Tøger Bøe Helgesen

Modern cyber responses to cyber security threats: EU, NATO and Norwegian strategic responses.

Bachelor's project in European Studies with Political Science.
Supervisor: Viktoriya Fedorchak
May 2020

Bachelor's project

NTNU
Norwegian University of Science and Technology
Faculty of Humanities
Department of Historical Studies

NTNU
Norwegian University of
Science and Technology

Tøger Bøe Helgesen

Modern cyber responses to cyber security threats: EU, NATO and Norwegian strategic responses.

Bachelor’s project in European Studies with Political Science.
Supervisor: Viktoriya Fedorchak
May 2020

Norwegian University of Science and Technology
Faculty of Humanities
Department of Historical Studies

NTNU
Norwegian University of
Science and Technology

Abstract:

Cyberspace is continuously evolving, and actors across the world need to be able to adapt, react and respond to this evolvement. This thesis presents a study where the EU and NATO's cyber strategies are analysed in a comparative analysis. The purpose of this is to illustrate what differences there are between the two units of analysis. The thesis will also include a case study of Norwegian cyber security, and how these strategies are affected by the differences that are provided in the EU-NATO comparative analysis. The thesis reveals that there are distinct differences between the two organizations in terms of how they arrange their cyber strategies. Even though they have similar objectives, namely establishing an effective cyberstrategy, the EU and NATO show that they have different approaches and ways of achieving said effective cyber strategy. Lastly, the thesis reveals clear indications that Norway's cyberstrategies are affected by NATO and the EU. This is illustrated in part by Norway's adoption of EU cyber security policies and military enhancements done as a result of NATO's focus on interoperability.

Cyberspace er under konstant utvikling, og aktører over hele verden må være villige til å tilpasse seg, reagere og svare på denne utviklingen. Denne avhandlingen presenterer en studie hvor EU og NATO sine cyber strategier blir analysert ved bruk av en komparativ analyse. Avhandlingen inkluderer også en casestudie av norske cyber strategier, og hvordan disse blir påvirket av forskjellene man finner i den komparative analysen. Avhandlingen viser at det er distinkte forskjeller mellom de to organisasjonene i form av hvordan de utarbeider sine cyber strategier. Selv om de har lignende mål, nemlig det å etablere en effektiv cyberstrategy, viser EU og NATO at de har forskjellige tilnærminger og metoder for å oppnå disse effektive cyberstrategiene. Til slutt avslører oppgaven tydelige indikasjoner på at Norges cyberstrategier er påvirket av NATO og EU. Dette illustreres delvis av Norges evne til å adoptere EU sin cybersikkerhetspolitikk og de militære forbedringene som er blitt gjennomført som et resultat av NATOs fokus på interoperabilitet.

Table of contents

1. Introduction.

1.1. Introducing the topic:

Cyber threats are proceeding to develop and evolve, NATO (North Atlantic Treaty Organization) stated in early 2019 (NATO, 2019). These threats are becoming more complex, destructive and frequent, and illustrate the need for cooperation between national governments, various alliances, and organizations.

Ever since the events that took place on the 11th of September 2001[1], a lot of people saw international terrorism as the greatest threat towards democracy and peace. This initiated a two decade long military conflict in the middle east, which still has seen no official end. For me, coming from a military family with a father who served several tours overseas with the Norwegian Army´s Telemark Battalion [2], I´ve found that during the years, threats that might lead to military involvement, are of great interest and importance to me and my family, as it may result in my father being deployed once again.

As of now, these views on security challenges, might have changed, at least in the eyes of the Norwegian foreign intelligence service. Each year, the Norwegian intelligence service, issue an assessment of the current security challenges that face Norway. Based on the assessment of the Norwegian foreign intelligence service, China and Russia are the two big actors affecting Norway and its interests, with technological advancement and its usage as an alternative to military force/involvement.

This thesis aims to illustrate exactly this. Cyber threats and cyber warfare as the new challenge that governments, alliances and organizations has to solve. One will look more closely at how NATO, the European Union and Norway, handle this cyber threat, and if there is any sort of division of responsibilities when it comes to the safety and security of one's citizens.

1.2. Presentation of the research question and the given timeframe:

In this thesis, the main focus will be on NATO, the EU, and Norway. The cyber threat in focus will be that of Cyber warfare, focusing on state on state cyber-attacks. Are we seeing a more effective form of Hybrid warfare with the development of technology? One will look more closely at the cooperation between the EU and their member states, NATO and Norway, and how this possible cooperation plays out in more practical terms.
One will look at what has been documented, and what various armies and alliance are in fact doing, and what their capabilities are.

The research question (RQ) in this thesis will therefore be: *What are the differences in EU-NATO cyberstrategy, and how do these affect Norway´s cyberstrategy?*

In order to answer the RQ in the best possible way, the timeframe will be limited to the period between 2013 to the present date. The main reason for this timeframe, is because during that time, cyberthreats have been more and more prioritized in terms of how to protect oneself from them. The Norwegian foreign intelligence service issued an

[1] Organized terrorist attack made by al-Qaeda against the United States
[2] Mechanised infantry unit of the Norwegian Army

assessment as early as 2013, stating that multiple superpowers[3] are preparing to use digital operations as a tool when it comes to solving conflicts (Forsvaret, 2013).
In 2012, Russia also issued several documents that indicated a continuous focus on cyber security, but also the fact that cyber-attacks will be seen as a declaration of war (Forsvaret, 2013).
Thus, the timeframe will be limited to the years following this statement as they illustrate the relevance of the cyberthreat to the contemporary security environment/situation.

One will also use various sub-questions to further answer the RQ such as:

- What is the European Union's approach to the continuous evolvement of cyber threats?
- What steps are NATO taking, in order to tackle the cyber threats?
- How do these two approaches regarding the rising cyber threats compare to each other, and how to these approaches affect Norway, and *its* approach to the rising threat of technological advancement with cyber warfare at its forefront?

Member states of both NATO and the EU with regards to their national armies will be explored in order to see in more practical terms how the given strategies of both the EU and NATO are actually working. The same will be done for Norway and its intelligence service and other branches of the Norwegian military.

2.0. Methodology.

2.1. Method:

Primarily, this thesis will use a qualitative case study as its research design. There will be a total of three main units of analysis, them being NATO, Norway and the EU. The thesis itself will be structured into different parts, primarily the first and the second. The first part will be a comparison between the EU and NATO and their cyber strategies. The second part will be a case study, where one looks at how EU and NATO´s different strategies affect Norway and its security. Throughout the first part, one will use an inductive strategy, by looking at, and using empirical data and observations. Furthermore, these will be used to draw various conclusions about how comparable NATO´s and the EUs strategies are, what their differences are, and what they are actually doing on the ground. Secondly, the same inductive approach will be used in the second part. Here, the comparative study in the first half, will be included into the analysis, in order to see how the differences in EU-NATO cyber strategies affect Norway and its security. Hence, this research combines case study, comparative analysis, document analysis with some elements of historical analysis methods of research. (Jacobsen, 2016).

