyber Defence Policy Framework* that some (the EU did not mention any state or organization by name) perceived cyberspace as a new domain of military activity, yet the EU did not comment on their own perception of it (Council of the European Union 2014, 2). Then, in 2018, when the EU adopted an updated version of the EU Cyber Defence Policy Framework, they clearly stated that they now perceived cyberspace as a new domain of military activity (Council of the European Union 2018, 2).

The challenges and countermeasures described above indicate, to an extent, how the EU is affected by the cybersecurity dilemma. Even though the EU itself does not refer to an existing or emerging cybersecurity dilemma, they hint at it a few times. In 2009, the European Commission published a working document titled *Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience* in which they portrayed the future of cyberspace very grim. They stated that malware, botnets and phishing were becoming the normality of cyberspace and that cyber infrastructure are under constant attack. Accordingly, this means that if Europe does not prepare itself, impacts from large scale attack will be severe (EU Commission 2009, 6). In this case, the EU will arguably begin to enhance their defensive capabilities. Accordingly, it is therefore essential that the EU continue their level of transparency in order for others to recognize what they are doing and to distinguish them from offensive capabilities in order to avoid a security dilemma from happening.

Additionally, the European Parliament stated in 2017 that the lack of trust on the EU-level and the supranational level causes a disengagement from the EU level policies and a scarcity in information sharing, ultimately leading to a weaker deterrence posture (European Parliament 2017, 26). The disengagement from the EU level agreements means that countries might circumvent the

EU and establish bilateral or multilateral deals on cybersecurity. France, Spain and Portugal have all launched bilateral cyber dialogues with Russia with the aim of halting any malicious cyber activity originating from Russia against their respective countries. These might prove fruitful for the three countries, but it carries the potential to ruin any pan-EU response or strategy (Gressel 2019, 8).

5.3. Sub conclusion

As shown in the section above, the EU's cybersecurity approach prior to 2014 was predominantly defensive and relying solely on soft power (Carriço 2017, 335-337; Darmois and Schméder 2016, 16). However, through implementation of the *Cyber Diplomacy Toolbox* and the *Council Decision Concerning Restrictive Measures Against Cyber-attacks Threatening the Union or its Member States* the EU's approach became less defensive and implemented hard power measures. Until the implementation of the *Cyber Diplomacy Toolbox*, the EU's approach was mainly legalistic and protective. It concentrated on fighting cybercrime and increasing resilience to ensure rapid recovery from cyberattacks (Darmois and Schméder 2016, 16). The EU's conceptualization of cyberspace also changed in accordance with the cybersecurity approach. This is evident in two statements, the first in 2014 as the EU stated that "[…] others see cyber as new domain" (Council of the European Union 2014, 1) to 2018 and 2019 where they stated that "[…] we see cyber as a domain" (Council of the European Union 2018, 2; European Court of Auditors 2019, 12). This indicates a shift towards a more offensive interpretation of cyberspace, which is consistent with their development of hard power capabilities. This development further indicates the development in the EU's cyber deterrence approach. Initially, the EU relied on deterrence by denial, i.e. through resilience and the ability to quickly recover from cyberattacks, to an approach relying both on denial and punishment, as evident in the development of the *Cyber Diplomacy Toolbox.*

However, despite the developments, the EU still faced internal trust issues which cause a lack of sharing of sensitive cybersecurity information. Such an issue arise as the cyber domain has become a considerable element of national security strategies of EU Member States. Member States might feel inclined to protect any such information, procedures and practices which can have a substantial impact of the security of their societies and economies. This lack of trust can hinder any steps towards an effective cybersecurity approach at the EU level (Ibid, 27).

6. Cyberspace in a NATO security framework

With the objective of analyzing NATO's cybersecurity and deterrence postures, the following chapter examines how the cyber threat landscape is described in strategies, statements, and reports by the Alliance, as well as relevant academic work (see appendix 2). The conclusions from this chapter will subsequently be used to elaborate on the research question and the rationale behind the *Joint Declarations.* While understanding how NATO perceives the current state of cyber threats, divided in threat types and threat actors, is useful to form a foundation of knowledge regarding which threats are viewed as urgent and how. This first step needs to be expanded in order to further analyze NATO's cybersecurity and deterrence postures. Thus, this part of the analysis is followed by an examination of NATO's cybersecurity conceptualization and deterrence strategies by analyzing three NATO cybersecurity strategies relevant to this thesis. This enables an analysis to further build an understanding of how NATO counters cyber threats strategically and on what basis. Finally, the reflections from the first two parts of the analysis in this section are subsequently discussed in the context of the concept of the cybersecurity dilemma.

6.1. Cyberspace and NATO's cyber threat landscape

The concept of cybersecurity challenges some of the key strategic thinking on which NATO was founded. NATO has traditionally been an alliance based on defending its Members from geographically proximate security threats, which collides with the principles of cybersecurity since it is not restrained by territory or geography (Burton 2015, 304; Alatalu 2018, 100). The cyber domain has become a critical geopolitical battleground for NATO in the current global context (Arts 2018, 1). Because cyberspace is a comparatively new and fast-developing domain and much less regulated than land, air and sea, and it has become a prime arena for 'grey zone' challenges (Ibid, 2).

The changing territorial dynamics of cyberspace pose significant issues with NATO's role, as cyberattacks occur over a globally linked network of computer systems and can be launched without warning, which constitutes a challenge to a geographically based security organization such as NATO (Burton 2015, 304). NATO is thus not only faced with an online dimension of geostrategic rivalries with states such as Russia and China (Ibid, 307), but also an evolving complex threat landscape as cyber threats are becoming more common, sophisticated and damaging (NATO 2016a, 1). This is evident in the vast amount of cyberattacks targeting NATO's infrastructure, which in 2017 experienced a 60% increase from the year before (NATO 2017, 1). In this challenging environment, NATO's primary task has been to secure its own institutional infrastructure and computer networks (Arts 2018, 3), since NATO's defenses are only as strong as the sum of those of its Members. NATO has thus relied strictly on defensive cyber tools. However, this approach has done little to discourage hostile actors (Ibid, 4).

The challenging nature of this field appears to have encouraged NATO to support and incite Alliance's Members to establish cyber defence capabilities (Arts 2018, 3; Robinson 2017, 134). Nonetheless, it is important to note that, as in other domains, the Alliance's cyber assets are not NATO-owned, except those protecting NATO networks and infrastructure. They are instead provided by the Alliance's Members (Stoltenberg 2018, 24; Arts 2018, 4). Relationally, NATO has made important adjustments to keep pace with changes in the cyber threat landscape in the last years (Arts 2018, 3; Burton 2015, 307), which General Secretary Jens Stoltenberg has stressed "[…] can be as dangerous as conventional attacks." (NATO 2014c, 1).

A caveat to keep in mind regarding NATO is that its mandate is only defensive (Pernik and Jermalavičius 2016, 5), and NATO will therefore not develop offensive cyber capabilities. Instead, it relies on individual Members to provide these, if deemed necessary by NATO (Goździewicz 2016, 14). If we ignore that caveat and should NATO, hypothetically, add offensive cyber capabilities to its force structure, it might increase NATO's deterrent capability (Lewis 2015, 2-3). However, cyberattacks often have political purposes such as 'influence-operations', for example Russia's involvement in the Ukraine crisis (Brangetto and Veenendaal 2016, 119) and are not intended to destroy or disrupt, as much as they are designed to put coercive political pressure on targets. This notion challenges any defensive cyber posture, why it might prove necessary to enhance defensive cooperation and increase technical cyber capabilities (Lewis 2015, 3). Moreover, according to Lewis, NATO has already received complaints that their defensive cyber doctrines is in fact more destabilizing than stabilizing as they, in reality, are more offensive than defensive. In their adversary's eyes, any NATO announcement relating to offensive cyber capabilities will be received with alarm and uncertainty (Ibid, 6).

Nonetheless, developing comprehensive cyber defense strategies is challenging, not least because this domain affects a wide variety of activities and services across the military, government, private sector and media, with vast implications for civilian life (Arts 2018, 3). According to Shea (2017a), the speed and global impact of cyberattacks continues to outrun defenders' efforts. Moreover, because cyberspace has accelerated the speed at which crises can evolve

(Shea 2017a, 21), the issue of attribution and deterrence has forced NATO to take a hard look at its preparedness, not only to fend off cyberattacks but also to preserve its political and military freedom of navigation in the cyber domain (Ibid, 19-20).

From the analysis above, it has become evident, that the increased focus on sophisticated cyberattacks against the Alliance and its Members has challenged NATO. For NATO, cyberspace can be understood as a sphere that has evolved into a critical geopolitical battleground in the current global context (Arts 2018, 1). This development, I argue, has clearly affected NATO's conceptualization of cyberspace. To further identify how these emerging challenges have affected NATO's understanding of threats in cyberspace – and how to accommodate those most efficiently – the thesis analyze three NATO cybersecurity strategies in the sections below. This analysis forms the basis for the subsequent discussion of the cybersecurity dilemma.

6.1.1. Threats

Figure 5 below depicts how the threats in cyberspace are perceived in strategies, statements and reports by NATO, as well as commentary to these by academics and experts within the field. These were selected based on the search terms (see section 4.1 on p. 14), thereby ensuring their relevance for shedding a light on NATO's cybersecurity policies and conceptualization of the cyber threat landscape. Moreover, these facilitate an analysis of NATO's perception of a cybersecurity dilemma, which ultimately assists with answering the research question. The threats are illustrated based on the number of times they were mentioned in the 30 articles selected for this analysis, see appendix 2. I acknowledge, that despite a specific threat type is mentioned more than another, it does not necessarily mean that it is more severe. It is, however, an indication of what it pertinent in NATO's public strategic documents and in academic work relating to cyber threats towards NATO.

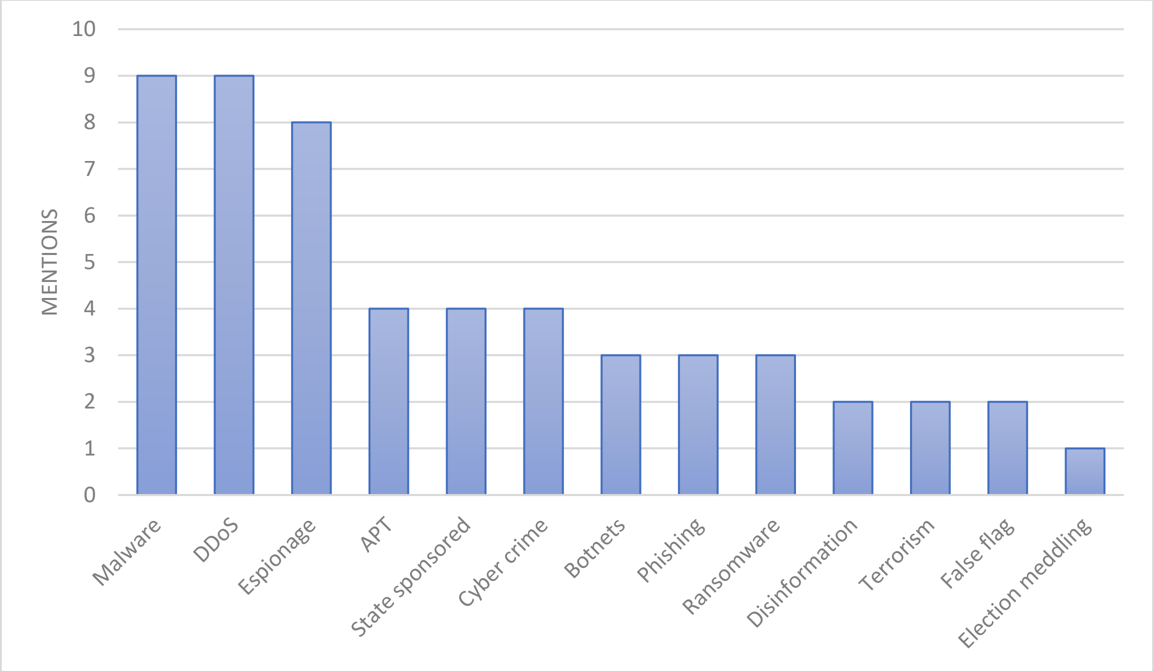

Figure 5 - Types of threats in cyberspace as perceived by the NATO

The rapidly growing technological sophistication of malware is such that NATO and its Members are at risk of being permanently lacking behind their adversaries' offensive capabilities (Burton 2015, 298). However, in a few of the NATO reports (Burton 2015; Davis 2019, Missiroli 2018) cyber terrorism figured as a potential threat. The reports did not explicit mention what the consequences of such an attack could be, but it fits into NATO's increased focus on terrorism after the 9/11 attacks in the United States (Burton 2015, 9) and the only time Article 5 on Collective Defence of the North Atlantic Treaty has been invoked (NATO 2016d, 5). However, according to Burton (2016) following the 2007 cyberattack on Estonia, NATO shifted its focus away from cyber terrorism and began to focus more on the threats emanating from states and state-sponsored groups (Burton 2015, 10).

A potential reason for the significant focus on espionage by NATO is the lack of established illegality surrounding espionage (Schmitt 2017, 169). This means that the usage of cyber espionage operations is most likely below the threshold of an armed attack, indicating that it could be a crime without punishment (Robinson 2016, 2). Accordingly, some NATO adversaries might consider cyber espionage as an integral part of their operational military capability, why the threat against NATO can be understood as a near constant. The danger thereof thus arises, as cyber espionage often targets closely guarded national secrets (Theiler 2011, 2-3) and try to compromise the confidentiality of information and information systems, potentially giving away secrets and sensitive information (Robinson 2016, 2).

From a somewhat similar background, stems NATO's focus on DDoS attacks. Based on the Alliance's own experiences with these types of attack against their networks, for example after the bombing campaign in former Yugoslavia in the 1990s (Nazario 2009, 166), or against the NATO member Estonia in 2007 (Ibid, 166) as well as against Ukraine in 2015 (Brangetto and Veenendaal 2016). NATO became aware of DDoS attacks' potential. Additionally, the Alliance's own website were targeted in 2014 (Lungescu 2014) which happened shortly after the Alliance released a statement disregarding the Crimean referendum to "quit" Ukraine in favor for Russia (NATO 2014d).

6.1.2. Actors

Figure 6 below illustrates how threat actors in cyberspace are perceived in strategies, statements and reports by NATO, as well as academic work regarding threat actors towards NATO in cyberspace. The actors in Figure 6 are visually presented based on the number of times they were mentioned in the 30 articles, see appendix 2, selected for this analysis based on their relevance in answering who NATO and experts within the field perceive as the main threat actors, which forms the basis for further analysis. The actors are subsequently discussed in the context of the previously described concept of cybersecurity dilemma.