2.2. Data:

My research question revolves around the cyber strategies of NATO and the EU, and how these affect the Norwegian cyber strategies. The focus will therefore lie on the different strategies of the different units of analysis, and how they interact. Given that NATO is a political and military alliance, their type of strategy might be quite different from that of the EU, which is a political union. Secondly, Norway´s strategy might also be quite different, given that Norway is a small country, compared to such big

[3] These being China and Russia.

international actors. Whether or not that means that it is easily affected by the strategies of the remaining two units of analysis remains to be seen.

In order to illustrate the potentially different strategies and how they work, one will be using official data from both NATO, the EU, and Norway. These will be examined within the given timeframe of the thesis, to see if the strategies have developed in any way shape or form that might affect each other. Both primary and secondary sources will be used. Primary sources include plans, strategy plans, military and political assessment, and various statements. By looking at more practical documentation, such as official strategies published by NATO, the EU and Norway, official statements made by various bodies within the organizations, and documents regarding how they are implementing these strategies into society.

The strategies will be linked to the rising tension between NATO and Russia/China. Political tension between the EU and Russia/China with documents linked to this tension will also be used to clarify some of the strategies, statements and other sources.

2.3. Variables:

This thesis, with its two-parted qualitative study, will have various variables. In terms of my RQ the independent variable would be the cyber strategies of EU and NATO, with Norway's cyber strategy to some extent, being the dependent variable. Of course, Norway faces its own threats outside the alliance with NATO and its cooperation with the EU, based on for example Norway's geopolitical location. Therefore, one can't fully say that Norway's cyber strategies are fully dependant on NATO and the EU's cyber strategies, but that in terms of Norway's cooperation with the two units of analysis, Norway's cyber strategies are somewhat dependent on the EU and NATO. If one looks at the bigger picture one can say that the cyber threats themselves are the independent variables, and that the various strategies are dependent as they are based on the given threats.

3.0. Literature review.

As previously mentioned, the thesis will use both primary and secondary sources. The literature found does not look at how the cyber strategies of the EU and NATO affect Norway´s strategies. Therefore, the following literature explains and justifies why in this research I explored primarily military documents from NATO, political literature from the EU, and then looking at how the different aspects in their strategies affected the Norwegian ones.

A good source regarding the comparative part of the thesis would be the article by Stitilis, Pakutinskas & Malinauskaite from 2016, which takes a dive into EU and NATO cybersecurity strategies and various national strategies. The authors of the article are able to reveal that even though the two main actors, being NATO and the EU, have similar goals, the various approaches that they use are quite different (Stitilis, Pakutinskas & Malinauskaite, 2016, p. 1151). The approach where they aim to compare the cyber security strategies of both NATO and the EU, is quite similar to the approach taken in this thesis, which therefore adds to the relevance of the article. The topic itself, being EU-NATO cybersecurity strategies and various other national cyber security strategies, is relevant for my research question because that is essentially what the research questions aims to answer with the addition of how these strategies affect Norway. The article covers part of what this thesis aims to answer, but in order to be able to answer my research question in the best possible way, this article alone will not be enough.

In 2014, Piret Pernik wrote an article regarding how to improve cyber security by focusing on the strategies by NATO and the EU. Pernik is able to reveal that NATO and the EU, have started to look at cyber security as something that might be of strategic security and defence concern (Pernik, 2014, p. 15).
The article touches on differences in NATO and the EU's cyber security, such as NATO's ability to ensure interoperability of cyber capabilities found within the alliance, and the EU´s ability to develop efficient strategies and policies (Pernik, 2014, p. 15).

An article published in 2019 regarding Norway's relationship to NATO and the EU was also an important source regarding this thesis. The article focuses on the challenges and opportunities that are given to Norway in a time where cooperation, institutions and organizations are challenged by changes in the current international security policy (Græger, 2019). Norway's relationship with the EU and NATO is analysed from a security policy perspective, while pointing out future security challenges (Græger, 2019).

Kveberg and Johnsen issued an article in 2013 with the intention of describing how cyberspace and cyber power is highly relevant for Norwegian interests, and that the knowledge obtained within these areas will help to determine the future role of the Norwegian Armed Forces (Kveberg, Johnsen, 2013, p. 3) The report manages to relate several issues regarding cyberspace to Norwegian foreign policy, also including Norway's relationship with NATO and EU in terms of cybersecurity and cyberspace (Kveberg, Johnsen, 2013, p. 3).

Roger Johnsen, a Norwegian Lieutenant Colonel, wrote an article in 2013 covering cyber warfare and the Norwegian Armed Forces' operational capabilities (Johnsen, 2013). The article, argues the fact that an increased cyber capability, will give the Norwegian Armed Forces a higher operational capability, if they are able to adapt to the technological potentials that are currently available (Johnsen, 2013, p. 250). The article sheds light on Norway's current military capabilities and give a good indication of how important cyber warfare will be for future military operations.

Touching on the same subject that Johnsen (2013) did in his article, Langø and Sandvik (2013) are able to take cyberspace and cybersecurity and put it in to a political and civilian perspective. They point out that cybersecurity has given both Norway and the international community a significant challenge, and that the political approach to the problem up until that point has turned out to divided (Langø, Sandvik, 2013, p. 1). They go into further detail, combining both academical and operational perspectives to the topic of cyber security by using military, political and legal sources to make their point (Langø, Sandvik, 2013, p. 227).

This thesis will use reports issued by the Norwegian Ministry of Foreign Affairs regarding the international cyber strategies for Norway in the years to come. This report from 2017, covers, at least to some extent, the gaps found in the article by Stitilis, Pakutinskas and Malinauskaite regarding how Norway adapts to the everchanging area of operation that is cyberspace. The report covers how Norway adapts to various cyberstrategies and cyberthreats, whilst going over the cooperation with NATO and the EU from a Norwegian perspective. What this report lacks in terms of how it's to help this thesis answer its research question, is Norwegian strategies at home, and how Norway is to become resilient on its own. This gap is filled by the National Cyber Security Strategy for Norway which was published in 2019. This report goes in depth regarding national cyberstrategies, while also covering how the EU and NATO's various cyberstrategies and policies have affected Norway's strategies.

By combining these different pieces of literature, one is able to create a more comprehensive and complete image regarding the topic of EU-NATO cyberstrategies and how they affect Norway. Together, these sources take a deep dive into different approaches, processes and effects, and complement each other in terms of answering this thesis's research question.