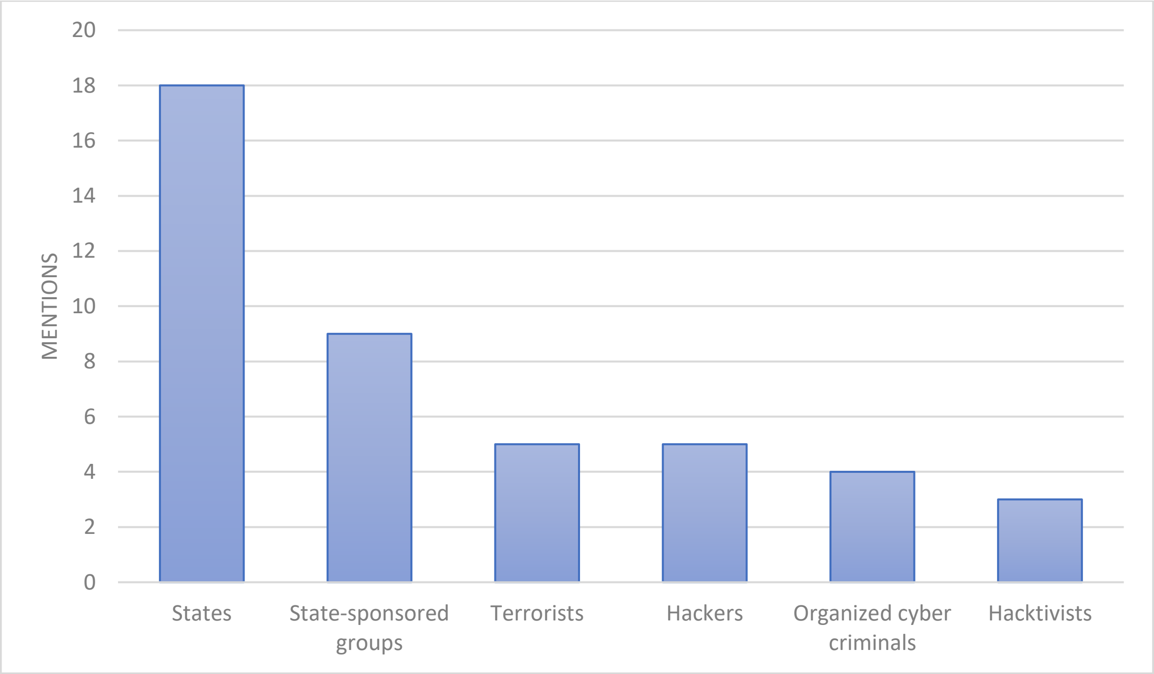

Figure 6 - Actors in cyberspace as perceived by NATO

For NATO, states represent the largest focus, which presumably stem from several cyber incidents involving NATO Members. NATO's focus arguably stems from the 2007 cyberattack in Estonia in which NATO witnessed what alleged state cyberattack could amount to (Burton 2015, 310). Moreover, several NATO Members have in recent years experienced cyberattacks accredited to states and state-sponsored groups such as Germany, Canada, Australia, the United Kingdom and the United States (Center for Strategic & International Studies 2020). This is supported by Slayton (2017) and Davis (2019) who argue, that only states and state-sponsored groups are capable to conduct cyberattacks that could meet the threshold of violence (Slayton 2017; Davis 2019, 2), that is to breach the UN Charter Article 2 Section 4 concerning the "Prohibition of threat or use of force in international relations" (United Nations 1945). Additionally, as espionage is perceived as a favored tool in state's arsenal and as its legality is still being debated (Schmitt 2017, 169), it might explain why state are perceived as being at the top of NATO's threat landscape.

6.2. NATO cybersecurity strategies

In the preceding sections, NATO's perception of cyberspace and cyber threat landscape have been examined. In the following section, three influential NATO cybersecurity summits are analyzed. These were all developed to counter the cyber threat landscape and to secure a peaceful, secure, stable and accessible cyberspace, which is a necessity for NATO as it relies on cyberspace to fulfil the Alliance's core tasks of collective defence, crisis management and cooperative security (NATO 2016a, 1).

The three Summits, Lisbon in 2010 (NATO 2010a) at which the *Strategic Concept* was endorsed (NATO 2010b), the Wales Summit in 2014 (NATO 2014a) and the Warsaw Summit in 2016 (NATO 2016c), each represented important strategy implementations for NATO, which is elaborated below. In short, they show that in the emerging globalized world, where complex new vulnerabilities and threats continue to emerge, cyber resilience has become an integral part of NATO's policy orientation. Additionally, it shows how NATO moved from an initial defensive posture, towards a more offensive posture, by for example confirming the applicability of Article 5 of the North Atlantic Treaty to cyberspace and recognizing cyberspace as a new domain of operations. Relatedly, NATO stresses that their development is in accordance with international law, including international humanitarian law and the UN Charter in its fullest, which NATO states are applicable to cyberspace (NATO 2014a, 14; NATO 2016c, 15).

The 2010 Lisbon Summit and subsequent *Strategic Concept* were marked by the events that occurred in Estonia in 2007 and Georgia in 2008 (Kamp 2016, 2; Christou 2016, 50). These highlighted NATO's need to develop its ability to prevent, detect, defend against and recover from cyberattacks

(NATO 2011, 1). At the 2010 Lisbon Summit, NATO acknowledged that cyber threats against the Alliance were rapidly increasing in numbers and in sophistication, which ultimately threatened NATO's existence in and access to cyberspace. It is noteworthy that the Summit Declaration does not mention the notion of deterrence (Burton 2015, 309) but only included vague references to their deterrence posture by stating the need to improve their capabilities to detect, assess, prevent, defend and recover in case of cyberattacks against infrastructure of critical importance to the Alliance (NATO 2010a, 10), which could be extrapolated to NATO acknowledging their reliance on deterrence by denial. In order to achieve this, NATO projected a further development of each NATO Members' national cyber defence capability along with an optimization of the information sharing, collaboration and interoperability internally in NATO. Moreover, NATO stressed the need to address threats through several bilateral cooperations with actors such as the UN and the EU (Ibid, 10). NATO envisioned that such bilateral cooperations would enhance wider international security and stability, while becoming a framework for political dialogue and regional cooperation in the field of security (Ibid, 7).

In the *Strategic Concept* (NATO 2010b), focus is on the frequency and costs of cyberattacks. It states that "[…] they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability" (NATO 2010b, 11). This statement is relevant for two reasons. Firstly, there is no direct referencing to NATO's Article 5 and collective defence, in relations to cyber, in the *Strategic Concept*. However, a somewhat vague and implied reference can be found stating that a national threat (given that the nation is a member of NATO) easily can become a NATO issue. Secondly, even though the sentence above seems rather vague in its reference to international law, it does refer to the UN Charter Article 2 Section 4 concerning the "Prohibition of threat or use of force in international relations" (United Nations 1945), which is consistent with NATO's argument, that international law applies to cyberspace (NATO 2014a, 14).

The 2014 Wales Summit (NATO 2014a) was also a major step for NATO in acknowledging the challenges posed by complex cyberattacks. It reiterated the earlier statement from the Lisbon Summit Declaration in that cyberthreats and attacks were becoming more common, sophisticated and damaging to the Alliance (NATO 2010a, 10; NATO 2014a, 14). Additionally, it was the first official NATO document in which NATO confirmed the possibility that a cyberattack could activate Article 5 of the North Atlantic Treaty (NATO 2014a, 14-15; Goździewicz, 2016, 12; Maldre 2016, 1). It is likely that the cyberattacks in Estonia in 2007 influenced the outcome of the Wales Summit (Missiroli 2018, 5), and placed cybersecurity at the very heart of NATO's operational outlook (Burton 2015, 2).

Additionally, it established a framework of assistance, building of capacity and capability and enhanced partnerships (NATO 2014a; Robinson 2017, 134).

As the Summit Declaration stated that cyber defence had become a part of NATO's core task of collective defence (NATO 2014a, 14), Article 5 of NATO's treaty on collective defence (NATO 1949) could potentially be invoked in cases where a cyberattack reaches the effects comparable to that of a conventional armed attack (NATO 2014a, 14-15). However, there are no criteria listed in the Summit Declaration explaining under which circumstances Article 5 could be invoked. On the contrary, it is stated that the North Atlantic Council on a case-by-case basis will decide if Article 5 could be invoked (Ibid, 15). This underlines the general difficulty with retaliating against a cyberattack, as the issue of attribution makes it extremely difficult to work out, where the attack actually came from (Ranger 2014, 3; Burton 2015, 12). Because of the lack of criteria regarding what constitutes a cyberattack justifiable of retaliation, it remains unclear if even a minor intrusion into NATO's networks would be enough, or if an attack it must cause a severe impact on the economy, critical infrastructure, or national security of a NATO member. Nevertheless, Jamie Shea, then head of NATO's Emerging Security Challenges (2010-2018), claimed that the reason behind the secrecy of the criteria is because this itself will work as a deterrent since the ambiguousness does not provide potential aggressors with the idea, that they can carry out certain types of cyberattacks with impunity (Ashford 2014, 1). This is supported by Davis (2019), who states that NATO's ambiguity means that it neither limits nor excludes punishment to cyberattacks. Instead, it keeps the option open to use the full range of the Alliance's capabilities to deter and counter cyberattacks (Davis 2019, 11). Consequently, this resembles an attempt to create a deterrence by punishment posture but because of the missing credibility, it risks becoming a hollow threat (Davis 2019, 12). Additionally, the statement that Article 5 might be used is certainly meant as a deterrent and a signal that NATO is not defending itself only in 20th century terms. But it can easily become interpreted as an escalatory means, which surely is not NATO's intent (Ranger 2014, 2; Arts 2018, 5).

Relationally, it is not clear what a collective defence response would look like: purely cyber, purely conventional, or a combination. Moreover, contrary to the EU, NATO does not have the authority to implement sanctions against states in response to cyberattacks and an attack using conventional force would need to be proportional to the original offence (Burton 2015, 12; Besch 2018, 1), unless NATO decides to disengage from its own statements, that international law applies to cyberspace.

An outcome of the 2016 Warsaw Summit was NATO's recognition of cyberspace as the fifth domain of operations (NATO 2016c, 15), which can be understood as a further step in NATO's conceptual evolution of cyberspace as an aspect of collective defence (Bigelow 2017, 2). This is a crucial element for NATO, since three-quarters of host-nation support for NATO operations is provided by commercial infrastructure and services. If the resilience level of the national networks is not increased, cyberattack can potentially paralyze the civilian infrastructure and seriously hinder NATO forces and operations (Stoltenberg 2018, 22-24). According to Jamie Shea (2017b), following the Wales Summit, the next logical step was to declare that NATO regards cyberspace as an operational domain. In essence, this means that NATO has shifted its focus on protecting its own internal networks to focusing on cyber defence of every military activity that NATO carries out (Shea 2017b, 167), while still keeping NATO's posture defensive (NATO 2016a, 1; Robinson 2017, 138). However, NATO's shift to acknowledging cyberspace as a new domain of operations indicates a change in NATO's cyber approach. NATO has shifted from information assurance, being protection of its internal network, to mission assurance, being cyber defence of its military activity (Shea 2017a, 20-21; Bigelow 2017, 6). Mission assurance differs from information assurance, as it seeks to ensure that a mission can be completed even if some systems have been attacked, whereas information assurance strives to protect all information systems and assets (Ibid, 6-7). By recognizing cyberspace as a domain of operations, NATO has thus shifted from focusing on cybersecurity as an information assurance task, to incorporating it into mission assurance. In other words, NATO's focus is no longer solely on protection of its own networks and supporting its Members in building defensive capabilities, but it is increasingly focused on integrating cyber capabilities, offensive and defensive, into operations and missions (Davis 2019, 6).

At the Warsaw Summit, NATO furthermore reaffirmed its responsibility and desire to enhance the cyber defence of national infrastructure and networks, as well as NATO's own networks. Accordingly, this should enhance NATO's cyber resilience, which ultimately enables the Alliance to fulfil its core tasks (NATO 2016c, 15). It is noteworthy that the Warsaw Summit Declaration states that by recognizing cyberspace as an operational domain, NATO supports its deterrence posture (Ibid, 15). This underlines that NATO's cyber deterrence posture is founded in deterrence by denial (Minárik 2016, 2; Burton 2015, 311) for several reasons. Firstly, in order to achieve deterrence by punishment in cyberspace, you need to show your offensive capabilities in order to make your adversaries fearful of your retaliation (Valeriano and Maness 2015, 48; Gartzke 2013, 47). Since cyberweapons are one time usage only, you lose your capability by showing it (Slayton 2017, 86).

Moreover, since NATO itself does not have offensive capabilities, it relies on the individual NATO Members to provide them in time of need (Goździewicz 2016, 14). These are per definition intrinsically linked to national security, why NATO Members quite possibly would not show them (Pernik and Jermalavičius 2016, 7). Secondly, the lack of a criteria for invoking Article 5, makes deterrence by punishment less credible, since it does not draw a clear line for when a cyberattack is sufficiently harmful to cross the threshold to an armed attack. Thirdly, NATO does not currently have an operational definition of what the collective response would be if that threshold were to be crossed (Davis 2019, 11).

The challenges and countermeasures described above indicate, to an extent, how NATO is affected by the cybersecurity dilemma. Even though NATO does not explicitly mention the existence of a cybersecurity dilemma, some of their actions indicate that it exists. Even if it might not have been deliberately, the lack of criteria for when a cyberattack could cause Article 5 to be invoked (NATO 2014a, 15), can possibly create an environment in which a cybersecurity dilemma will evolve. The lack of transparency might cause an increased uncertainty for NATO's adversaries. They might interpret the lack of criteria, as an opportunity to test NATO's resolve. This will create a need for NATO, as well as NATO's adversaries, to build up their cyber capabilities to counter each other's capabilities. Contrary, Davis (2019) argues, that an increase in transparency might actually serve as a deterrence in cybersecurity. NATO could, in a limited way, signal their cybersecurity and defence capabilities and show that they appear to be making progress (Davis 2019, 12).

The cybersecurity dilemma has already surfaced to some extent, as Russia has complained about the destabilizing effects of NATO's cybersecurity approaches. This will only be exacerbated by any NATO announcements relating to the development of offensive cyber capabilities (Lewis 2015, 6). Evidently, NATO could pursue a very transparent and defensive cybersecurity approach in order to quell any cybersecurity dilemmas.

In addition, in cases where defenders detect a breach, they might not be aware of the intruder's intentions. Such operations could range from spying, establishing a foothold for future defensive measure (in cases where the intruder might feel threatened by the defender), or prepare for an imminent for future cyberattack (Slayton 2017, 73). Assessing intent in cyberspace is difficult and states tend to assume the worst, which ultimately can lead to misinterpretation and an escalatory spiral of hostile action (Buchanan 2016, 97-98).

The analysis of NATO's cybersecurity strategies above has indicated that NATO is moving towards an operationalization of cyberspace in which offensive is becoming increasingly important. It is also important to note that NATO's cybersecurity is only as strong as the Alliance's weakest link, and NATO has put much effort into increasing Members' defensive capabilities. This long-lived project has nevertheless done little to discourage hostile actors from targeting NATO's systems (Arts 2018, 4). This evidently supports the notion that, even though cybersecurity and defensive capabilities continue to improve, offense has the advantage in cyberspace (Davis 2019, 5). Relationally, malware evolves in technological sophistication in such a tempo that NATO and its Members are at risk of becoming permanently 'behind the cybersecurity curve' (Burton 2015, 298). Shea agrees with Burton's notion and stresses that the speed and global impact of cyberattacks continues to outrun defenders' efforts and accelerate the speed at which cyber crises can evolve (Shea 2017a, 21).

Even with NATO confirming that cyberattacks can invoke Article 5 (NATO 2014a, 14-15), and NATO seemingly ensuring that the Alliance can make appropriate responses to cyberattacks, the problem of attribution remains. The possibility of anonymity in cyberspace is an excellent advantage for the attacker and even if the defender eventually identifies the attacker after plowing through vast reams of technical data, the problem of attacks below the threshold still exists (Davis 2019, 12). This leaves us with a relevant question: if the attacker can remain anonymous, how can the defender credibly threaten and warn off attackers (Ibid, 10)? This conundrum underscores the complexity of cyberspace as a conceptual field and a threat landscape as well as the relevance of implementing appropriate strategies to counter the issues herein.

6.3. Sub conclusion

In a rapidly evolving cyber threat landscape characterized by complex and sophisticated threats and elusive actors, NATO's cybersecurity strategy has shifted from a deterrence by denial posture to a combination of deterrence by denial and punishment. NATO's recognition that threats in cyberspace can threaten the prosperity, security and stability of the Euro-Atlantic area, NATOs initial response was to call for an increase in cooperation with organizations such as the EU and UN (NATO 2010b, 11), since building relationships with key partners is central to NATO, as physical borders are largely, if not entirely, irrelevant in cyberspace (Robinson 2017, 136). Moreover, NATO's cybersecurity posture was largely defensive and relied on a deterrence by denial posture (NATO 2010a, 10). To counter the evolving threat landscape facing NATO and its Members, NATO recognized the need to balance its defensive capabilities and deterrence by denial strategy, with some offensive capabilities and deterrence by punish measures. This was evident as NATO acknowledged that cyberattacks could invoke an Article 5 retaliation (NATO 2014a, 14-15) and that cyberspace became a new domain of operations (NATO 2016c, 15). However, these actions have also exemplified that a cybersecurity dilemma lurks under the surface. By expressing that Article 5 could be invoked because of a cyberattack, but not stating under which circumstances it might happen, NATO adds to the already uncertain cyberspace environment. In addition, the ambiguity extends into the type of retaliatory punishment NATO threatens with (Davis 2019, 11). Moreover, the declaration that cyberspace has become a new domain of operations, might instill insecurities within NATO's adversaries about their own cyber capabilities and prompt them to increase their capabilities. This can arguably start a cyber arms race, which might be strengthened by the apparent advantage held by the offense.