4.0. EU approach to cyber security

In this part of the thesis, one will analyse the European Union´s and NATO´s approach to cyber security. The analysis will be divided into three different parts, EU approach to cyber security, NATO approach to cyber security, and a discussion of implications for Norway. The parts will consist of different threat perceptions, cyber security policies and the various direct actions within those policies. One will look at the similarities and the differences with NATO and the EU´s approaches to cyber security, and what implications these will have for Norway.

In 2016, the European Union issued a global strategy for the European Union´s foreign and security policy. Within that strategy, the topic of Cyber Security and strategies regarding this topic was disclosed. The EU stated that it would increase its focus on cyber security, mainly by giving the EU and its member states the tools that are required in protecting themselves from possible threats, while simultaneously providing a safe, free and open cyberspace within the EU (European Union, 2016, p. 21). The approach that the EU focused on in their Global Strategy from 2016, was that of enhancing various technological capacities and capabilities directed at reducing threats whilst increasing the resilience of different critical services, networks and infrastructures (European Union, 2016, p. 22.).

An important factor in the EUs approach to cyber security in 2016, was that of cooperation between member states, and also their core partners, being the United States and NATO (European Union, 2016, p. 22). The EU acknowledged the fact that in order to counter the cyber threats and to have an effective strategy regarding cyber security, cooperation with others would be imperative. This emphasis on cooperation would become increasingly important in the years to come and was an essential part of the European Cybersecurity Act which entered into force on June 27th of 2019.

In 2017, the European Commission issued a Recommendation on how to approach large-scale cybersecurity events. This Recommendation gives light to copious approaches to cyber security, whether it be cooperation, or independent training and preventive actions. The Recommendation recognises that cybersecurity and cybersecurity events might be different for various member states, and they therefore have different approaches based how the severity of the attack.
For example, one approach is that the member state has the main responsibility when it comes to tackling the incident, but that the various EU bodies are there to help if the approach taken by the member state is not sufficient enough (European Commission,

2017, p. 37). Another approach may be to train certain actors on how to handle certain events, by initiating various training events regarding cyber security and then evaluating the results. After this has been completed one is able to see if the approach is effective or not, and thereby the EU is able to adapt accordingly.

5.1. The European Union’s threat perception:

Regarding the European Union´s approach to cyber security, one important factor must be addressed and that is how the EU perceives the threat of cyber-attacks. This thesis will draw upon the Britain´s Security Service and their threat levels. There is a total of 5 levels of threat, them being low, moderate, substantial, severe and critical (Security Service, 2019). A low threat means that an attack is unlikely, moderate indicates a possible attack but that it is not likely, substantial indicated that an attack is likely (Security Service, 2019). The severe level means that an attack is highly likely, whilst critical threat levels indicates that an attack is highly likely to occur within the near future (Security Service, 2019). Of course, each member state might have their own approach as to how they choose to categorise various types of threats, but for the purpose of this thesis, the threat categorization provided by the British Security Service will be more than sufficient.

In 2017, the current president of the European Commission, stated that cyber-attacks were of a greater threat to the democracies and economies of the world, than that of the threat posed by guns and tanks (European Parliament, 2019). This is a drastic change from not too long ago during the Cold War, when the threat of nuclear warfare was upon us as a substantial threat, including tanks, guns and nuclear warheads. The development of warfare during the last five decades have been astonishing, with technological advancement being one of the main driving forces for military innovation.

With these technological advancements, nations and non-state actors can wage war without actually fighting with guns and tanks. The military strategist Sun Tzu was a head of his time by saying that a person who processes the given skill in terms of military tactics, will be able to subjugate the enemy forces without having to go to war (Sun Tzu, 2020, p. 48). This is to some extent what we’re seeing with the increasing threat of cyber-attacks and cyber warfare.

The European Strategy and Policy Analysis System (ESPAS) pointed out that violent conflict will be a continuous feature in the years to come, undeterred by our efforts to avoid it (ESPAS, 2019, p. 25). If one is to take ESPAS’s and the statements made in their report, for example that they point out that cyberspace will become the battlefield, on which various states and non-state actors will confront each other (ESPAS, 2019, p. 19), and to see them as a form of threat assessment, one can argue that ESPAS, and the EU look at the threat of cyber-attacks as a substantial or severe threat. This, alongside the European Agenda on Security from 2015, where they undeniably prioritize fighting cybercrime by implementing an effective form of cybersecurity (European Commission, 2015, p. 19), one might argue that the EU assess the threat of cyber- attacks to be on a substantial level. This is backed up by the ENISA Threat Landscape Report from 2018, which states that web-based attacks, data breaches, and information leaks are just some of the cybercrime categories that have gone up since 2017 (ENISA, 2018).

The 13th of September 2017, the European Commission issued a Recommendation on how one is to orchestrate a coordinated response to extensive cybersecurity events and crises (European Commission, 2017). This is essentially a crisis plan on how one is to respond to a large-scale cyber-attack of some sort, a standard operating procedure (SOP) if you will. The level of detail and planning that has gone into this strategic Recommendation is tremendous, and it's an evident example of the European Union perceiving the threat of cyber-attacks to be very much real, and that the threats themselves are indeed substantial and/or severe.
The Recommendation itself is for when an attack has already happened, but the EU´s level of commitment when it comes to tackling the threat of cyber-attacks is uncanny and shows the EU´s threat perceptions and evaluations to be legitimate.

5.2. Overall European policy on dealing with cyber threats:

One important question which will be important to ask, is how the European Union deals with this substantial or severe threat. What kinds of systems have been put in place in order to combat the various threats, and what do these systems consist of? One of the important systems that have been put in place in the recent years, is the implementation of the Cybersecurity Act, which sets the European Union Agency for Cybersecurity (ENISA) on the path of becoming ever more important and influential in the field of cyber security.

One of the more significant enhancements bestowed on ENISA through the implementation of the Cybersecurity Act is the fact that ENISA now has a permanent mandate (European Commission, 2019). This mandate gives ENISA and the EU a significant role when it comes to establishing and maintaining the certification framework regarding cybersecurity (European Commission, 2019). This enables ENISA to be able to arrange the technical grounds where one finds given certification schemes, and also being able to inform the general public on said certification schemes by establishing a website (European Commission, 2019). To put it more simply, the Cybersecurity Act introduced onto the European Union, a give set of rules that one would have to comply with in order to receive a cybersecurity certification.

The Cybersecurity Act, with ENISA, can therefore be seen as more of a measure made to prevent the given threats in becoming a severe threat to the European Union and its members. Thus, it is important to ask how the EU would respond to a cyber-attack. Would a cyber-attack be taken as seriously by the EU and its members as an attack done with military force? Would a cyber-attack for example trigger the use of article V in the Treaty of Brussels from 1948? Article V states that if a member state would on the receiving end of an armed attack, the other member states will help in any given way possible, including military and other types of aid and assistance (The University of Oslo [UiO], 2012). As previously mentioned, this article is from 1948, and at that given age the cyber threat was not as substantial as they are today, hence the reason behind questioning its relevance in a potential cyber-attack.

In 2017 the Council of the European Union gave a press release stating that activities that may constitute wrongful acts under international law, also the ones that may take place in cyberspace, could set in motion a joint EU response (Consilium, 2017). This, coupled with article V in the Treaty of Brussels, indicates that the EU does in fact have a strategy that involves a form of retaliation and or reprisal. It is clear that the EU strategy on cyber security also values and respects the goals and values of the EU in general, for example that the EU is to offer freedom, security and justice without the existing boundaries of internal borders, with an emphasis on security (European Union, 2020). Through the issuing of the statement in 2017, coupled with article V of 1948, the EU are taking preventive steps to avoiding cyber-attacks, by showing international actors that pose a threat that the EU are taking the necessary steps towards protecting themselves.

That said, one also finds that the EU are taking clear systematic approaches. The Cybersecurity Act, with ENISA is a clear example of the EU taking systematic approaches on dealing with the given cyber threats. Through their newly given mandate, ENISA is now able to establish websites that significantly increases the flow of information onto the member countries within the EU, but also other countries that are not currently member states. Through this increase in information regarding cyber threats, the individual citizen is able to take preventive action and protect themselves from the threat, and also instilling that knowledge onto others. The importance of putting the increased threat of cyber-attacks on the daily agenda is seemingly an important part of the EU´s systemic approach to dealing with cyber threats.

Secondly, ENISA is able to issue various rules that member states are expected to comply with if one wishes to be a part of the European Union´s defence. These rules require some sort of compliance if one wishes to be given a cybersecurity certification. This systematic approach drastically increases the likelihood of each member state being up to date when it comes to the latest means of responding to a cyber threat.

As previously mentioned, the Recommendation of 2017 issued by the European Commission, does not primarily indicate how the EU perceives cyber threats, but rather how one is to deal with them. The document in and of itself is a systematic approach to cyber-threats, but by going through the document thoroughly, one finds diverse methods on dealing with cyber threats, all of which are combined into one functioning and coordinated strategy in response to large cybersecurity events and crises. That being said, by reading the document and looking at its suggested measures on dealing with cyber threats, it is possible to suggest that that the Recommendation of 2017 as a whole most likely perceive the threat as severe.

One defensive measure that is highlighted early on in the document is cooperation. Cooperation that has been continuously rehearsed on so that each individual within that cooperation knows the given procedures on how to handle the cyber-threat is key (European Commission, 2017, p. 36). More precisely, the enhancement of cross-border cooperation with a direct relation to preparedness, will have huge implication on a large-scale cyber incident of some sort (European Commission, 2017, p. 37). Even though it is the member states that have the primary responsibility when it comes to incidents regarding cybersecurity, the EU institutions still have an important role when it comes to helping, so that the cyber threat does not impact sections of economy, security or relations within or outside the EU (European Commission, 2017, p. 37). The policy for the members of the EU are mainly of a defensive or preventive nature, but the EU as a whole might act as a whole and issue a join response with possible retaliation.

The EU also uses cybersecurity exercises in order to train and improve how they handle cyber threats. Firstly, by issuing various systematic approaches, legislations and strategies, the EU is able to be well prepared for diverse cyber threats. However, in order to make sure that these measures actually work, they have also implemented cybersecurity exercises as a way to prepare and deal with cyber threats.
These Cyber incident exercises called Cyber Europe, are essential when it comes to seeing whether or not the measures that are written down, works when executed by the given professionals (European Commission, 2017, p. 39).
Cyber Europe exercises not only stimulates and improve the cooperation across member states and other sectors, they are an invaluable resource to the further development of EU policy on how to deal with cyber threats (European Commission, 2017, p. 39).
The Recommendation itself takes some inspiration from for example the communication made by the European Commission in 2016, regarding cyber resilience and its systems. However, that does not take away the importance that the Recommendation of 2017 had, and still has on EU policy regarding how to deal with cyber threats.

With this in mind, it´s important to ask why cyber security has become such an important topic within the European Union. Take cybercrime for instance. The ENISA Threat Landscape Report from 2018, show that malicious email sent by cyber-criminals with the intent to compromise different businesses, have resulted in a 12 billion-dollar loss since 2013 (ENISA, 2018, p. 119). That´s an average of 2,4 billion dollars each year, through malicious emails alone. In the same report, one finds evidence 880 million dollars in losses as a result of attacks aimed at cryptocurrencies (ENISA, 2018, P. 119). The devastating effects of cyber-attacks are not only of an economic nature, but they can have a profound effect on the ability to provide healthcare and pharmaceutical equipment. As recently as April 2020, officials from the United States said that they experienced a flood of hacks on the behalf of Chinese hackers directly targeting the people who provide healthcare and the people who manufacture pharmaceutical equipment (CSIS, 2020, p. 1). Ahead of the EU elections in 2019, Russian hackers directly targeted several European governments and their agencies (CSIS, 2020, p.9). Lastly, over the course of several years, Russian hackers targeted the embassies, including the foreign affairs ministries in multiple countries across Europe (CSIS, 2020, p. 4). These cyber incidents provided by the Centre for strategies & international studies, show the devastating effects that cyber-attacks might have upon multiple sectors within society. This further supports the EU´s decision to emphasize cyber security and mitigating the threat of cyber-attacks.

The overall EU policy on dealing with cyber threats have taken many forms, some taking strictly systematic approaches, while others focus on prevention and retaliation. The fact is that the cyber threats themselves also take on many forms, and that there is an abundance of cyber threats out there. The EU has over several years developed ways of dealing with these threats, by improvising and adapting to the development of cyberspace and its continuous influence in society.

5.0. NATO approach to cyber security

NATO´s approach to cyber security will in some instances be quite different from that of the European Union. One important detail to remember, is the fact that NATO is a military organization (Stitilis, Pakutinskas & Malinauskaite, 2016, p. 1155), whereas the European Union is a more economic and political union. Therefore, their operational procedure regarding cyber security will be different in some areas.

One of the things that NATO and the EU do agree in, is the fact that cyber threats continue to evolve, and it is important to keep up with that continuous evolvement. The Wales Summit Declaration of 2014 stated that cyber threats and various cyber-attacks would become more refined, frequent and quite possibly more damaging (North Atlantic Treaty Organization, 2014). NATO then stated that they had endorsed an Enhanced Cyber Defence Policy, and that this policy would stay true to NATO´s core tasks and their duties as a military alliance (North Atlantic Treaty Organization, 2014). The Summit emphasized NATO responsibility to defend their Allies if necessary, but that protecting oneself through developing the relevant and necessary capabilities with regards to a cyber-attack, would be up to each member (NATO, 2014).