In this environment characterized by uncertainty, NATO has taken steps to increase its own cybersecurity level, possibly at the expense of their adversaries. Nevertheless, a relevant question remains: Can NATO on their own, create and sustain a credible deterrence posture in cyberspace, when much of their strategies are surrounded by ambiguity and arguably a lack of credibility?

7. EU and NATO: How and why cyber strategies differ

The following chapter compares and analyzes the differences in the conceptualization of cyberspace by the EU and NATO, respectively. More specifically, the chapter focuses on variations in how the cyber threat landscape and cybersecurity is conceptualized by each entity. Additionally, the two organizations' perception of the cybersecurity dilemma is compared. By understanding their differences and possible similarities, these steps ultimately enable a nuanced analysis and discussion of why the EU and NATO in 2016 and 2018 decided to expand their cooperation by agreeing to an enhanced cyber partnership. The *Joint Declarations* is analyzed in the next chapter.

While the two organizations differ in structure, origin and current aims, they are nevertheless targeted by some of the same actors and threats, for example politically motivated non-state actors, sophisticated state actors, cybercriminals and espionage operations. This subsequently threatens the civil, political, economic and military levels of society of both organizations' Members (Lété and Pernik 2017, 1). By 2016, the apparent benefits from increasing their cooperation were acknowledged by the EU and NATO and the two organizations' leaders signed the *Joint Declarations* bolstering cooperation in areas such as cyber resilience building, cyber capacity building, education and training (European Parliament 2017, 55). For both organizations, cyberspace constitute a strategic challenge impacting the organizations' and their Members' security and defence (Pernik 2014, 1).

It is therefore useful to understand the foundational differences between the two organizations, as this might shed some clarity on why they place more focus on and perceive certain elements differently, thus making their response different from the other. While the EU and NATO to some degree share similarities e.g. common liberal values and strategic interests (European Parliament 2017, 52; Smith 2019, 20; NATO 2020c, 1), their origin are nonetheless different.

The EU is a politico-economic organization which general purpose is to promote economic, social and political cooperation among its Members. It is fundamentally a supranational government based upon a parliamentary system in which representatives are elected by the Member States. Its political framework is designed to promote cooperation among Member States in pursuit of common political, social and economic interests (European Union 2020a). As its name declares, its scope of authority is confined geographically to the European sub-continent (European Union 2020b).

Contrary, NATO is a politico-military organization with the stated goal of safeguarding the freedom and security of its Members through political and military means, which is emphasized in its Article 5 on Collective Defence (NATO 1949; Pernik 2014, 1). The organization consists of 30 European countries along with the United States, Canada and Iceland (NATO 2020a) along with various partners across the globe, e.g. Australia, New Zealand and Japan (NATO 2020b). In relations to this thesis, the two organizations especially differ in regard to their focus on security and military.

Whereas the two elements are foundational for NATO, the EU's approach is not as security-centered and military-related as NATO's. EU's area of interest and responsibility is related to data protection, as seen in the General Data Protection Regulation (GDPR), cyber-crime prevention, i.e. the Budapest Convention on Cybercrime, online rights and cyber diplomacy (Pernik 2014, 2-4; Giantas 2019, 28-29). Within the EU, as stated previously, each Member State is responsible for their own defense and security, while the EU provides assistance, advise and support through its institutions. Besides its advisory role, the EU functions as a regulator and lawmaker, while ensuring coordination, cooperation and policy harmonization between its Member States (Ibid, 29). NATO focuses more on national security, for example the security of individual Members, while the EU deals with a broader, mainly non-military range of cyber issues (Internet freedom and governance, online rights and data protection) and internal security aspects (Pernik 2014, 2-3).

7.1. EU and NATO cyberspace conceptualization

As shown in the two previous chapters, NATO and the EU do, to a large extent, have similar cyberspace conceptualizations. This has come about, despite their underlying reasoning were different: NATO were concerned about secure its own institutional infrastructure and computer networks (Arts 2018, 3), while the EU feared for their digitalized economy and societies (European Commission 2009, 3; European Commission 2016, 10). Ultimately, they share the premise that cyberspace is understood as a form of global community, transcending physical borders from which various costly attacks can originate against them (European Commission 2009, 3; European Commission 2018, 7; European Parliament 2019, 1; Arts 2018, 1; NATO 2014c, 1; NATO 2016a, 1).

However, the EU conceptualizes cyberspace more defensively than NATO, as the EU seemingly has been reluctant to recognize cyberspace as a new domain. In 2014, they stated that some understood cyberspace as a new domain of military activity, while not expressing their own opinion (Council of the European Union 2014, 2), which could be extrapolated as though the EU did not perceive it similarly. Then, in 2018, the EU stressed that they now perceived cyberspace as a new domain of military activity (Council of the European Union 2018, 2), which clearly signals a move towards a more offensive interpretation of cyberspace. Consequently, this might entail a future characterized by more offensive strategic decisions when dealing in cyberspace. Relatedly, it should be noted that NATO in 2016 at the Warsaw Summit stated that they perceived cyberspace as the fifth domain of operations (NATO 2016c, 15). It is worth noting that the EU's statement that cyberspace was a new domain of operations came after the *Joint Declaration*, indicating that the EU might have been affected by the cooperation with NATO. Relatedly, NATO's recognition of cyberspace as a new domain of operations could be seen as a further step in their conceptual evolution of cyberspace as a part of their collective defence (Bigelow 2017, 2), which they stressed at the 2014 Wales Summit (NATO 2014a, 14). Accordingly, cyberspace became part of NATO's core task of collective defence (Ibid, 14) and cyberattacks can therefore potentially trigger Article 5 of NATO's treaty on collective defence (NATO 1949). This indicates that NATO's conceptualization of cyberspace is founded in their belief of cyberspace developing into a global geopolitical battleground (Arts 2018, 1). Contrary, even though the EU has reaffirmed that they perceive cyberspace as a domain, they have not been clear on how the Union's Article 42(7), the mutual defence clause (European Union 2012a, 27), or Article 222, the solidarity clause (European Union 2012b, 102), could utilized in case of a cyberattack. The EU has solely reaffirmed the possibility, that the two Articles could be applied, in order for each Member State to assist any other Member State that is under cyberattack (European

Parliament 2018b, 3; Signoretti, 2019, 3). Moreover, as the 2018 Resolution did not state the EU's perception on the threshold of a cyberattack (European Parliament 2018b), the application of the two Articles to cyberspace seems as a distant option.

While NATO and the EU seemingly have closed in on each other in regard to their cyberspace conceptualization, a gap still exist, see Figure 7.

	EU	NATO
Focus	Internal security	Internal security
Approach	Diplomatic	Military
Collective defence	No	Yes

Figure 7 - EU and NATO cyberspace conceptualization gap

This gap might stem from each organizations' respective subsistence. As a political-military alliance, NATO's mission is to ensure its Members' security through collective defence, deterrence and cooperative security through partnership and the organization's own networks and infrastructure, against cyberattacks (Pernik 2014, 1; Štitilis, Pakutinskas & Malinauskaitė 2017, 1155). Whereas the EU as a politico-economic union, primarily is concerned with internal security issues, such as fighting cybercrime through criminal justice cooperation, the protection of critical infrastructures (Pernik 2014, 2) and ensuring that the EU continues to benefit economically from cyberspace (European Commission 2017a, 2).

7.2. EU and NATO cyber threat landscape

The cyberattacks on Estonia in 2007 forced both NATO and the EU to rethink their positions within cyberspace, and both have consequently intensified their initiatives towards the cyber domain (Lété and Pernik 2017, 2). According to Lété and Pernik (2017), the initial conditions for creating a credible response to malicious cyberattacks is ability and willingness. Conducting collective responses and deterrence is not possible if the states or organizations compiling the response have different perceptions of the threats or willingness to respond, which thus risks further conflict (Ibid, 2). Relatedly, in the following section, similarities and differences between the threats and actors, respectively, that are present to the EU and NATO are compared and analyzed. It shows that even though NATO's and the EU's cyber threat landscape are not entirely similar, they share key elements, which, following Lété and Pernik's (2017) argument, might foster a mutually beneficial partnership moving forward.

7.2.1. Threats

As seen in Figure 8, NATO and the EU perceive the top cyber threats similarly, albeit with a few exemptions. Both perceive malware attack high and while NATO mostly focus on espionage and DDoS attacks, as these are some of the attacks they have experienced in recent years (Nazario 2009, 166; Lungescu 2014), the EU focuses more on cybercrime, ransomware and botnets, which are threat types that Members within the Union have been exposed to with grave consequences (ENISA 2017).

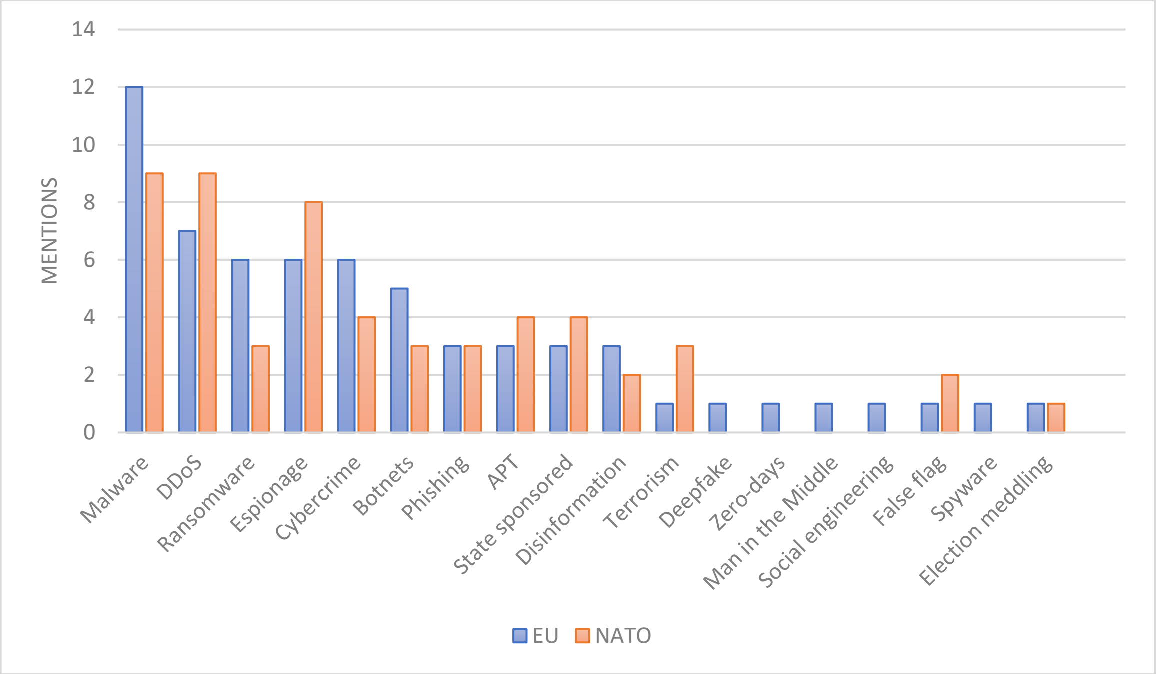

Figure 8 - Types of threats in cyberspace, the EU and NATO compared

For NATO, prior to the cyberattacks in Estonia in 2007, the 9/11 attacks in the United States dictated much of their focus towards terrorism (Burton 2015, 9). Following the Estonian cyberattacks, NATO's focus shifted away from cyber terrorism and began to focus more on the threats emanating from states and state-sponsored groups (Burton 2015, 10). Nonetheless, several NATO reports still portray cyber terrorism as a potential threat (Burton 2015; Davis 2019, Missiroli 2018). Conversely, the EU does not give much attention to the issue of cyber terrorism. In fact, EUROPOL state in their 2016 TE-SAT report, that although cyber terrorism carries a high potential, it currently has a low probability (EUROPOL 2016, 17), which is reiterated in their 2018 report (EUROPOL 2018, 15)

Both NATO and the EU place much focus on espionage, which arguably must stem from the lack of established illegality surrounding espionage (Schmitt 2017, 169). By employing espionage, attackers can hypothetically obtain critical information (Theiler 2011, 2-3) to which the target cannot legally respond, as espionage most likely is placed below the threshold of an armed attack. This means, ultimately, that espionage could be a crime without consequences for the attackers - without punishment (Robinson 2016, 2). Additionally, espionage can be difficult to distinguish from offensive cyber operation preparations, since both types of threats entail system penetration. Consequently, such challenges contribute to the risk that an act of cyber espionage will be misinterpreted as another type of activity, such as a cyber use of force (Schmitt 2017, 172-173).

Additionally, DDoS attacks receive much attention by both NATO and the EU but for different reasons. NATO's focus on DDoS attacks can be argued to stem from the Alliance's own experiences with these types of attack against their networks, for example after the bombing campaign in former Yugoslavia in the 1990s (Nazario 2009, 166) and since they witnessed that attack type's capability in both Estonia in 2007 (Ibid, 166) and Ukraine in 2015 (Brangetto and Veenendaal 2016, 119). DDoS attacks are unarguably among the most observable and disruptive cyberattack and are often coupled with a political motivation (Nazario 2009, 164). Besides being relatively cheap and easily available, the tool can be used through independent botnets to create plausible deniability for the attack (Ibid, 175). This threat type is naturally relevant for the EU as well, which EUROPOL (2019) also stressed in their *Internet Organised Crime Threat Assessment* report. In it, EUROPOL stated that even though the report's primary focus is the threat emanating from ransomware, DDoS attacks come in at a close second (EUROPOL 2019, 22).

7.2.2. Actors

As seen in Figure 9, NATO and the EU do not perceive the cyber threat landscape actors in the same way. For NATO, states and state-sponsored groups make up the majority, while the EU, albeit placing states in the top, is more focused on cyber criminals and hackers.

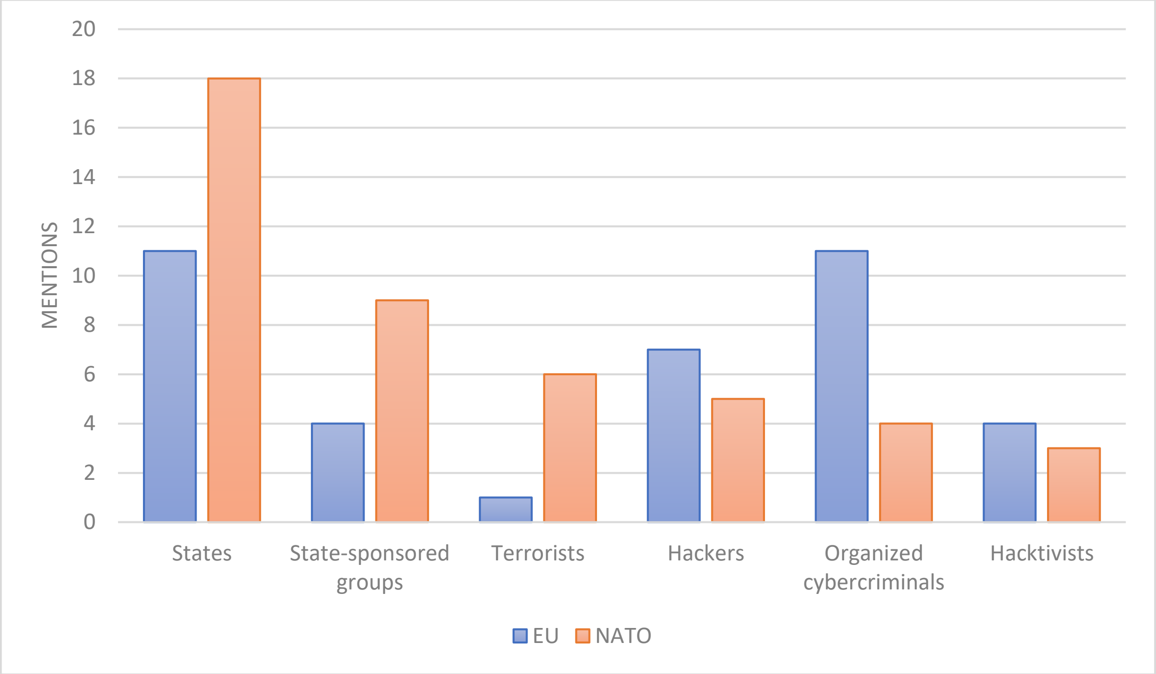

Figure 9 - Types of actors in cyberspace, the EU and NATO compared

For NATO, the most imminent actor is arguably those who are able to mount sophisticated cyberattack, which in most cases will be state and state-sponsored actors (O'Flaherty 2018, 1; Moore 2020, 3; Burton 2015, 310; Slayton 2017; Davis 2019, 2). In both Estonia, Georgia and Ukraine, NATO witnessed what sophisticated cyberattack could amount to. All of these have largely been contributed to Russia (Alatalu 2018, 96; Mauer 2015, 78; Weedon 2015, 73), which could be seen as an underlying reasoning for NATO’s focus on state actors. The EU also places state actors highly, as evident in their strategies *An Open, Safe and Secure Cyberspace* (European Commission 2013) and *Cyber Diplomacy Toolbox* (Council of the European Union 2017). These stress that foreign states have already inflicted costly damages against the EU and show little to indicate that they are about to halt (European Commission 2013, 4; Council of the European Union 2017, 3). Moreover, different from NATO, the EU also emphasizes organized cyber criminals as key actors in regard to cyber threats. This relates to the relative ease that cybercriminals can create income by using tools such as ransomware. Through such crude tools, cybercriminals continue to cause significant problems and financial losses in the EU (EUROPOL 2019, 15), why European Union Agency for Law Enforcement Cooperation (EUROPOL) places this actor type highest in their 2019 report the *Internet Organised Crime Threat Assessment (iOCTA)* (Ibid, 22). The EU’s focus on cybercrime is not new, as they in 2001 adopted the *Budapest Convention on Cybercrime* (Council of Europe 2001).