However, this does not mean that NATO will sit idle if someone within the alliance is attacked. NATO´s approach relies on a continuous development of cyber defence capabilities, so that the national governments are able to function, so that NATO in turn, is able to function. The approach not only covers their only alliance, but they are committed to engaging actively with other international organisations, including the European Union (NATO, 2014).

Again, during the Warsaw Summit Communiqué in 2016, NATO once again laid out their approach to cyber security. Bilateral and multilateral cyber defence cooperation is once again one of the main priorities, alongside the strengthening of national networks and infrastructures regarding cyber defence and security (NATO, 2016). NATO´s Brussel Summit Declaration of 2018 continues to set the path for NATO´s approach to cyber security in pretty much the same fashion as the previous four years with miniscule changes along the way. The message remains the same: NATO will continue to evolve and develop its skills in order to best tackle the threats found in cyberspace.
The Brussels Summit enabled the establishment of a new Cyber Operations Centre, that will strengthen NATO´s structure of command, giving NATO the capabilities to integrate cyber defence into its various operations around the world (Arts, 2018, p. 4). By sharing their knowledge with their own allies and various international organizations, one finds that NATO´s approach to cyber security is based on cooperation, collective defence and developing the necessary capabilities needed to withstand the threats posed by cyber-attacks.

Various differences between the EU and NATO´s approaches can be found, but they share the desire for cooperation and continuous development. The European Union is clearly aimed towards their citizens in terms of economics and politics, whereas NATO addresses its responsibility as a military alliance, in charge of protecting its members from a military perspective.

6.1. NATO´s threat perception:

NATO´s threat perception will be different than that of the EU. The reason for this is because NATO will analyse the threat through a military point of view, therefore perceiving the various threats in a different manner. The tools and capabilities at NATO´s disposal will also come into play when analysing the various threats and putting them into different categories. The different threat levels will be the same as previously mentioned, them being classified as low, moderate, substantial, severe and critical. The countries that are a part of the NATO Alliance will also have their own approach as to how they categorize the different threat levels. In order to provide a thesis as concise and clear as possible, the threat levels from the British Secret Service will provide a more than satisfactory threat categorisation.

In the Wales Summit Declaration, cyber threats are perceived as something damaging and sophisticated (NATO, 2014). NATO once again covered the topic in 2020, describing cyber threats directed towards NATO as becoming more destructive, complex and persistent NATO, 2020). As a result of this, cyber defence has become one of NATO´s primary tasks with regards to its collective defence (NATO, 2019). After the 2016 Summit in Warsaw, NATO declared that cyberspace is to be regarded as a domain of operations, alongside sea, land and air (NATO, 2019). This significant increase when it comes to prioritizing cyber defence and how to deal with cyber threats, gives a good indication that NATO is perceiving this as a substantial threat which needs to be dealt with accordingly. Therefore, one can argue that NATO perceives the threat of cyber-attacks to be, at the very minimum, a substantial threat to the NATO alliance.

Furthermore, the International Centre for Defence and Security issued a report in 2018, stating that many NATO countries at the time, had begun developing cyberspace capabilities of a more offensive nature within their significant armed forces (Pernik, 2018, p. 1). This coupled with the fact that NATO has made and continues to make crucial adjustments in order to keep up with the ever-changing threat landscape of cyberspace (Arts, 2018, p. 3), gives the indication that they are perceiving the threat as substantial

The Tallinn Papers provide a good illustration as to how seriously NATO is taking the threat of cyber-attacks. The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) published the Tallinn Papers in 2015, where they quickly gave examples of successful attacks on NATO networks made by international actors such as Russia (Lewis, 2015, p. 1). The CSIS provide in their incident report at least nine cyber-attacks aimed at Ukraine, three attacks aimed at Poland and two aimed at Estonia (CSIS, 2020) to name a few. These events happened between 2016 and 2020, and just this one report gives a good indication of the high frequency of cyber-attacks aimed at NATO and its allies. These attacks on NATO networks not only imply that the cyber threat is substantial, but it confirms that the threat is indeed severe and quite possibly critical in some cases.

This alongside the fact that malicious cyber campaigns are recognised as a long-term strategic risk to NATO and its Allies (Davis, 2019, p. 2), further substantiate the reasoning behind NATO´s perception and classification of the cyber threat.

6.2. Overall NATO policy on dealing with cyber threats:

Not only are there differences between NATO and the EU when it comes to approaches and perceptions regarding cyber threats, one also discovers further distinctions in their policy on dealing with the threats. One factor that has to be taken into consideration, is once again the fact that NATO is a military alliance, and therefore has different standard operating procedures (SOP). Another key thing to remember is that as a military organization with armed forces under its command, NATO has to have certain rules of engagement (ROE) which will once again affect their overall policy regarding cyber threats.

With that said, the Warsaw Summit in 2016 was a significant step in the right direction when it comes to NATO´s ableness to dealing with cyber threats. As previously mentioned, this Summit declared cyberspace as an area of operation, equal with air, sea and land (NATO, 2019). This not only enabled NATO and its Allies to deal with the cyber threat accordingly, but it gave NATO the possibility to develop diverse tools and approaches when it comes to dealing with the cyber threats. Some of these include systematic approaches, defensive action, preventive action, and if necessary, retaliation.

Another important milestone was set during the Brussels Summit of 2018, where Allies of NATO agreed to establish the Cyberspace Operations Centre (CyOC) as a new part of the strengthened NATO Command Structure (NATO, 2020).

The CyOC is in charge of equipping NATO with the necessary situational awareness, the planning of NATO operations and missions, and the coordination of operational interests in cyberspace (Brent, 2019). Essentially what CyOC is, is a more effective way on concentrating expertise, be that technical, operational or intelligence, into one complete credible situational awareness capability regarding cyberspace (Bigelow, 2018, p. 134). In turn, this leads to military operations focused on cyberspace becoming more effective (Bigelow, 2018, p. 134). In order for NATO to be able to deal with the cyber threat in the most effective way possibly, CyOC alone is not enough. The Brussels Summit furthermore strengthened NATO´s ability to deal with cyber threats. This was done by allowing members of NATO to integrate their sovereign cyber capabilities, into NATO operations and missions (Brent, 2019). In turn, this gave NATO the capacity to not only defend itself in a more effective manner, but also doing this in alignment with NATO´s defensive mandate (Brent, 2019). By putting these policies in place, NATO will be able to take full advantage of their Allies capabilities with regards to cyber, whilst simultaneously giving their Allies full sovereignty and ownership over their own capabilities and materiel (NATO, 2019).

Through cooperation with its Allies, NATO is able to provide extensive education, training and various programs, in order to best tackle the cyber threats. This systematic approach comes to life through exercises such as Locked Shields, which is a unique cyber defence exercise which offers complex training on an international level (NATO Cooperative Cyber Defence Centre of Excellence, 2019). This training gives NATO´s Allies the chance to test out their cyber security experts, and in turn enhancing their skills in defending themselves and NATO (CCDCOE, 2019).

In terms of cyber defence, this is one of the areas where cooperation between NATO and the EU have been strengthened (NATO, 2020). They share information and exchange experiences across their various crisis response teams, while simultaneously enhancing training, research and exercises between the two international organisations (NATO, 2020).

What´s interesting is that in alignment with its defensive mandate, NATO has no intentions of developing cyber capabilities of an *offensive* nature (NATO, 2019). This is supported by statements made in the Tallinn Papers of 2015, stating that NATO recognises the increased need for policies regarding how to deal with cyber threats, but that these policies should be focusing on cyber defence and staying true to the Alliance´s task of being a defensive organisation in charge of collective defence, cooperative security and crisis management (Lewis, 2015, p. 1).

Thus far, NATO has shown that it is willing to handle the substantial and severe threat of cyber-attacks through both systematic approaches such as training programs, but also that the Alliance is taking defensive and preventive actions in order to best deal with the threats. With this in mind, how would NATO react to a potential cyber-attack? Would this attack be enough to trigger the collective security clause, and if so, to what extent?

The Wales Summit of 2014 states that whether or not a cyber-attack is to lead to the invocation of Article 5 of the Washington Treaty, that decision is to be made by the North Atlantic Council whilst evaluating it on a case-by-case basis (NATO, 2014). In other words, yes, a cyber-attack could trigger the collective security clause, but it is not guaranteed.

In a general report issued by NATO´s Parliamentary Assembly in 2019, they stated that in order for the collective defence clause to be invoked, the cyber attacks would have to hit NATO's core, such as threatening an Ally´s national security, territorial integrity or political independence (Davis, 2019, p. 1).

It seems like NATO is hesitant to clearly define in which scenarios it is ready to invoke the collective defence clause under Article 5. The question is just whether or not this is a smart tactic when it comes to preventive actions. One might argue that in terms of deterring cyber-attacks, NATO could benefit from treating a cyber-attack in the same manner that it would an attack with a warhead. As previously mentioned, NATO has been on the receiving end of cyber-attacks made by superpowers such as Russia. One can argue that the likelihood on that attack happening if Russia knew that an attack would trigger Article 5, would decrease substantially.

It is of course important to take into account that NATO is primarily a defensive alliance, where the focus is collective security, but one has to argue that a slightly unspecified cyber defence policy does not mitigate the threat of cyber-attacks, quite possibly the opposite. Then again, the majority of cyber-attacks would most likely not have the same destructive tendencies and effects as that of common weapons of war (Lewis, 2015, p. 4).

Nonetheless, clearly defined cyber defence strategies, and a lack thereof, might leave NATO and its Allies open to numerous incidents that potentially could have been avoided with e clearer policy on how to deal with cyber threats and attacks. However, as a defensive alliance, one can understand as to why NATO has chosen to be fairly vague regarding their stance on invoking Article 5 which is understandable. NATO wishes to maintain its role as a defence alliance, therefore a more clarified offensive strategy might give off the wrong impression.

With that in mind one also understands why NATO is so ambiguous as to when it can invoke Article 5. Without a clearly defined line whereas to when NATO might call on Article 5, NATO and its allies give themselves to possibility to have multiple courses of actions if an ally was to be attacked, without having to invoke Article 5 (Arts, 2018, p. 8). This statement is also supported in the Tallinn Papers where the reasoning behind the vagueness surrounding the invocation of Article 5 has its strategic benefits. By being ambiguous NATO's hostile aggressors will have to change their risk calculations, forcing them to consider their offensive actions, and whether or not the risk is worth the rewards (Lewis, 2015, p. 7). NATO´s equivocal standpoint, might have their enemies walking on eggshells if you will.

NATO has a commitment and a responsibility when it comes to protecting its members (NATO, 2019). This can be achieved through both political and military measures, whilst giving consultation, preventive action and council (NATO, 2019). Over the last few years NATO has done exactly this.

By devoting funds so that new organisation, events and institutions such as CyOC and Locked Shields could be established, NATO has made itself one of the most important actors when it comes to dealing with cyber threats, orchestrating cyber defence training and providing a level of professional competence for others to use for their own advancement. Above all, it seems that NATO is trying its best to adapt to this new and ever evolving threat that is cyber threats. In a field of work where threats change rapidly, it seems that NATO is managing to stay on top of this and continue to adapt and overcome the challenges that cyber threats and attacks pose on NATO and its Allies.

6.0. Implications for Norway.

Both the European Union and NATO have shown through their various approaches, perceptions and policies, that they are adapting to the ever-changing cyber threat. In this this part of the chapter, one will take a closer look at how the different NATO and the EU's approaches affect Norway's cyber security policy. Norway's relationship with the EU and NATO will be examined in order to truly identify how each organization affects Norway, and what the effects truly are in terms of possible Norwegian policies, newly established organisations, and potential training programs. If there are any arrangements between the actors in terms of cyber cooperation, these will be examined.

7.1. How does the European Union's approach affect Norway's cyber security policy and defence?

As a country that is not a member of the European Union, Norway and the EU has got somewhat of a special relationship. Nevertheless, the Norwegian Government points out that the EU is an important trading partner for Norway, and that economic integration and political cooperation is of grave importance for both parts (Regjeringen, 2014). Norway and the EU also cooperation on security policy, one important part of that being Norway's entry into the European Defence Agency (EDA) in 2006 (Regjeringen, 2014). This enables Norway and the EU to exchange information, to participate in various projects and programmes and to share their ideas (Regjeringen, 2014).

In 2017, the Norwegian Ministry of Foreign Affairs (NMFA) issued its international cyber strategy for Norway. One of Norway's strategic priorities at the time was to support and promote a common European security level (Regjeringen, 2017, p. 7).
Norway as a large producer of electronic communication services, is reliant on infrastructures from outside suppliers, and therefore it needs a European framework that addresses security challenges (Regjeringen, 2017, p. 7). An example of how the EU's cyber security approach affects Norway, is through the fact that Norway started the implementation the Directive on Security of Network and Information Systems, also known as the NIS Directive (Regjeringen, 2017, p. 7). What this implies for Norway, is the establishment of a Computer Security Incident Response Team (CSIRT), which is responsible for the security demands bestowed upon Norwegian businesses (Regjeringen, 2019). The implementation of the NIS Directive also obligated Norwegian businesses who play an important role in the maintenance of the internal market, to implement safety measures and to report serious incidents regarding cyber security (Regjeringen, 2019). For Norwegian businesses, this entails increased security inspections, maintaining an efficient contingency plan and having a process to determine possible flaws in their security systems (Regjeringen, 2019). Norway's strategic priority of strengthening its cooperation with the EU through the adaptation of EU policies clearly show the positive effects of the EU's approach to cyber security.