NATO, conversely, to a somewhat low degree include organized cyber criminals in their focus areas. Instead they place much attention on state-sponsored groups. NATO has already experienced the effect of these, for example as a response to NATO's bombing campaign in Serbia in 1999 (Nazario 2009, 166) or after NATO's presence in Ukraine following Russia's annexation of Crimea (Mauer 2015, 78; Croft and Apps 2014, 1). Additionally, several NATO Members have been targeted by state-sponsored groups, such as Germany, Canada, Australia, the United Kingdom and the United States (Center for Strategic & International Studies 2020).

In addition, due to the ambiguous legality of cyber espionage (Schmitt 2017, 169), many states and state-sponsored groups employ this tool, which support NATO's notion that states and state-sponsored groups are understood as being their main adversaries. This being said, NATO (2010b) has stated that the Alliance should not dismiss non-state actors as irrelevant, as they can still inflict costly attacks and threaten the Euro-Atlantic prosperity, security and stability (NATO 2010b, 11).

7.3. EU and NATO approaches to cybersecurity

Both the EU and NATO understand cybersecurity as a strategic issue with the potential to affect the security and defence of both their organizations and Members. Accordingly, both organizations place much emphasis on resilience and defence of each of their networks and infrastructure, which in turn means that their individual Members are responsible for their own national cyber security (Pernik 2014, 1-7).

Over the past years, the EU's has begun evolving into a global diplomatic and security actor (Renard, Thomas and Barrinha 2018, 181; Scheffer 2018, VI; European Commission 2016, 10), which is evident in their continuously efforts to ascertain their values (European Union 2020, 1; European External Action Service 2017, 13; ENISA 2017, 4). Despite making somewhat similar remarks (NATO 2010a, 7; Porter 2019, 1; Štitilis, Pakutinskas & Malinauskaitė 2017, 1158), NATO has focused less on the diplomatic elements of cyberspace and more on readying the Alliance to the challenges that cyberspace poses while building cyber capabilities. The latter has contested the Alliance's original purpose of countering geographically proximate security threats (Burton 2015, 304; Alatalu 2018, 100; NATO 2010a, 10; Robinson 2017, 134). Yet both organizations have undergone a great development in regard to their cybersecurity conceptualization, which have resulted in what appears to be somewhat similar cybersecurity approaches today. While the EU's initial cybersecurity approach was previously predominantly defensive, relying solely on soft power such as diplomacy, capacity-building, resilience and recovery from cyberattacks (Carriço 2017, 335-

337; Darmois and Schméder 2016, 16), they have now become less defensive. This is evident in their implementation of the *Cyber Diplomacy Toolbox*. This follows the EU's own statement that soft power alone would not be sufficient and how hard power tools are a necessary to incorporate in such efforts (European Commission 2017b, 6). It can therefore be claimed that the EU's cybersecurity approach is based on a combination of deterrence by simultaneous denial and punishment. NATO has undergone a similar development, from an approach relying mainly on deterrence by denial posture to a combination of deterrence by denial and punishment (NATO 2010a, 10; NATO 2014a, 14-15; NATO 2016c, 15; Shea 2018, 5). Similar to the EU's acknowledgement that they needed to incorporate hard power tools, NATO also recognized the need to balance its defensive capabilities with offensive ones, which was evident in their acknowledgement of cyberattacks being able to invoke an Article 5 retaliation (NATO 2014a, 14-15) and that cyberspace had indeed become the fifth domain of operations (NATO 2016c, 15).

While the EU and NATO's cybersecurity approaches show similarities on a strategic level, they differ when it comes to the concrete fight against cybercrime. As the EU perceives organized cybercriminal as one of the main adversaries (see Figure 8), elements of their cybersecurity approach are targeted towards it, for example the Budapest Convention on Cybercrime. Contrary, NATO's cybersecurity approach does not distinguish cybercriminals the same way as the EU (Štitilis, Pakutinskas & Malinauskaitė 2017, 1154), although the context might be similar as NATO's strategic concept is related to "[…] develop further our ability to prevent, detect, defend against and recover from cyberattacks" (NATO 2010b, 16) which might as well stem from cybercriminals. Moreover, NATO's cybersecurity approach is not laid out in great detail as those coming from the EU often are, take for example NATO's Wales Summit Declaration which contained two paragraphs on NATO's cybersecurity approach (NATO 2014a). It remain unknown, if this lack of clarity is based on the same logic as Jamie Shea argued for in regard to the lack of criteria of what constitutes a cyberattack justifiable of retaliation; that it keeps the Alliance's adversaries in the dark (Ashford 2014, 1).

7.4. Subconclusion

The apparent differences between the EU and NATO correlate with the basic notion that NATO is a military organization, and the EU is not. In general, as a politico-economic union, the EU's approach to cyberspace is more geared towards dealing with issues such as cybercrime and resilience of critical infrastructure (Carriço 2017, 337-338; European Parliament, 2018b, 3; Pernik 2014, 1). This is underlined by the fact that the EU often deals with a broader non-military range of cyber challenges, for example the applicability of fundamental human rights, democracy and the rule of law in cyberspace (European Commission 2013, 2; Pernik 2014, 1). This is demonstrated, as the EU's remains undecided on the application the Union's Article 42(7), the mutual defence clause (European Union 2012a, 27) and Article 222, the solidarity clause (European Union 2012b, 102) as a response to cyberattacks (European Parliament 2018b, 3; Signoretti, 2019, 3), while NATO has clearly stated that a cyberattack can invoke the Alliance's collective defence clause (NATO 2014a, 14-15).

Despite being largely in agreement regarding the threat types, the two organizations only agree that states represent a main threat actor in cyberspace, which might stem from the legal ambiguity of espionage in cyberspace (Schmitt 2017, 169). Contrary, NATO regards state-sponsored groups as the other main part of the threat actors landscape, as they are able to mount sophisticated cyberattacks against the Alliance (O'Flaherty 2018, 1; Moore 2020, 3; Burton 2015, 310; Slayton 2017; Davis 2019, 2) while the EU focus more on cybercriminals, which according to the EU stem from the relative ease cybercriminals can cause significant problems and financial losses in the EU (Council of the European Union 2017; EUROPOL 2019, 15; Council of Europe 2001).

Both the EU and NATO's conceptualization of cybersecurity have moved from a predominantly defensive deterrence by denial to a more offensive posture combining both deterrence by denial and punishment. As a political union, the EU has relied more on soft power tools, such as diplomacy, however with their implementation of the *Cyber Diplomacy Toolbox*, the EU has incorporated hard power tools (European Commission 2017b, 6). NATO has undergone a similar change moving from a posture relying mainly on deterrence by denial posture to a combination of deterrence by denial and punishment, for example by stressing that Article 5 is applicable to cyberspace (NATO 2010a, 10; NATO 2014a, 14-15; NATO 2016c, 15; Shea 2018, 5). However, as Pawlak (2017) notes, while countering threats in cyberspace requires a mix of soft and hard tools, there is a chance that the EU's responses might become too closely aligned with NATO's approach, shifting their approach from diplomatic to military (Pawlak 2017, 12). This is a challenge that the EU is aware of, noting that as NATO will continue to rely on their military capabilities, the EU should exploit its broader and more soft capabilities (European Commission 2017b, 12).

8. The EU-NATO Joint Declarations

As described in the previous chapter, the EU and NATO differ in regard to their conceptualization of cyberspace, their cyber threat landscape, and their approach to cybersecurity. Nonetheless, they have deemed their cooperation as necessary to facilitate an effective response to the contemporary cyber threat landscape. As such, some form of complementarity and cooperation is needed, since neither NATO nor the EU can tackle the whole scale of cyber challenges by themselves (Tardy and Lindstrom 2019, 2; Lété and Pernik 2017, 2).

The following chapter analyzes the *Joint Declarations* and subsequently discuss the rationale behind the *Joint Declarations* by operationalizing the theories of liberalism, realism, deterrence, and the security dilemma. Additionally, it draws on findings from step 3 and five progress reports on the implementation of the *Joint Declarations*. This is done in order to shed light on various possible explanations behind the developments of the first *Joint Declaration* in 2016 and the developments in the EU-NATO partnership after 2016.

In the challenging cyber environment, as analyzed in the previous chapters, the EU and NATO envisioned a complementary partnership to increase their resilience levels in a cyber context. Especially the events in Estonia in 2007 appears to have intensified both the EU and NATO's initiatives in cyberspace (Lété and Pernik 2017, 2). This intensification culminated at NATO's Warsaw Summit in 2016 where the EU and NATO adopted the first *Joint Declaration* in order to deepen the EU-NATO cyber partnership. At the NATO Summit in 2018, a second *Joint Declaration* was signed, which included a shared vision on how the EU and NATO should work together to counter what was perceived as common cybersecurity threats (Council of the European Union 2019b, 1).

The 2016 *Joint Declaration* laid the foundation for an enhanced cyber cooperation between the two organizations as it called for, "[…] a new impetus and new substance to the NATO-EU strategic partnership." and defined four areas of cyber security cooperation such as integration of cyber defense into missions and operations, exercises, education, training (NATO 2016d, 1; Lété and Pernik 2017, 2; Shea 2018, 3). According to NATO and the EU, the decision to enhance their cooperation stems from increased and unprecedented challenges to the Euro-Atlantic community "emanating from the South and East" (NATO 2016d, 1), which can be interpreted as common adversaries such as Russia and China. However, the reference to "the South" should be seen in relations to the other areas the *Joint Declarations* covers, such as cooperation at sea and on migration in the Mediterranean (Ibid, 1). However, the *Joint Declaration* states that "Together they can better provide security in Europe and beyond" (NATO 2016d, 1), which collides with NATO's original mandate for collective defence of its Members against external aggression in the North Atlantic area (NATO 1949; Tardy and Lindstrom 2019, 8). However, NATO's recent engagement in for example Afghanistan, have challenged the Alliance's geographical restriction (Ibid, 8), which most likely will be the case for the cyberspace as well. For the EU, its focus on the 'neighbors of the neighbors' are being challenged by its own ambition of becoming a global security actor (Ibid, 8; Renard, Thomas and Barrinha 2018, 181; Scheffer 2018, VI; European Commission 2016, 10).

Relationally, NATO and the EU's security have to some extent become interconnected, to which they argue that a stronger NATO equals a stronger EU and vice versa. However, very little is stated in the *Joint Declaration* regarding how to mitigate cyber challenges. In the Declaration, it is stressed that the EU and NATO can jointly mobilize a broad range of tools to respond to the challenges, which correlates with the statement that the EU and NATO will "[…] use all ways and means available to address these challenges […]" (NATO 2016d, 1). Even though it is not directly stated that the EU and NATO will use all means available, i.e. cyber capabilities, diplomacy, conventional force, the statement above clearly indicates that they are willing. On one hand, one can argue that this development indicates that the EU and NATO rely on deterrence by punishment (Tolga 2018, 7). However, the *Joint Declaration* also notes that it will counter the threats by bolstering resilience (Ibid, 1), which, on the other hand, indicates that the EU and NATO to some extent also rely on the deterrence by denial strategy (Brantley 2018, 48).

Another perspective to understanding the development of the EU-NATO partnership is the adaptation of a newer Declaration in which cyber deterrence takes on a slightly different role. In 2018, NATO and the EU adopted a second "*Joint Declaration"*. The 2018 Declaration emphasizes the Euro-Atlantic bond and the level of improvement achieved since 2016 in areas such as timely information exchange on cyberattacks, the efforts to strengthen resilience and coordinated exercises (NATO 2018a, 2). The 2018 *Joint Declaration* reiterates the 2016 statement that the challenges to the EU and NATO originates from the East and South. However, in contrast to the 2016 *Joint Declaration*, deterrence by punishment is not hinted as a measure. The 2018 *Joint Declaration* only references deterrence by denial, as it states that the resilience of the EU and NATO Members will be increased even further (Ibid, 1).

Nonetheless, interestingly to this discussion, the 2018 *Joint Declaration* keeps stressing the need for the partnership to "[…] take place in the spirit of full mutual openness" and adds that "In this context, we view transparency as crucial. We encourage the fullest possible involvement of the NATO Allies that are not members of the EU in its initiatives. We encourage the fullest possible involvement of the EU Member States that are not part of the Alliance in its initiatives." (Ibid, 1-2). The need to stress this, might indicate that certain parts of the EU and NATO partnership is not functioning as intended. This has been a returning challenge for the EU and NATO partnerships (Koenig 2018, 3; Raik and Järvenpää 2017, 6). In relations to the *Joint Declarations*, both the EU and NATO have tried to mitigate these challenges, by stressing the organizations' complementarity and that the partnership will not distort the security and defence policies of those EU Members who are not NATO Members and vice versa (Savin 2019, 41).

However, even though the expectations of the *Joint Declarations* were high, by examining the annual implementation progress reports (Council of the European Union 2017b; Council of the European Union 2017c; NATO 2018b; NATO 2019b; NATO 2020d), it becomes evident that the partnership is not yet functioning perfectly. It is therefore pertinent to further discuss if the foundational and conceptual differences between the organizations can be blamed for the lack of progress.

9. Discussion

In this section, the rationale behind the *Joint Declarations* is discussed by drawing on key theoretical perspectives and concepts from liberalism, realism, deterrence and the cybersecurity dilemma. This is supported by discussing the reflections from step 3 of the analysis of the *Joint Declarations* (see section 7 on p. 55).

From a realist point of view, the anarchical tendencies in cyberspace flourish in cyberspace because of the lack of an international governing body. The basic argument is therefore that it is necessary to make alliances or partnerships in order to enhance one's security. However, this need for strategic partnerships can be overshadowed by mistrust (Craig and Valeriano 2018, 94-95) as releasing information on one's cyber capabilities often means that others can close potentially targeted vulnerabilities rendering the capabilities useless (Bendiek and Metzger 2015, 558-559; Goychayev et al. 2017, 51). However, another argument is that by signing the *Joint Declarations* and increasing integration of cyber defense into missions and operations and conducting joint exercises, the level of mistrust is potentially lowered, and the two organizations gradually become more confident in their partnership.

From a liberal point of view, the *Joint Declarations* can one the one hand be understood as mainly a relevant partnership within the realm of cyberspace. According to the liberal school of thought, international organizations are emerging as a central balance of power-tool within the international political realm. This correlates with the *Joint Declarations*, which state that an increased cooperation between the two organizations will make both entities stronger and provide better security in Europe and beyond (NATO 2018a, 1). On the other hand, the two organizations conceptualize cyberspace very differently, which may impact their basis for a constructive partnership (also see Figure 6 on p. 48). The variation within conceptual understandings of cyberspace might stem from the basic notion that NATO is a military organization, and the EU is not. In general, as a politico-economic union, the EU's approach to cyberspace is more geared towards dealing with issues such as cybercrime and resilience of critical infrastructure.

The EU's current conceptualization of cyberspace appears to be mostly defensive minded, as it mostly concerns responding to challenges such as organized cybercrime through soft power tools e.g. the Budapest Convention on Cybercrime (Burton 2015, 298-313). However, the EU's conceptualization of cyberspace has shifted slightly, as they have recognized a need to incorporate offensive measures in order to create a credible deterrence posture, i.e. through the *Cyber Diplomacy Toolbox*. Somewhat similar, NATO's conceptualization of cyberspace was predominantly offensive, as seen in their statements that cyberspace has become the fifth domain of operations and that Article 5 of the NATO Treaty can be activated in case of a of cyberattack. However, NATO appears now to have recognized the potential of the EU's *Cyber Diplomacy Toolbox,* which indicates that NATO has identified the need to combine their military capabilities with diplomatic capabilities, such as sanctions.

Despite their different conceptualizations of cyberspace, the *Joint Declarations* argue that because the two organizations' security is interconnected, and they face similar challenges, there is a need to "step-up our efforts" (NATO 2018a, 1). This notion coincides with Keohane and Nye's (2012) concept of complex interdependence theory. Interdependence refers to a situation of mutual dependence, which in international politics refers to situations characterized by reciprocal effects among states (Keohane and Nye 2012, 7), similar to those expected due to the increased EU-NATO partnership. Another central element is the decline of the use of military force as a balance of power-tool (Ibid, 9). This manifests itself, as states in which a complex interdependence exists, cease to use military means to resolve disputes (Ibid, 21-23). Such a line of argumentation fits within the general notion that cyberspace transcends borders and geography that arguably creates an interdependency among its users. Both the EU and NATO have stated that their Members rely heavily on cyberspace for economic reasons, why they seek to protect a free cyberspace (European Commission 2018; NATO 2018c). This arguably means that the use of military force in cyberspace will decline and more focus will be put on soft power means, such as the EU's *Diplomatic Toolbox.* Moreover, this is in line with Eriksson and Giocomello's (2016) assessment, that in cyberspace no one can counter all threats alone, which is why cooperation increases in order to counter threats originating from cyberspace (Eriksson and Giocomello 2016, 231-232).

Thus, in case of a fruitful partnership, the organizations involved could on one hand diminish their mutual security dilemma as trust, confidence, and transparency of the other grows. On the other hand, organizations or states not included in such partnerships, might feel the need to increase their own security, as they perceive theirs as being decreased. This in turn would cause a security dilemma to increase.

It is noteworthy that little was stated regarding the cyber threat landscape in the two *Joint Declarations*. This lack of mentioning instills the question of whether it was done intentionally as a political and/or strategic decision. By not stating that the two organizations differ in cyber threat landscape perception, such a difference so to speak 'does not exist'. According to Lété and Pernik (2017), if organizations does not share the same threat perception, or willingness to respond, their partnership will not become effective (Lété and Pernik 2017, 2). Relatedly, as shown in Figure 7 on p. 58, the EU and NATO's perception of the cyber threat landscape does not differ much regarding threat types. However, the two organization's perception of actors differs more substantially. This might stem from the fact that NATO is founded on a basis that is grounded in realism, in which the international arena is seen as a competitive and hostile stage dominated by states (Waltz 1979, 102; Morgenthau 1948, 13) and state-sponsored groups. The anarchical structure of cyberspace furthermore prompts NATO to focus on their own security - and ultimately survival (Craig and Valeriano 2018, 88). This is not to say that NATO as an organization does not have liberal characteristics, i.e. the wish to establish mutual beneficial cooperation with other organizations but, I argue, realism is arguably the most dominant based on the original purpose of the organization. Contrary, the EU is more grounded in liberalism than realism. In line with the findings in Figure 7 in chapter three, the EU also perceive states as a central actor in cyberspace. However, contrary to NATO, the EU perceives other actors than states and state-sponsored groups as central in cyberspace, which is a key element in the liberal school of thought (Eriksson and Giocomello 2006; Keohane and Martin 1995).

Consequently, this could mean that a partnership between two organization, whose perception of the cyber threat landscape differs *too* much, might not reach their stated goals. This can be said to be the case, to some extent, for the EU-NATO partnership. When examining the first progress report from mid-2017 it is stated that the EU and NATO recognize that all issues of common interest or concern should be addressed, which could be interpreted as a subtle attempt to bridge any existing cyber threat landscape gap (Council of the European Union 2017b, 2). Yet, when examining the following progress reports it is clear that progress is moving quite slow and, in some cases, not at all, which will be elaborated on later. However, these differences can also lead to a degree of complementarity in which the two different approaches lead to a broader mitigation of cyber threats.

The EU and NATO exhibit some comparative advantages that partly follow their cybersecurity conceptualization, i.e. NATO being more focused on a military nexus versus EU's civilian focus. This is captivated by the fact that NATO is by mandate the collective defence organization and thus covers the upper end of the military spectrum, while the EU is better positioned to conduct more civilian related activities. This division is also acknowledged in the *Joint Declarations,* which state that NATO will continue to play its essential role as the primary cornerstone of collective defence for its Allies (NATO 2018a, 2). As shown in chapter three, both organizations have gone through a period of development in regard to their cybersecurity conceptualization, which have resulted in their cybersecurity approaches becoming more similar overtime. Moreover, based on the *Joint Declarations* one can argue that the two organizations are still attempting to align their cybersecurity strategies even further in order to avoid duplication of their efforts and increase their capabilities.

The EU's development correlates with the statement that their former reliance on soft power is not sufficient making hard power tools necessary to incorporate in a cyber context (European Commission 2017b, 6). On one hand, the development of the EU's cyber sanction regime is aligned with the liberal thought regarding state's usage of military force as a balance of power-tool being in decline (Keohane and Nye 2012, 9). On the other hand, Waltz' (1979) notion of defensive realism can also be seen in the EU's development. As outlined in section 3.2 on p. 14, Waltz' argues that states are not inherently aggressive, but the anarchical nature of the international system encourages them to undertake defensive and balanced policies. According to Waltz, defensive realism is not about maximizing power but about maintaining one's position in the international system (Waltz 1979, 126). One of the EU cyber hard power capabilities comes from their ability to impose cyber sanctions through their *Cyber Diplomacy Toolbox.* The goal of the *Cyber Diplomacy Toolbox* is to promote security and stability in cyberspace, which can be understood in line with the notion of defensive realism (Council of the European Union 2017a, 4). It therefore appears evident that the EU's cybersecurity approach is mainly based on a combination of deterrence by both denial and punishment.

NATO has undertaken a similar change moving from a posture relying mainly on deterrence by denial to a combination of deterrence by denial and punishment, for example by stressing that Article 5 is applicable to cyberspace (NATO 2010a, 10; NATO 2014a, 14-15; NATO 2016c, 15; Shea 2018, 5). Even though NATO displays some liberal tendencies, i.e. the wish to form partnerships with other organizations, their approach is arguable, based on the above mentioned characteristics, mostly influenced by realism. As shown in chapter three, NATO's development in cyberspace has mainly historically been offensive, for example by stating that cyberspace is the fifth domain of operations and that a cyberattack can trigger an Article 5 response (NATO 2016c, 15). This should not come as a surprise since NATO is a politico-military organization with the stated goal of safeguarding the freedom and security of its Members through political and military means (NATO 1949). The realist thought of the anarchical tendencies in cyberspace flourishing due to the lack of an international governing body means that national security and power are still very much the most central elements in the realm of cyberspace (Craig and Valeriano 2018, 94). For NATO, this means that the Alliance has to rely on their allies, such as EU, with whom trust issues have been indicated. Consequently, one can argue that this causes NATO to build both offensive and defensive cyber capabilities.

The EU and NATO's development towards security measures in cyberspace can be detected in the 2016 *Joint Declaration*, which in regard to cyber challenges states "[…] we use all ways and means available to address these challenges […]", which can be interpreted as a warning and thus as an indication that both organizations adhere to deterrence by punishment. However, in the 2016 as well as the 2018 *Joint Declaration* it is also stated that there is an urgent need to bolster both organization's resilience levels (NATO 2016d, 1; NATO 2018a, 1), which indicates that both rely on a mix of deterrence by denial and punishment in cyberspace. This development correlates with arguments presented by several authors within IR in that relying on one type of deterrence alone, will not be sufficient (Tolga 2018, 18; Nye 2017, 68; Brantley 2018, 49). Such a line of argumentation can be read alongside Nye's notion that deterrence by punishment works against states and some criminals, while deterrence by denial is best suited against the general notion of non-state actors, i.e. the majority of criminals, hackers, and hacktivists (Nye 2017, 68). Furthermore, Nye expands his notion stating that a completely different alternative might be shifting towards what he refers to as deterrence by entanglement (Ibid, 58). According to Nye, deterrence by entanglement involves making an actor perceive that the costs of an action will exceed the benefits. Entanglement refers to the existence of various interdependencies that can make an attack successful and simultaneously impose serious costs on the attacker as well as the victim. Accordingly, because of the serious costs to both parties, a potential adversary may not attack, even if the attack is not defended against, because it has something highly valuable to lose. This ultimately means that the most beneficial outcome is to maintain the status quo (Ibid, 60).

As mentioned above, when examining the progress reports, it becomes evident that progress moves slow. For instance, in each of the progress reports it is informed that increasing complementarity and developing an understanding of each other's cybersecurity approach is ongoing (Council of the European Union 2017b, 3; Council of the European Union 2017c, 3; NATO 2018b, 5; NATO 2019b, 5; NATO 2020d, 6). This indicates that there might be a lack of complementarity, which slows the process, an unwillingness or even that they are unable to align they cybersecurity strategies. This can be captured in the different approach the two organizations have when it comes to responding to cyberattacks reaching the threshold of an attack. As presented in chapter three, NATO has acknowledged that Article 5 of the NATO Treaty is applicable in cyberspace, meaning that an attack reaching the threshold of an attack can active the Alliance's collective defence clause.

The EU has a similar mutual defence clause in Article 42(7) of the Treaty of the European Union, but the EU has not been clear on how - and if - it can be activated. This leaves another gap to be filled by the EU and NATO, as they must align their conceptualizations and strategies to achieve a common response and thereby create a more credible deterrence approach. In other words, the circumstances in which the EU and NATO would work together to adopt a responsive or offensive posture are still ambiguous (Lété 2019, 33). If the EU and NATO expect their partnership to achieve the stated goals, it is pertinent that they agree on how to conduct "digital self-defence" and create a template on how to synchronize as well as use their respective cyber tools (Lété and Pernik 2017, 7-8). The absence of a clear definition of the circumstances, degree and manner in which countermeasures can or should be taken if Member States suffer a cyberattack, make it more difficult for the EU and NATO to respond collectively to a potential cyberattack (Lété 2019, 33). These difficulties could be perceived by adversaries as an attempt to hide the true intentions and possible reactions in case of a cyberattack. The lack of clarity and transparency could moreover cause the adversaries to believe, that their defence is insufficient prompting them to enhance their capabilities, ultimately causing a security dilemma.

In addition, out of the five progress reports, four state that two of the four main areas of cyber cooperation (training and education) are not being achieved. According to the progress reports, NATO has, on several occasions, invited the EU to either observe, take part in as full participant or plan NATO-led cyber exercises and workshops, but this has not been reciprocal. Accordingly, not until 2017 did NATO receive an invitation from the EU to observe on of its cyber exercises (European Parliament 2017, 54; Council of the European Union 2017c, 3; NATO 2018b, 1; NATO 2019b, 5; NATO 2020d, 6).

The apparent mistrust and unwillingness between the two entities can perhaps be explained by the fact that the *Joint Declarations* were signed and issued by the two organizations' senior representative. They were thus not passed by voting from Member States. On one hand, this might influence the degree of political will within each organizations' Members. In particular, those states that belong to only one of the two organizations might not see cooperation with the other organization as a top priority and also have divergences with the idea of mutually-beneficial partnership (Sliwinski 2014, 9; Tardy and Lindstrom 2019, 9). This is, for example, evident in the continuously ongoing standoff between Cyprus and Turkey over the unresolved conflict on Cyprus (Raik and Järvenpää 2017, 6; Christou 2016, 54; Tardy and Lindstrom 2019, 10), which might impede their willingness to cooperate and level of trust. According to Koenig (2018), the *Joint Declarations* were implemented in a way so to circumvent potential political blockades at the two organizations (Koenig 2018, 3). According to Petallides (2012), partnerships will be impaired when any member of it decides not to reveal their capabilities or contribute equally. When not doing so, the level of trust and ultimately the level of security the partnership could create, will diminish. This is often the case, when members feel that they have to give up more information than they might like, fearing that they will weaken their own position (Petallides 2012, 2-3). On the other hand, the political blockades also arguably continue to place a 'glass ceiling' over implementation of the *Joint Declarations* (European Parliament 2017, 55), meaning that it will not reach the stated goals. This is also argued by some NATO officials who complained that the *Joint Declarations* were nothing more than "bureaucratic stuff" and that it lacked substantive joint action in the cyber area (Koenig 2018, 4).

This is likewise evident as the EU and NATO's attempt to develop a joint procedural playbook on how to counter cyber threats (NATO 2016d, 1) was halted due to the EU's reluctance of associating its broad diplomatic tools exclusively with NATO (Koenig 2018, 4). This blockage could be explained with some EU Member States being unwilling to deepen the two organizations' partnership in fear of the EU unintentionally ending up shifting its optics from its diplomatic approach towards a more military approach (Pawlak 2017, 12).

10. Conclusion

The rapidly changing environment in cyberspace brings new challenges on the traditional structures of intergovernmental organizations such as the EU and NATO. While cybersecurity has long been part of EU and NATO calculus, it has only recently moved to the top of agendas. In this thesis, I have analyzed *how* developments in cyberspace have affected the development of *Joint Declarations* as well as *why* such declarations were perceived as the next rational step for both organizations in making cyberspace more secure.

Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges states and organizations face in modern times. Especially one incident, the 2007 Estonia cyber-attacks, prompted the EU and NATO' to think more seriously about threats from – and within - cyberspace. Since 2007, both the EU and NATO have rethought and redesigned their security strategies as a response to the changing threat landscape. This is due to a realization that what works in the physical arena will not necessarily work in the cyber arena. Consequently, the cyber threat landscape differs from the traditional threat landscape, strategies and approaches, which might have worked for the EU and NATO before in mitigating and deterring threats, are not necessarily applicable to cyberspace. When analyzing how cyber strategies by the EU and NATO have developed, I have drawn on elements from two classic theoretical schools of thought within International Relations (IR), realism and liberalism, to discuss the complexities of how and why the EU and NATO have conceptualized cyberspace and responded to threats herein, respectively and comparatively.

Cyberspace's nature, and the anarchical tendencies within, creates an environment in which cyberattacks, sometimes, can be conducted not only by state but also by the emerging non-state actors with no apparent consequences. This is a result of the difficulty of attribution, which can lead to a reciprocal challenge. Without the ability to correctly attribute an attack, how can one create a credible response? In this climate of urgency and interdependency, defenders can seldom stand-alone as very few, if any, has the capability to deter and defend against all cyber threats. Because cyberspace transcends physical borders and is not limited by time and space, the challenges stemming from it becomes global. This recognition of the specificities of cyberspace as a threat landscape highlights the need to establish partnerships in order to secure oneself. Moreover, this can help to quell any potential cybersecurity dilemmas, which might stem from states increasing their capabilities in order to mitigate the cyber threat landscape. Also, as cyberspace has become an integral part of many states' economy and security, it has become a sensitive area and mistrust may come easy. One can however argue that strategic partnerships have the potential to build trust among partners and lay foundation for future cooperation and increased security.

In this thesis, I have found that it was against this background that the EU and NATO saw each other as complementary partners in a pursuit to increase their mutual cybersecurity, deterrence and, resilience capabilities, as well as situational awareness. The analysis has shown that, on paper, the two organizations appear compatible, as they share the same liberal values and have the same overall goals in cyberspace. This was also stated by both organizations prior to signing the first *Joint Declaration* in 2016. For NATO, EU might be an advantageous partner as the EU has the ability to implement cybersecurity legislation within Europe, and thus impose a minimum standard, which NATO itself cannot impose on its European Members. For the EU, partnership with NATO would entail a strengthening of their defensive efforts on Europe's borders.