To further illustrate the EU's effect on Norway's security strategy, the NMFA stated that it will try its best to advocate for a greater adoption of principles presented by the Council of Europe Convention on Cybercrime, more formally the Budapest Convention (Regjeringen, 2017, p. 8) This is a clear example of EU policies regarding cybercrime, directly effecting Norway's strategies regarding cyber related issues. The Norwegian Government is looking at the EU and seeing an organization that is trying its best to adapt to the current threat of cyber-attacks, and therefore Norway stated that it would encourage Norwegian actors involved in the information security sector, to join the European Cyber Security Organisation (ECSO) (Regjeringen, 2017, p. 8)
What this collaboration entails for Norway, is increased education when it comes to cybersecurity, training and increased awareness surrounding cyber security (ECS, 2020). One of the ECSO members is the Norwegian University of Science and Technology (ECS, 2020).

The Norwegian Intelligence Service issued its assessment of the current security challenges in 2020, one of them being various threats in cyberspace. They also stated in this report that the security policies regarding cyberspace and cybersecurity is becoming more advanced as states are able to increase their experience and skill level (Norwegian Intelligence Service, 2020, p. 76). The strategies issued by Norway also include cooperation with both the EU and NATO. It is possible to imagine that this level of cooperation could have been achieved without the EU's policies affecting Norway. Even so, Norway has shown, by being open to the effects of EU cyber defence policies, that this more likely than not has increased the level of cooperation between the two, and that the result is an increase of capability with regards to handling cyber threats.

Through the implementation of the NIS directive, and the strengthening of ENISA, Norway will continue to work closely with ENISA (Regjeringen, 2019, p. 16). Because of ENISA's increased capacity Norway will start prioritizing working with ENISA and also increasing the usage of the ENISA deliveries across national levels (Regjeringen 2019, p. 16). This gives another indication of how much EU policy affect Norwegian policy. As previously mentioned, Norway is not a member of the EU.

What´s interesting is that the EEA Agreement does not cover the NIS directive, and therefore Norway is not obliged to implement it into its cyber defence strategy (Regjeringen, 2019, p. 16). Nevertheless, the Norwegian government deemed the NIS directive to be relevant and acceptable with regards to the already existing EEA agreement, and therefore Norway chose to adopt it (Regjeringen, 2019, p. 16).

7.2. How does NATO's approach affect Norway's cyber security policy and defence?

Norway is a founding member of NATO, with more than 70 years as an official Ally of NATO. In a report given by the Norwegian Defence Research Establishment (FFI) in 2014, NATO is described as essential to Norway's security policy (Johnsen, 2014, p. 3). The report illustrates the fact that NATO has increased its efforts with regards to the rising threat of cyber-attacks (Johnsen, 2014, p. 3) Norway is as a whole, utterly reliant on NATO for its collective defence in case Norway is ever under attack (Johnsen, 2014, p. 3). Therefore, in order for Norway to have the most effective defence possible, it is reliant on NATO to keep updating and adapting their cyber defence policies.

NATO policies are therefore strongly influenced by something called interoperability, which NATO describes as the ability for Allies to be able to effectively, efficiently and consistently accomplish various objectives, be them operational, strategic or tactical (Johnsen, 2014, p. 11). This enables Allies to operate using several forces, systems and units simultaneously, and for them to share, learn and increase their competence and the capacity to which they operate (Johnsen, 2014, p. 11). This of course includes Norway. Take the military exercise Trident Juncture of 2018 for example. This was one of the biggest NATO exercises in recent years, and it included training at sea, on land, in the air, but also in cyberspace (NATO, 2018).

If it hadn't been for the Warsaw Summit of 2016, Allies would not have regarded cyberspace as an official area of operation and a large military exercise such as Trident Juncture would thereby not include training on potential events in cyberspace.
This affects Norway in the way that it would not be able to include such training exercises into its priorities, and therefore would lack the necessary training themselves. In an alliance as large and complex as NATO, consistent exercises and training across Allies is necessary if NATO wishes to uphold its position as a defensive Alliance in charge of the collective defence of several states.

Another one of these exercises in Cyber Coalition, which is NATO's main exercise regarding cyber defence (NATO, 2018). Once again, had it not been for NATO's decision to make cyberspace an area of operation, Norway and all the other Allies in NATO would not be given the chance to share their expertise and experience, and more importantly, they would not have been able to train together at all.

With regards to the Norwegian Intelligence Service's views on potential cyber threats, the Warsaw Summit of 2016 enables the Norwegian Armed Forces to handle these threats in a more effective manner. Thus, NATO's approach to cyber threats directly affect Norway's capabilities with regards to dealing with the threats effectively. Consequently, Norway's national cyber defence policy clearly benefits from NATO's approach.

As previously mentioned, NATO requires each of their Allied members to develop and enhance their cyber defence capabilities, as NATO alone can't be responsible for every member´s national security. As a result, Norway established the Norwegian Armed Forces Cyber (CYDEF) during the fall on 2012 (Johnsen, 2014, p. 18). This was done to illustrate that the Norwegian Armed Forces recognize that cyberspace was and continues to play a critical part in the activities that the Armed Forces conduct (Johnsen, 2014, p. 18). The establishment of CYDEF gave Norway the possibility to prove itself as an important ally with highly developed skill regarding cyber defence, including the systems and processes that go into making that happen (Johnsen, 2014, p. 18)

Another affect that the NATO approaches have on Norway's cyber defence is the fact that it will make Norway try harder. In other words, Norway is a small state in the midst of a rather large alliance. Larger allies within NATO are sceptical when it comes to sponsoring smaller allies if they feel like they are getting nothing in return (Johnsen, 2014, p. 19). Not to say that large allies treat Norway like a charity, but truth be told, Norway is dependent on NATO and its allies if the state was to be attacked. Therefore, Norway as a nation with the qualifications needed in order to become a considerable ally to rely on regarding cyber defence, should take advantage of every opportunity given to prove to the larger allies within NATO that it is a force to be reckoned with (Johnsen, 2014, p. 19). This might include participating in the interoperability initiatives that NATO propose, similarly to Trident Juncture and Cyber Coalition as previously mentioned.

In Norway's National Cyber Security Strategy from 2019, it is clearly stated that Norway is to follow the obligations that were put in place during the 2016 NATO Summit and its proposal of an authorized joint cyber pledge (Regjeringen, 2019, p. 24). For Norway, this entails to improve several cyber defence areas on a national level, for example information sharing, a further development of skills and capabilities, and a continued focus on collaboration (Regjeringen, 2019, p. 24).

7.3. Norwegian funding, newly established departments and national actions as a result of foreign cyber policy influence.