I argue that despite the challenges for the EU-NATO partnership, the rationale behind a strategic cyber partnership makes sense for several reasons. In this thesis, I have found the following reasons to be compelling arguments in favor of such a partnership as a mutually beneficial response to current cyber threats, as conceptualized by the EU and NATO, respectively:

- Firstly, the rapidly changing and complex cyber threat landscape that both states and organizations face establish a foundation for partnerships that can mutually benefit both organizations' security, as they widen their cybersecurity approach.
- Secondly, the combination of their different cyber deterrence approaches, enables the EU and NATO to create a more credible deterrence posture - not only limited to militarily or diplomatic responses.
- Thirdly, by entering into a strategic partnership, the EU and NATO can avoid duplication of their efforts to mitigate the cyberthreat landscape.
- Fourthly, in relation to the above, the partnership can lead to a better usage of their respective defence budgets.
- Lastly, international and global partnerships can eventually influence the creation of international norms, values and acceptable state behavior in cyberspace. However, this process might have long prospects as efforts to encourage long term global changes have proven to become protracted in the past.

Concluding, in this thesis I have shown how developments in cyberspace have affected the development of *Joint Declarations* in that specificities of threats that transcend borders, and where perpetrators are challenging to pinpoint, enable the foundation of a mutually beneficial partnership between the two organizations. In relation hereto, the partnership represents a rational step for both the EU and NATO in their attempt to mitigate current and future threats from cyber space.

10.1. Further studies

Building on the conclusion from this thesis, further studies regarding overcoming the challenges to strategic cyber partnerships would be valuable in order to ensure that partnerships such as the EU and NATO actually achieve their stated goals. In the case of the EU and NATO strategic cyber partnership, despite the political will being present at top level, some Members of both organizations have seemed less inclined to commit to this partnership. While the rationale behind the partnership makes sense, when analyzing the annual implementation progress reports it is evident that the partnership is not yet functioning as expected. Further studies could therefore reflect on why the partnership has not yet been fruitful, in which an element of mistrust could be seen as a factor. Consequently, this level of mistrust has affected various areas of the partnership, from information sharing to joint exercises and alignment of strategies. Moreover, a potential consequence of the mistrust between the two organizations, might cause that the partnership's goal of increasing complementarity between the EU and NATO's cyber deterrence and cybersecurity approaches will not be achieved. Based on the progress reports, it is insinuated that the two organizations still retain their initial cyberspace conceptualization, deterrence, and cybersecurity approaches. This might be a result of the aforementioned mistrust which might cause a level of uncertainty regarding the partnership's potential for success. This might explain, why both organizations are reluctant to depart with their own strategies as these are based on their respective original purpose and sticking with them, leave them with a fallback strategy in case the partnership fails.

Bibliography

Aarhus University. “Tekststudier”, *Metodeguiden*. Accessed 24.03.2020. Available at: https://metodeguiden.au.dk/tekstanalyse/

Alatalu, Siim. “NATO’s responses to cyberattacks“, In *Chaillot Paper No. 148*, edited by Nicu Popescu and Stanislav Secrieru, 103-114, *European Union, Institute for Security Studies*, 2018

Alexander, Dean C. “Cyber Threats Against the North Atlantic Treaty Organization (NATO) and Selected Responses”. *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi*, 2014. Accessed 12.03.2020. Available at: https://www.researchgate.net/publication/287714732_Cyber_Threats_Against_the_North_Atlantic_Treaty_Organization_NATO_and_Selected_Responses

Appathurai, James. ”The Future of NATO’s Partnerships” in *DIIS Report – Cooperative Security: NATO’s Partnership Policy in a Changing World*, edited by Trine Flockhart, 121-131, 2014. Accessed 10.04.2020. Available at: https://pure.diis.dk/ws/files/58169/WP2014_01_NATO_tfl_web.pdf

Arts, Sophie. “Offense as the New Defense: New Life for NATO’s Cyber Policy”, *The German Marshall Fund of the United States*, 2018. Accessed 15.04.2020. Available at: http://www.gmfus.org/publications/offense-new-defense-new-life-natos-cyber-policy

Ashford, Warwick. ”Nato to adopt new cyber defence policy”, *ComputerWeekly*, 2014. Accessed 23.04.2020. Available at: https://www.computerweekly.com/news/2240228071/Nato-to-adopt-new-cyber-defence-policy

Beach, Derek and Rasmus Brun Pedersen. *Process-Tracing Methods: Foundations and Guidelines*. Michigan: University of Michigan Press, 2013

Bendiek, Annegret and Tobias Metzger. “Deterrence theory in the cyber-century”, German Institute for International and Security Affairs (May, 2015).

Besch, Sophia. “Protecting European networks: What can NATO do?”, *Centre for European Reform – Insight*, 2018. Accessed 12.03.2020. Available at: https://www.cer.eu/insights/protecting-european-networks-what-can-nato-do

Bhaskar, Roy. *A Realist Theory of Science*. New York: Routledge, 2008

Bigelow, Brad. “Mission Assurance: Shifting the Focus of Cyber Defence”, *9th International Conference on Cyber Conflict*, 2017. Accessed 15.04.2020. Available at: https://ieeexplore.ieee.org/abstract/document/8240327

Bowen, Glenn A. “Document Analysis as a Qualitative Research Method”. *Qualitative Research Journal*, Vol. 9, No. 2 (2009): 27-40

Brangetto, Pascal and Matthjis A. Veenendaal. “Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations”, *8th International Conference on Cyber Conflict*, 2016. Accessed 05.05.2020. Available at: https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf

Brantley, Aaron F. “The Cyber Deterrence Problem”, *2018 10th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn (2018): 31-54

Brodie, Bernard, Frederick Sherwood Dunn, Arnold Wolfers, Percy Ellwood Corbett, and William T. R. Fox. *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt, Brace and Co., 1946

Brodie, Bernard. “The Anatomy of Deterrence”, *U.S. Air Force – Project RAND*. RAND Corporation, 1958

Buchanan, Ben. “Cyber Deterrence Isn’t MAD; It’s Mosaic”, *Georgetown Journal of International Affairs*, Vol. 1 (2014): 130-140

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. New York: Oxford University Press, 2016

Burton, Joe. “NATO’s Cyber Defence: Strategic Challenges and Institutional Adaptation”, *Defence Studies*, Vol. 15, No. 4 (2015): 297-319

Burton, Joe. “Cyber Deterrence: A Comprehensive Approach?”, *NATO Cooperative Cyber Defence Centre of Excellence*, 2018

Buzan, B., Ole Wæver and Jaap de Wilde, *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers, 1998

Carrapico, Helena and André Barrinha. “The EU as a Coherent (Cyber)Security Actor?”, *Journal of Common Market Studies*, Vol. 55, No. 6 (2017): 1254-1272

Carriço, Gonçalo. “Strengthening the EU’s Resilience in the Virtual Domain”, *European View*, Vol. 16, No. 2 (2017): 331-347

Center for Strategic & International Studies. ”Significant Cyber Incidents”, *Center for Strategic & International Studies*, 2020. Accessed 19.04.2020. Available at: https://csis-prod.s3.amazonaws.com/s3fs-public/200403_Significant_Cyber_Events_List.pdf?.tlmv65Bm5D0d5UVqRtac3qdYqd.BYtLj

Christou, George. “The EU’s Approach to Cyber Security”, *EU-China Security Cooperation - Policy Paper*, 2014. Accessed 10.04.2020. Available at: https://pdfs.semanticscholar.org/4f1e/d6b053c7c8d0a882277515b2ce393a7a19fe.pdf

Christou, George. *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*. New York: Palgrave MacMillan, 2016

Cirlig, Carmen-Cristina. “Cyber defence in the EU Preparing for cyber warfare?”, *European Parliament*, 2014. Accessed 18.03.2020. Available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2014)542143

Council of Europe. “Convention on Cybercrime”, *European Union*, 2001. Accessed 13.05.2020. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Council of the European Union. "EU Cyber Defence Policy Framework”, *Council of the European Union*, 2014. Accessed 20.03.2020. Available at: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf

Council of the European Union. ”Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") - Adoption”, *Council of the European Union*, 2017a. Accessed 20.03.2020. Available at: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

Council of the European Union. “Progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016” *Council of the European*

Union, 2017b. Accessed 20.06.2020. Available at: https://www.consilium.europa.eu/media/23997/170614-joint-progress-report-eu-nato-en.pdf

Council of the European Union. "Second progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016" *Council of the European Union*, 2017c. Accessed 20.06.2020. Available at: https://www.consilium.europa.eu/media/35577/report-ue-nato-layout-en.pdf

Council of the European Union. "EU Cyber Defence Policy Framework (2018 update)", *Council of the European Union*, 2018. Accessed 20.03.2020. Available at: https://www.consilium.europa.eu/media/37024/st14413-en18.pdf

Council of the European Union. "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States", *Council of the European Union*, 2019a. Accessed 08.04.2020. Available at: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32019D0797

Council of the European Union. "Cooperation between the EU and NATO". *Council of the European Union*, 2019b. Accessed 16.04.2020. Available at: https://eu2019.fi/en/backgrounders/eu-and-nato

Craig, Anthony J. S. and Brandon Valeriano. "Realism and Cyber Conflict: Security in the Digital Age" In *Realism in Practice – An Appraisal,* edited by Davide Orsi, J. R. Avgustin and Max Nurnus, 85-101 Bristol: E-International Relations Publishing, 2018

Croft Adrian and Peter Apps. "NATO Websites hit in cyber attack linked to Crimea tension", *Reuters*, 2014. Accessed 14.05.2020. Available at: https://www.reuters.com/article/us-ukraine-nato/nato-websites-hit-in-cyber-attack-linked-to-crimea-tension-idUSBREA2E0T320140316

Darmois, Emmanuel and Geneviève Schméder. "Cybersecurity: a case for a European approach", *Security in Transition*. Accessed 10.04.2020. Available at: https://www.fes-london.org/fileadmin/user_upload/publications/files/FES_LSE_Cybersecurity_Schmeder_Darmois_XXXXXX-XXXX

Davis III, John S., Benjamin Boudreaux, Jonathan W. Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern & Michael S. Chase "Stateless Attribution: Toward International Accountability in Cyberspace", *RAND Corporation* (2017): 1-57

Davis, Susan. ”NATO in the Cyber Age : Strengthening Security and Defence, Stabilizing Deterrence”, *NATO Parliamentary Assembly, Science and Technology Committee*, 2019. Accessed 12.03.2020. Available at: https://www.nato-pa.int/document/2019-nato-cyber-age-strenghtening-security-and-defence-stabilising-deterrence

Denning, Dorothy. “Cybersecurity’s Next Phase: Cyber Deterrence”, *Scientific American*. 2016. Accessed 22.01.2020. Available at: https://www.scientificamerican.com/article/cybersecuritys-next-phase-cyber-deterrence/

Easton, Geoff. “Critical Realism in Case Study Research”. *Industrial Marketing Management*, Vol. 39 (2010): 118-128

Efthymiopoulos, Marios Panagiotis. “A cyber-security framework for development, defense and innovation at NATO”, Journal of Innovation and Entrepreneurship, Vol. 8, No. 12 (2019): 1-26

Eriksson, Johan and Giampiero Giocomello. “The Information Revolution, Security, and International Relations: (IR)relevant Theory?”, *International Political Science Review*, Vol 27, No. 3 (2006): 221–244

EULEX. “About EULEX”, *European Union Rule of Law Mission Kosovo*, 2020. Accessed 09.05.2020. Available at: https://www.eulex-kosovo.eu/?page=2,60

European Commission. "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”. SEC 399, 2009. Accessed 17.03.2020. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52009DC0149

European Commission. “JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace”. JOIN 1 final, 2013. Accessed 17.03.2020. Available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission. “JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Joint Framework on countering hybrid threats a European Union response“, JOIN 18 final, 2016. Accessed 20.03.2020. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

European Commission. "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU". JOIN 450 final, 2017a. Accessed 17.03.2020. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450

European Commission. "Reflection paper on the future of European Defence", *European Commission*, 2017b. Accessed 20.03.2020. Available at: https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf

European Commission. "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL - Increasing resilience and bolstering capabilities to address hybrid threats". JOIN 16 final, 2018. Accessed 17.03.2020. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN%3A2018%3A16%3AFIN

European Commission. "Cybersecurity". *European Union*, 2020. Accessed 07.02.2020. Available at: https://ec.europa.eu/digital-single-market/en/cyber-security

European Court of Auditors. "Challenges to Effective EU Cybersecurity Policy", *European Court of Auditors*, 2019. Accessed 18.03.2020. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

European External Action Service. "Shared Vision, Common Action: A Stronger Europe", *European External Action Service,* 2017. Accessed 20.03.2020. Available at: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

European External Action Service. "EU-NATO cooperation - Factsheet", *European Union,* 2019. Accessed 08.05.2020. Available at: https://eeas.europa.eu/sites/eeas/files/eu-nato_cooperation_factsheet_june_2019.pdf

European Parliament. "Cybersecurity and Cyberpower : Concepts, Conditions and Capabilities for Cooperation for Action within the EU", *Directorate-General for External Policies of the Union,* 2011. Accessed. 10.04.2020. Available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EXPO-SEDE_ET(2011)433828

European Parliament. “Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union”, *European Parliament and the Council of the European Union*, 2016. Accessed 18.03.2020. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L1148

European Parliament. “Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and Risks for the EU”, *European Parliament*, 2017. Accessed 18.03.2020. Available at: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-eu-common-security-and-defence-policy-csdp-challenges-and-risks-for-the-eu

European Parliament. “Stepping up EU cyber defence and cooperation with NATO”, *European Union*, 2018a. Accessed 08.05.2020. Available at: https://www.europarl.europa.eu/news/en/agenda/briefing/2018-06-11/7/stepping-up-eu-cyber-defence-and-cooperation-with-nato

European Parliament. ”Cyber defence”, *European Union*, 2018b. Accessed 08.05.2020. Available at: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0258_EN.html?redirect

European Parliament. “Foreign influence operations in the EU”. *European Union*, 2018c. Accessed 17.03.2020. Available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2018)625123

European Parliament. “Cyber: How big is the threat?”. *European Union*, 2019. Accessed 17.03.2020. Available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2019)637980

European Union Agency for Cybersecurity (ENISA). “Botnets”. Accessed 09.02.2020. Available at: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets

European Union Agency for Cybersecurity (ENISA). “WannaCry Ransomware: First ever case of cyber cooperation at EU level”. Accessed 17.06.2020. Available at: https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level

European Union Agency for Cybersecurity (ENISA). “Review of Cyber Hygiene practices”, 2016. Accessed 29.03.2020. Available at: https://www.enisa.europa.eu/publications/cyber-hygiene

European Union Agency for Cybersecurity (ENISA). “Overview of Cybersecurity and Related Terminology”, 2017. Accessed 29.03.2020. Available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology/view

European Union Agency for Cybersecurity (ENISA). “Do you know who is who in EU cybersecurity?”, 2020. Accessed 09.04.2020. https://www.enisa.europa.eu/news/enisa-news/do-you-know-who-is-who-in-eu-cybersecurity

European Union. "Consolidated version of the Treaty on European Union”, *European Union,* 2012a. Accessed 19.05.2020. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF

European Union. "Consolidated version of the Treaty on the Functioning of the European Union”, *European Union,* 2012b. Accessed 19.05.2020. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_2&format=PDF

European Union. “The EU in brief”, *European Union*¸ 2020a. Accessed 19.05.2020. Available at: https://europa.eu/european-union/about-eu/eu-in-brief_en

European Union. “Countries”, *European Union*¸ 2020b. Accessed 19.05.2020. Available at: https://europa.eu/european-union/about-eu/countries_en

European Union. “Goals and Values of the EU”, *European Union,* 2020c. Accessed 29.04.2020. Available at: https://europa.eu/european-union/about-eu/eu-in-brief_en

EUROPOL. “TE-SAT 2016”, *EUROPOL,* 2016. Accessed 13.05.2020. Available at: https://www.europol.europa.eu/sites/default/files/documents/europol_tesat_2016.pdf

EUROPOL. “TE-SAT 2018”, *EUROPOL,* 2018. Accessed 13.05.2020. Available at: https://www.europol.europa.eu/sites/default/files/documents/tesat_2018_1.pdf

EUROPOL. “Internet Organised Crime Threat Assessment (iOCTA) 2019”, *EUROPOL,* 2019. Accessed 13.05.2020. Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

Garfinkel, Ben and Allan Dafoe. ”How Does the Offense-Defense Balance Scale?”, *Journal of Strategic Studies*, Vol. 42, No. 6 (2019): 736-763

Gartzke, Erik. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth”, *International Security,* Vol. 38, No. 2 (2013): 41-73

Gergely, Szentgáli. ”The NATO Policy on Cyber Defence: The Road so Far”, *AARMS*, Vol. 12, No. 1 (2013): 83-91

Giantas, Dominika. “Cybersecurity in the EU: Threats, Framework and Future Perspectives”. Laboratory of Intelligence & Cyber-Security, University of Piraeus, 2019. Accessed 15.03.2020. Available at: https://www.researchgate.net/publication/335909463_Cybersecurity_in_the_EU_Threats_frameworks_and_future_perspectives

Gibson Dunn. ”The EU Introduces a New Sanctions Framework in Response to Cyber-Attack Threats”, *Gibson Dunn, 2019.* Accessed 07.04.2020. Available at: https://www.gibsondunn.com/eu-introduces-new-sanctions-framework-in-response-to-cyber-attack-threats/#_edn4

Glaser, Charles L. “Deterrence of Cyber Attacks and U.S. National Security”, *The George Washington University*, 2011

Glaser, Charles L. and Chaim Kaufmann. “What Is The Offense-Defense Balance And How Can We Measure It?”, *Offense, Defense, and International Politics,* Vol. 22 No. 4 (1998): 44-82

Goodman, Will. “Cyber Deterrence – Tougher in Practice than in Theory?”, *Strategic Studies* Quarterly, Vol. 4, No. 3 (Fall 2010): 102-135

Goychayev, R. et al. *Cyber Deterrence and Stability*. Washington: Pacific Northwest National Laboratory, 2017

Goździewicz, Wiesław “From Riga to Wales. NATO’s Road to Collective Cyberdefence”, in *NATO Road to Cybersecurity*, edited by Joanna Świątkowska, 11-16, 2016. Accessed 15.04.2020. Available at: https://www.academia.edu/39600685/NATO_Road_to_Cybersecurity

Gressel, Gustav. ”Protecting Europe Against Hybrid Threats”, *European Council on Foreign Relations*, 2019. Accessed 18.03.2020. Available at: https://www.ecfr.eu/publications/summary/protecting_europe_against_hybrid_threats

Healey, Jason and Klara Tothova Jordan. "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow", *Atlantic Council – IssueBrief*, 2014. Accessed 12.03.2020. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf

Herz, John H. "Political Ideas and Political Reality", *The Western Political Quarterly*, Vol. 3, No. 2 (1950): 161-178

Iasiello, Emilio. " Is Cyber Deterrence an Illusory Course of Action?", *Journal of Strategic Security*, Vol. 7, No. 1 (2014): 54-67

Jervis, Robert. "Cooperation Under the Security Dilemma", *World Politics*, Vol. 30, No. 2 (Jan., 1978): 167-214

Jervis, Robert. "Deterrence Theory Revisited", *World Politics*, Vol. 31, No. 2 (1979): 289-324

Jervis, Robert, Richard Ned Lebow and Janice Gross Stein. *Psychology and Deterrence*. Baltimore MD: Johns Hopkins University Press, 1985

Jervis, Robert. "From Balance to Concert: A Study of International Security Cooperation", *World Politics*, Vol. 38, No. 1 (Oct., 1985): 58-79

Jørgensen, Knud Erik. *International Relations Theory: A New Introduction.* London: Palgrave, 2nd edition, 2018

Kamp, Karl-Heinz. "Why NATO Needs a New Strategic Concept", *Research Division NATO Defence College*, 2016. Accessed 03.05.2020. Available at: http://www.ndc.nato.int/news/news.php?icode=997

Kennedy, Brianna L. "Deduction, Induction, and Abduction" In *The SAGE Handbook of Qualitative Data Collection*, edited by Uwe Flick, 49-64. Thousand Oaks: SAGE Publications, Inc., 2018

Keohane, Robert O. and Lise L. Martin. "The Promise of Institutionalist Theory", *International Security*, Vol. 20, No. 1 (Summer, 1995): 39-51

Keohane, Robert O. and Joseph S. Nye. *Power and Interdependence*. New York: Longman, 4th edition, 2012

Knopf, Jeffrey W. “The Fourth Wave in Deterrence Research”, *Contemporary Security Policy*, Vol. 31, No.1 (2010): 1-33

Koenig, Nicole. ” The EU and NATO: A Partnership with a Glass Ceiling”, *EU Global Strategy Watch*, 2018. Accessed 08.05.2020. Available at: https://www.iai.it/sites/default/files/eugs_watch_8.pdf

Kovács, László. “Cyber Security Policy and Strategy in the European Union and NATO”, *Land Forces Academy Review*, Vol 89., No. 1 (2018): 16-24

Lacity, Mary C. and Marius A. Janson. “Understanding qualitative data: A framework of text analysis methods”. Journal of Management Information Systems, Vol. 11, No. 2, (Fall 1994): 137-152

Legendre, Thierry. ” NATO’s Cooperation with the EU doesn’t work and it doesn’t really matter … yet!” in *DIIS Report – Cooperative Security: NATO’s Partnership Policy in a Changing World*, edited by Trine Flockhart, 121-131, 2014. Accessed 10.04.2020. Available at: https://pure.diis.dk/ws/files/58169/WP2014_01_NATO_tfl_web.pdf

Lété, Bruno. “Cooperation in Cyberspace” In The *EU and NATO: The Essential Partners*, edited by Gustav Lindstrom and Thierry Tardy, 28-36. European Union Institute for Security Studies: Paris, 2019

Lété, Bruno and Piret Pernik. ”EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions”, *The German Marshall Fund of the United States, Security and Defence Policy*, No. 38, 2017. Accessed 08.05.2020. Available at: https://www.gmfus.org/publications/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions

Lewis, James A. “Reconsidering Deterrence in Cyberspace”, *Center for Strategic and International Studies* (October 2013): 1-8

Lewis, James A. “The Role of Offensive Cyber Operations in NATO’s Collective Defence”, *The Tallinn Papers*, No. 8, 2015

Libicki, Martin C. “Cyberdeterrence and Cyberwar”, *Project Air Force - RAND Corporation*, 2009

Libicki, Martin C. ”Is There a Cybersecurity Dilemma?”, *The Cyber Defense Review*, Vol. 1, No. 1 (Spring 2016): 129-140

Lindstrom, Gustav. ”Emerging Cybersecurity Challenges” in *Handbook on Cybersecurity: The Common Security and Defence Policy of the European Union* edited by Jochen Rehrl, 156-165, as part of *European Security and Defence College* and *Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria*, 2018. Accessed 20.03.2020. Available at: https://op.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1

Lockyer, Sharon. ”Textual Analysis” In *The SAGE Encyclopedia of Qualitative Research Methods*, edited by Lisa M. Given, 865-866. Thousand Oaks: SAGE Publications, Inc., 2008

Lungescu, Oana. “DDoS attack”, Twitter, March 16, 2014. Available at: https://twitter.com/NATOpress/status/445112624578306048

Lynn III, William J. “Defending a New Domain: The Pentagon's Cyberstrategy”, *Foreign Affairs*, Vol. 89, No. 5 (2010): 97-108

Maldre, Patrick. “Moving Towards NATO Deterrence for the Cyber Domain”, *CEPA – Cyber Intelligence Briefing No. 1,* 2016. Accessed 12.04.2020. Available at: https://cepa.ecms.pl/files/?id_plik=2446

Mälksoo, Maria. “Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO”, *European Security*, Vol. 27, No. 3 (2018): 374-392

Malwarebytes. “What is a Backdoor?”. *Cybersecurity Basics*, 2020. Accessed 21.02.2020. Available at: https://www.malwarebytes.com/backdoor/

Mauer, Tim. “Cyber Proxies and The Crisis in Ukraine”, In *Cyber War in Perspective: Russian Aggression Against Ukraine,* edited by Kenneth Geers, 78-86. NATO CCDCOE, 2015

Maxwell, Joseph A. *Qualitative Research Design: An Interactive Approach.* London: Sage Publications, 1996

Maxwell, Joseph A. *A Realist Approach for Qualitative Research.* Thousand Oaks: SAGE Publications, Inc., 2011

Mazarr, Michael J. “Understanding Deterrence”, *RAND Corporation*, 2018. Accessed 10.01.2020. Available at: https://www.rand.org/pubs/perspectives/PE295.html

McConnell, Michael J. “Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee”, 27 February 2008. Accessed 02.02.2020. Available at: https://www.dni.gov/files/documents/Newsroom/Testimonies/20080227_testimony.pdf

Mearsheimer, John. *The Tragedy of Great Power Politics*. New York: W. W. Norton & Company, 2001

Meer, Sico van der. “EU Creates a Diplomatic Toolbox to Deter Cyberattacks”, *Council of Foreign Relations*, 2017. Accessed 20.03.2020. Available at: https://www.cfr.org/blog/eu-creates-diplomatic-toolbox-deter-cyberattacks

Milja, Kurki. “Critical Realism and Causal Analysis in International Relations”. *Millenium – Journal of International Studies,* Vol. 35, No. 2 (2007): 361 - 378

Mills, Melinda C. “Comparative Analysis” In *The SAGE Encyclopedia of Qualitative Research Methods,* edited by Lisa M. Given, 100-101. Thousand Oaks: SAGE Publications, Inc., 2008

Minárik, Tomáš. “NATO Recognises Cyberspace as a ‘Domain of Operations’ at Warsaw Summit”, *NATO CCDCOE,* 2016. Accessed 15.04.2020. Available at: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

Missiroli, Antonio. ”The Cyberhouse Rules: Resilience, Deterrence and Defence in Cyberspace”, *Italian Institute for International Political Studies*, 2018. Accessed 12.04.2020. Available at: https://www.ispionline.it/it/pubblicazione/cyberhouse-rules-resilience-deterrence-and-defence-cyberspace-20378

Moret, Erica and Patryk Pawlak. “The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?” *European Union, Institute for Security Studies*, 2017. Accessed 05.04.2020. Available at: https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime

Morgenthau, Hans J. *Politics Among Nations: The Struggle for Power and Peace.* New York: Alfred A. Knopf Inc., 1948

NATO. “The North Atlantic Treaty”, *NATO,* 1949. Accessed 19.04.2020. Available at: https://www.nato.int/cps/en/natolive/official_texts_17120.htm

NATO. “Lisbon Summit Declaration”, *NATO,* 2010a. Accessed 11.04.2020. Available at: https://www.nato.int/cps/en/natolive/official_texts_68828.htm

NATO. ”Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization”, *NATO,* 2010b. Accessed 11.04.2020. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

NATO. “Defending the networks The NATO Policy on Cyber Defence”, *NATO*, 2011. Accessed 11.04.2020. Available at: https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf

NATO. ”Wales Summit Declaration”, *NATO,* 2014a. Accessed 12.03.2020. Available at: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO. ”Press Conference by NATO Secretary General Anders Fogh Rasmussen following the meeting of the North Atlantic Council at the level of Heads of State and Government during the NATO Wales Summit”, *NATO¸* 2014b. Accessed 12.03.2020. Available at: https://www.nato.int/cps/en/natohq/opinions_112871.htm

NATO. “Joint press point with NATO Secretary General Jens Stoltenberg and Sven Mikser, Minister of Defence of Estonia”, *NATO,* 2014c. Accessed 21.04.2020. Available at: https://www.nato.int/cps/en/natohq/opinions_115063.htm

NATO. “Secretary General statement on the so-called referendum in Ukraine’s Autonomous Republic of Crimea”, *NATO,* 2014d. Accessed 21.04.2020. Available at: https://www.nato.int/cps/en/natolive/news_108021.htm

NATO. ”NATO Cyber Defence. Fact Sheet”, *NATO*, 2016a. Accessed 12.03.2020. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf

NATO. ”Cyber Defence Pledge”, *NATO,* 2016b. Accessed 12.03.2020. Available at: https://www.nato.int/cps/su/natohq/official_texts_133177.htm

NATO. ”Warsaw Summit Communiqué”, *NATO*, 2016c. Accessed 12.03.2020. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO. ”Press conference by NATO Secretary General Jens Stoltenberg following the North Atlantic Council meeting at the level of NATO Defence Ministers”, *NATO*¸2016d. Accessed 12.03.2020. Available at: https://www.nato.int/cps/en/natohq/opinions_132349.htm

NATO. “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”, *NATO,* 2016e. Accessed 08.05.2020. Available at: https://www.nato.int/cps/en/natohq/official_texts_133163.htm

NATO. “Doorstep by NATO Secretary General Jens Stoltenberg prior to the informal meeting of EU Ministers of Defence, Tallinn, Estonia”, *NATO,* 2017. Accessed 03.05.2020. Available at: https://www.nato.int/cps/en/natohq/opinions_146642.htm?selectedLocale=en.

NATO. “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”, *NATO,* 2018a. Accessed 08.05.2020. Available at: https://www.nato.int/cps/en/natohq/official_texts_156626.htm

NATO “Third progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017” *NATO,* 2018b. Accessed 20.06.2020. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_180608-3rd-Joint-progress-report-EU-NATO-eng.pdf

NATO. “Cyber defense”. *NATO,* 2019a. Accessed 07.02.2020. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO “Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017” *NATO,* 2019b. Accessed 20.06.2020. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf

NATO. “NATO Member Countries”, *NATO,* 2020a. Accessed 08.05.2020. Available at: https://www.nato.int/cps/en/natohq/nato_countries.htm

NATO. “Partners”, *NATO,* 2020b. Accessed 08.05.2020. Available at: https://www.nato.int/cps/en/natohq/51288.htm

NATO. “Relations with the European Union”, *NATO*, 2020c. Accessed 08.05.2020. Available at: https://www.nato.int/cps/en/natohq/topics_49217.htm

NATO. “Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017” *NATO*, 2020d. Accessed 20.06.2020. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200615-progress-report-nr5-EU-NATO-eng.pdf

Nazario, Jose. “Politically Motivated Denial of Service Attacks” In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck and Kenneth Geers, 163-181. IOS Press: Amsterdam, 2009.

Nye, Joseph S. “Cyber Power”, *Belfer Center for Science and International Affairs*, 2010

Nye, Joseph S. “Deterrence and Dissuasion in Cyberspace”, *International Security*, Vol. 41, No. 3 (2017): 44-71

Nyemann, Dorthe Bach. “Cybermagt er spoilermagt - Hvordan tæmmer vi våbenkapløbet i cyberspace og hæmmer destabiliseringen af internationale relationer?”, *Forsvarsakademiet*, 2018

O’Mahoney, Joe and Steve Vincent. “Critical Realism as an Empirical Project” In *Studying Organizations Using Critical Realism: A Practical Guide*, edited by Paul K. Edwards, Joe O'Mahoney, and Steve Vincent, 1-20. Oxford: Oxford University Press, 2014.

Pawlak, Patryk. “Countering hybrid threats: EU-NATO cooperation”, *European Parliament Think Tank*, 2017. Accessed 08.05.2020. Available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2017)599315

Pawlak, Patryk. “Protecting and defending Europe’s cyberspace“ In *Chaillot Paper No. 148*, edited by Nicu Popescu and Stanislav Secrieru, 103-114, *European Union, Institute for Security Studies*, 2018

Pernik, Piret. “Improving Cyber Security: NATO and the EU”, *International Centre for Defence Studies*¸ 2014. Accessed 20.03.2020. Available at: https://icds.ee/improving-cyber-security-nato-and-the-eu/

Pernik, Piret and Tomas Jermalavičius. ” Resilience as Part of NATO’s Strategy: Deterrence by Denial and Cyber Defense”, *International Centre for Defence and Security*, 2016. Accessed

12.03.2020. Available at: https://icds.ee/resilience-as-part-of-natos-strategy-deterrence-by-denial-and-cyber-defence/

Petallides, Constantine J. “Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat”, *Inquiries Journal*, Vol. 4, No. 3 (2012)

Philbin, Michael J. “Cyber Deterrence: An Old Concept in a New Domain”. *U.S. Army War College*, 2013

Pijnenburg, Lilly Muller and Tim Stevens. “Upholding the NATO Cyber Pledge. Cyber Deterrence and Resilience: Dilemmas in NATO Defence and Security Policies”, *Norwegian Institute of International Affairs*, 2017. Accessed 15.04.2020. Available at: https://www.nupi.no/en/Publications/CRIStin-Pub/Upholding-the-NATO-cyber-pledge-Cyber-Deterrence-and-Resilience-Dilemmas-in-NATO-defence-and-security-politics

Porter, Christopher B. “Collective Defense of Human Dignity: The Vision for NATO’s Future in Cyberspace”, *Atlantic Council, Issue Brief*, 2019. Accessed 19.05.2020. Available at: https://www.jstor.org/stable/resrep20714?seq=1#metadata_info_tab_contents

Prior, Lindsay F. “Document Analysis” In *The SAGE Encyclopedia of Qualitative Research Methods*, edited by Lisa M. Given, 231-232. Thousand Oaks: SAGE Publications, Inc., 2008

Raik, Kristi and Pauli Järvenpää. ”A New Era of EU-NATO Cooperation How to Make the Best of a Marriage of Necessity”, *International Centre for Defence and Security*, 2017. Accessed 08.05.2020. Available at: https://icds.ee/a-new-era-of-eu-nato-cooperation-how-to-make-the-best-of-a-marriage-of-necessity-2/

Ranger, Steve. ”NATO updates cyber defence policy as digital attacks become a standard part of conflict”, *ZDNet*, 2014. Accessed 14.04.2020. Available at: https://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/

Renard, Thomas and André Barrinha. ” The EU as a partner in cyber diplomacy and defence” in *Handbook on Cybersecurity: The Common Security and Defence Policy of the European Union* edited by Jochen Rehrl, 180-189, as part of *European Security and Defence College* and *Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria*, 2018. Accessed 20.03.2020. Available at: https://op.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1

Rid, Thomas. “Cyber War Will Not Take Place”, *Journal of Strategic Studies*, Vol. 35, No. 1 (2012): 5-32

Robinson, Neil. “NATO: Changing gear on cyber defence”, *NATO,* 2016. Accessed 19.04.2020. Available at: https://www.nato.int/docu/review/articles/2016/06/08/nato-changing-gear-on-cyber-defence/index.html

Robinson, Neil. “Cyber Defense at NATO: From Wales to Warzaw, and Beyond”, *Turkish Policy Quarterly,* Vol. 16, No. 3 (2017): 133-143

Royal Danish Defense College. “Joint Doctrine for Military Cyberspace Operations”. *Royal Danish Defense College*, 2019

Rugge, Fabio. ”The case for NATO-EU cooperation in the protection of cyberspace”, *Conference Paper: Third Worldwide Cybersecurity Summit*, 2012. Accessed 08.05.2020. Available at: https://ieeexplore.ieee.org/document/6780880

Ryan, N. J. “Five Kinds of Cyber Deterrence”, *Philosophy & Technology*, Vol. 31, No. 3 (2017): 331-338

Saltzman, Ilai. “Cyber Posturing and the Offense-Defense Balance”, *Contemporary Security Policy*, Vol. 34, No. 1 (2013): 40-63

Savin, Dorin. ”Consideration Regarding NATO and European Union Relationship”, *Research and Science Today,* No. 1 (2019): 37-45

Sayer, Andrew. *Realism and Social Science.* Thousand Oaks: SAGE Publications, Inc., 2000

Scheffer, Jaap de Hoop. “Strengthening the EU’s Cyber Defence Capabilities”, *CEPS Task Force,* 2018. Accessed 15.03.2020. Available at: https://www.ceps.eu/ceps-publications/strengthening-eus-cyber-defence-capabilities/

Schelling, Thomas. *Arms and Influences*. New Haven: Yale University Press, 1995

Schmitt, Michael N, *Tallinn Manual 2.0: On the IL Applicable to Cyber Operations, 2nd ed.*, Cambridge: Cambridge University Press, 2017

Schulze, Matthias. “Cyber Deterrence is Overrated”, *German Institute for International and Security Affairs*, No. 34 (2019)

Shea, Jamie. ”How is NATO Meeting the Challenge of Cyberspace?”, *PRISM: The Fifth Domain¸* Vol. 7, No. 2 (2017a): 18-29

Shea, Jamie. “NATO: Stepping up its game in cyber defence”, *Cyber Security*, Vol. 1, No. 2 (2017b): 165-174

Shea, Jamie. “Building Cyber Resilience: Aligning Strategies and Increasing Cooperation”, *Friends of Europe*, 2018. Accessed 04.05.2020. Available at: https://www.friendsofeurope.org/events/building-cyber-resilience-aligning-strategies-and-increasing-cooperation/

Signoretti, Massimiliano. “European Parliament lists priorities for cyber defence and highlights cooperation with NATO”, *NATO CCDCOE*, 2019. Accessed 18.01.2020. Available at: https://ccdcoe.org/incyder-articles/european-parliament-lists-priorities-for-cyber-defence-and-highlights-cooperation-with-nato/

Singer, Peter W. and Kenneth Lieberthal. “Cybersecurity and U.S. – China Relations”, *21st Century Defense Initiative*, 2012

Slayton, Rebecca. “What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment”, *International Security*, Vol. 41, No. 3 (2017): 72-109

Sliwinski, Krzysztof Feliks. ” Moving beyond the European Union's weakness as a cyber-security agent”, *Contemporary Security Policy*, Vol. 35, No. 3 (2014): 468-486

Smith, Hanna. “Countering hybrid threats” In The *EU and NATO: The Essential Partners*, edited by Gustav Lindstrom and Thierry Tardy, 13-20. European Union Institute for Security Studies: Paris, 2019

Štitilis Darius, Paulius Pakutinskas and Inga Malinauskaitė. “EU and NATO Cybersecurity Strategies and National Cyber Security Strategies: a Comparative Analysis”, *Security Journal*, Vol. 30, No. 4 (2017): 1151-1168

Stoltenberg, Jens. ”The Secretary General’s Annual Report 2018”, *NATO*, 2018. Accessed 12.03.2020. Available at: https://www.nato.int/cps/en/natohq/opinions_164187.htm

Strauss, Anselm L. *Qualitative analysis for social scientists.* Cambridge: Cambridge University Press, 1987

Taddeo, Mariarosaria. “How to Deter in Cyberspace”, *Strategic Analysis,* The European Centre of Excellence for Countering Hybrid Threats, (June-July 2018): 1-9

Taipale, K. A., “Cyber-Deterrence”. *Law, Policy and Technology: Cyberterrorism, Information, Warfare, Digital and Internet Immobilization,* 2009

Tardy, Thierry and Gustav Lindstrom. “The Scope of EU-NATO Cooperation” In The *EU and NATO: The Essential Partners*, edited by Gustav Lindstrom and Thierry Tardy, 5-12. European Union Institute for Security Studies: Paris, 2019

Theiler, Olaf. “New threats: the cyber-dimension”, *NATO,* 2011. Accessed 19.04.2020. Available at: https://www.nato.int/docu/review/articles/2011/09/04/new-threats-the-cyber-dimension/index.html

Tiirmaa-Klaar, Heli. ”Two Generations of EU Cybersecurity Strategies” in *Handbook on Cybersecurity: The Common Security and Defence Policy of the European Union* edited by Jochen Rehrl, 18-26, as part of *European Security and Defence College* and *Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria*, 2018. Accessed 20.03.2020. Available at: https://op.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1

Tolga, İhsan Burak. “Principles of Cyber Deterrence and the Challenges in Developing a Credible Cyber Deterrence Posture”, NATO CCD COE Publications, Tallinn (2018): 1-21

Tor, Uri. “‘Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence”, *Journal of Strategic Studies*, 40, no. 1-2 (2017): 92-117

Tropeano, Rosemary. “Deterrence in Cyber, Cyber in Deterrence”, *RealClearDefense*, 2019. Accessed 22.01.2020. Available at: https://www.realcleardefense.com/articles/2019/05/28/deterrence_in_cyber_cyber_in_deterrence_114456.html

Waltz, Kenneth N. *Theory of International Politics*. New York: McGraw-Hill, Inc., 1979

Wivel, Anders. “Realismen efter Waltz: Udvikling eller Afvikling?”, *Politica*, Vol. 34, No. 4 (2002): 431-448

Yağlı Serkan and Selçuk Dal. "Active Cyber Defense within the Concept of NATO's Protection of Critical Infrastructures", *International Journal of Computer and Systems Engineering*, Vol. 8, No. 4 (2014): 909-913

Appendix 1

Carrapico, Helena and André Barrinha. "The EU as a Coherent (Cyber)Security Actor?", *Journal of Common Market Studies*, Vol. 55, No. 6 (2017): 1254-1272

Christou, George. "The EU's Approach to Cyber Security", *EU-China Security Cooperation - Policy Paper*, 2014

Christou, George. *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*. New York: Palgrave MacMillan, 2016

Cirlig, Carmen-Cristina. "Cyber defence in the EU Preparing for cyber warfare?", *European Parliament,* 2014

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

European Commission. "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". SEC 399, 2009

European Commission. "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". JOIN 1 final, 2013

European Commission. "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU". JOIN 450 final, 2017a

European Commission. "Reflection paper on the future of European Defence", *European Commission*, 2017b

European Commission. "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL - Increasing resilience and bolstering capabilities to address hybrid threats". JOIN 16 final, 2018

European Commission. "Cybersecurity". *European Union*, 2020

European Court of Auditors. ”Challenges to Effective EU Cybersecurity Policy”, *European Court of Auditors*, 2019

European External Action Service. “Shared Vision, Common Action: A Stronger Europe”, *European External Action Service,* 2017

European Parliament. “Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union”, *European Parliament and the Council of the European Union,* 2016

European Parliament. “Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and Risks for the EU”, *European Parliament*, 2017

European Parliament. “Foreign influence operations in the EU”. *European Union,* 2018a

European Parliament. ”Cyber defence”, *European Union,* 2018b

European Parliament. “Stepping up EU cyber defence and cooperation with NATO”, *European Union,* 2018c

European Parliament. “Cyber: How big is the threat?”. *European Union,* 2019

Giantas, Dominika. “Cybersecurity in the EU: Threats, Framework and Future Perspectives”. Laboratory of Intelligence & Cyber-Security, University of Piraeus, 2019

Gressel, Gustav. ”Protecting Europe Against Hybrid Threats”, *European Council on Foreign Relations*, 2019

Pawlak, Patryk. “Countering hybrid threats: EU-NATO cooperation”, *European Parliament Think Tank,* 2017

Pawlak, Patryk. “Protecting and defending Europe’s cyberspace“ In *Chaillot Paper No. 148,* edited by Nicu Popescu and Stanislav Secrieru, 103-114, *European Union, Institute for Security Studies,* 2018

Pernik, Piret. “Improving Cyber Security: NATO and the EU”, *International Centre for Defence Studies*¸ 2014

Scheffer, Jaap de Hoop. “Strengthening the EU’s Cyber Defence Capabilities”, *CEPS Task Force,* 2018

Sliwinski, Krzysztof Feliks. " Moving beyond the European Union's weakness as a cyber-security agent", *Contemporary Security Policy*, Vol. 35, No. 3 (2014): 468-486

Smith, Hanna. "Countering hybrid threats" In The *EU and NATO: The Essential Partners,* edited by Gustav Lindstrom and Thierry Tardy, 13-20. European Union Institute for Security Studies: Paris, 2019

Tardy, Thierry and Gustav Lindstrom. "The Scope of EU-NATO Cooperation" In The *EU and NATO: The Essential Partners,* edited by Gustav Lindstrom and Thierry Tardy, 5-12. European Union Institute for Security Studies: Paris, 2019

Tardy, Thierry and Gustav Lindstrom. "The scope of EU-NATO cooperation" In The *EU and NATO: The Essential Partners*, edited by Gustav Lindestrom and Thierry Tardy, 5-12. European Union Institute for Security Studies: Paris, 2019

Tiirmaa-Klaar, Heli. "Two Generations of EU Cybersecurity Strategies" in *Handbook on Cybersecurity: The Common Security and Defence Policy of the European Union* edited by Jochen Rehrl, 18-26, as part of *European Security and Defence College* and *Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria*, 2018

Appendix 2

Alatalu, Siim. “NATO’s responses to cyberattacks“, In *Chaillot Paper No. 148,* edited by Nicu Popescu and Stanislav Secrieru, 103-114, *European Union, Institute for Security Studies*, 2018

Alexander, Dean C. “Cyber Threats Against the North Atlantic Treaty Organization (NATO) and Selected Responses”. *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi*, 2014

Besch, Sophia. “Protecting European networks: What can NATO do?”, *Centre for European Reform – Insight*, 2018.

Burton, Joe. “NATO’s Cyber Defence: Strategic Challenges and Institutional Adaptation”, *Defence Studies*, Vol. 15, No. 4 (2015): 297-319

Davis, Susan. ”NATO in the Cyber Age : Strengthening Security and Defence, Stabilizing Deterrence”, *NATO Parliamentary Assembly, Science and Technology Committee*, 2019

Efthymiopoulos, Marios Panagiotis. “A cyber-security framework for development, defense and innovation at NATO”, Journal of Innovation and Entrepreneurship, Vol. 8, No. 12 (2019): 1-26

Gergely, Szentgáli. ”The NATO Policy on Cyber Defence: The Road so Far”, *AARMS*, Vol. 12, No. 1 (2013): 83-91

Healey, Jason and Klara Tothova Jordan. “NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow”, *Atlantic Council – IssueBrief*, 2014

Lewis, James A. “The Role of Offensive Cyber Operations in NATO’s Collective Defence”, *The Tallinn Papers*, No. 8, 2015

Maldre, Patrick. “Moving Towards NATO Deterrence for the Cyber Domain”, *CEPA – Cyber Intelligence Briefing No. 1*, 2016

Mälksoo, Maria. “Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO”, *European Security*, Vol. 27, No. 3 (2018): 374-392

Missiroli, Antonio. ”The Cyberhouse Rules: Resilience, Deterrence and Defence in Cyberspace”, *Italian Institute for International Political Studies*, 2018

NATO. “Lisbon Summit Declaration”, *NATO*, 2010a

NATO. “Defending the networks The NATO Policy on Cyber Defence”, *NATO*, 2011

NATO. ”Wales Summit Declaration”, *NATO,* 2014a

NATO. “Joint press point with NATO Secretary General Jens Stoltenberg and Sven Mikser, Minister of Defence of Estonia”, *NATO,* 2014c

NATO. “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”, *NATO,* 2016a

NATO. ”Warsaw Summit Communiqué”, *NATO*, 2016c

NATO. ”Press conference by NATO Secretary General Jens Stoltenberg following the North Atlantic Council meeting at the level of NATO Defence Ministers”, *NATO¸*2016d

NATO. “Doorstep by NATO Secretary General Jens Stoltenberg prior to the informal meeting of EU Ministers of Defence, Tallinn, Estonia”, *NATO,* 2017

NATO. “Cyber defense”. *NATO,* 2019

Pernik, Piret and Tomas Jermalavičius. ” Resilience as Part of NATO’s Strategy: Deterrence by Denial and Cyber Defense”, *International Centre for Defence and Security,* 2016

Porter, Christopher B. “Collective Defense of Human Dignity: The Vision for NATO’s Future in Cyberspace”, *Atlantic Council, Issue Brief,* 2019

Robinson, Neil. “NATO: Changing gear on cyber defence”, *NATO,* 2016

Robinson, Neil. “Cyber Defense at NATO: From Wales to Warzaw, and Beyond”, *Turkish Policy Quarterly,* Vol. 16, No. 3 (2017): 133-143

Shea, Jamie. ”How is NATO Meeting the Challenge of Cyberspace?”, *PRISM: The Fifth Domain¸* Vol. 7, No. 2 (2017a): 18-29

Shea, Jamie. “NATO: Stepping up its game in cyber defence”, *Cyber Security,* Vol. 1, No. 2 (2017b): 165-174

Smith, Hanna. “Countering hybrid threats” In The *EU and NATO: The Essential Partners,* edited by Gustav Lindstrom and Thierry Tardy, 13-20. European Union Institute for Security Studies: Paris, 2019

Theiler, Olaf. “New threats: the cyber-dimension”, *NATO,* 2011

Yağlı Serkan and Selçuk Dal. "Active Cyber Defense within the Concept of NATO's Protection of Critical Infrastructures", *International Journal of Computer and Systems Engineering*, Vol. 8, No. 4 (2014): 909-913