One of the most important national actions that have come as a result of the EU and NATO influence on Norwegian cyber defence policy, is Norway's participation in international exercises. As already mentioned, Norway participates in NATO's Cyber Coalition exercise, which is NATO's biggest cyber defence exercise with the purpose to train national capacity to protect both NATO's and national governments networks (Regjeringen, 2019, p. 28). Another very important exercise in which Norway participates is Locked Shields. Norway's national security authority (NSM), is in charge of coordinating the Norwegian participants by using its own resources and resources from other sectors, in order to ensure that professional development and the increase of skill is guaranteed (Regjeringen, 2019, p. 28).

The National Cyber Security Strategy for Norway, which was launched in 2019, and covers several topics, one of them being the national strategy for cyber security competence (Regjeringen, 2019, p. 9). The priority areas within just this topic, are approximately over 800 million Norwegian kroner (Regjeringen, 2019, p. 9). ENISA established that the measures within Norway's strategy would end up requiring a budget of 1,6 billion Norwegian kroner (ENISA, 2019). The strategy also includes several advices that are to be given to companies in Norway so that the level of cybersecurity level across the nation can be increased (ENISA, 2019).

The Norwegian Armed Forces Cyber Defence (CYDEF) was established during the fall of 2012 and gave the Norwegian Armed Forces new ways of operating in the cyber domain in terms of warfare (Johnsen, 2014, p. 18). CYDEF's primary task include defending, securing and maintaining Norway's Armed Forces´ very own systems, advanced platforms, networks and other military materiel from malicious attacks (Johnsen, 2014, p. 18).

By establishing CYDEF, Norway not only makes itself more able to defend itself in cyberspace, but it also enables Norway to be able help NATO in a more effective way that before, thereby proving themselves as a serious, competent and effective ally to have on board in potential military cyberspace operations that might take place in the near future (Johnsen, 2014, p. 28).

7.0. Summary

Throughout this thesis, the aim has been to identify the differences in EU-NATO cyberstrategy, as well as to determine how these strategies affect Norwegian cyberstrategy. Based on the comparative analysis carried out in this thesis, one has been able to point out the differences in the EU-NATO cyberstrategies. Regarding their different approaches to cybersecurity, this thesis illustrates a significant distinction between the two units of analysis such as the apparent focus on sovereignty that can be found in NATO's approaches. That is not to say that the EU does not value their members states' sovereignty, just that NATO require their members to uphold a certain standard of national independence and resilience if the Alliance is to survive at all.

However, the EU's various approaches seem to cover a larger portion of cyberspace and how to protect oneself from the threats that exist in this new area of operation. This is of course understandable given the fact that the EU is an economic and political union, whereas NATO is a military alliance, therefore resulting in the EU focusing more on cybercrime, rather than NATO's focus on state-on-state cyber warfare.
This will affect and play a role in how the two different units of analysis approach cyber security, and this has been clearly reflected on, and answered in this thesis.

The threat perceptions of the two units of analysis mostly resemble each other, varying between being categorized as substantial, severe or critical. With that said, this thesis illustrates why and how the two units of analysis categorize the threats as they do, by providing statements, statistics and threat analyses. What's most interesting about the EU and NATO's resembling threat perceptions, is the fact that they are two very different actors, with different challenges to face and with different tools in their belt. Nevertheless, they are able to categorize the threats somewhat similar. Of course, this is in part due to the fact that this thesis bases its threat perception with the same categories for both units of analysis, but it is still interesting to see that two organizations with such different approaches and courses of action, view the threats in cyberspace from a fairly equal point of view.

In regard to NATO and the EU's overall policies on how to deal with the cyber threats, this thesis further illustrates differences between the two. It should come as no surprise that there would be, and are, obvious differences between the policies of NATO and the EU. The reason for this is once again the fundamental difference in how the two organizations operate, one being political, the other military. What is interesting, is the lack of policies that "steer the ship in the right direction" if you will.

Both organizations obviously want to deal with the threat of cyber-attacks in the best possible way, but it seems that what they fail to recognize is the fact that cyberspace and the threats within, see no national borders. One could argue that based on research in this thesis, that both the European Union and NATO may be too concentrated on their areas of expertise, rather than both organizations becoming experts at all the areas within cyberspace. This thesis shows that the EU might be too concentrated on threats such as cybercrime, whereas NATO concentrates on cyber warfare and the military aspect of cyberspace. I am not saying that the EU should become solely military union, nor am I suggesting that NATO should focus all its attention towards political and economic challenges. I am simply proposing that both organizations, with their vast amount of resources and allies, could benefit of trying to excel at other areas than what they previously though would be necessary. The world as we know it is evolving, so are threats. Therefore, the EU and NATO as two of the biggest political and military actors in the world, need to adapt alongside with it.

This thesis set out to find out what the differences in EU-NATO cyberstrategies are, and how these differences affect Norway's cyberstrategy. Through the comparative analysis that has been conducted in this thesis, alongside the case study of how this affects Norway, one is able to point out several effects that the EU and NATO have on Norwegian cyberstrategy. EU and NATO policies give Norway the opportunity to be a part of political, economic and military decisions in Europe, whilst simultaneously giving Norway the chance to prove itself as an important actor in terms of cyber defence and cyber security. As a result of EU and NATO policy making regarding cyber strategies, Norway was given the opportunity to host multiple important military cyber exercises such as Trident Juncture and Cyber Coalition. These military exercises gave the Norwegian Armed Forces a chance to show that are an important ally for NATO and an important partner for the EU.

Various cybersecurity implementations done by the EU also gave Norway an example of how one could establish their own strategies, and therefore the Norwegian government has adopted several EU policies regarding cyber security and strategies such as the NIS Directive.

The differences in EU-NATO cyberstrategy have throughout this thesis been exemplified, along with clear examples of how these differences affect Norway's cyberstrategy. One thing is evident when dealing with cyberspace and the threats that in contains, cooperation is key.

NATO, Norway and the EU, illustrate copious amounts of cooperation, but what this thesis can help with, is making these units of analysis realize that they have to adapt their cyberstrategies so that they cover all of cyberspace, not just parts of it.

8.0. Bibliography.

- Bigelow, B. (2018). *The Topography of Cyberspace and Its Consequences for Operations*.* Retrieved from https://www.ccdcoe.org/uploads/2018/10/Art-07-The-Topography-of-Cyberspace-and-Its-Consequences-for-Operations.pdf
- Brent, L. (2019). NATO's role in cyberspace. *NATO Review*. Retrieved from https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html
- CCDCOE. (2019). Locked Shields. Retrieved from https://ccdcoe.org/exercises/locked-shields/
- CSIS. (2020). *Significant Cyber Incidents Since 2006*. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/200504_Cyber_Attacks.pdf?0M9lsdHhOXhw.BahGk5hYXgDtEWrs6x9
- Davis, S. (2019). *NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence*. Retrieved from https://www.nato-pa.int/download-file?filename=sites/default/files/2019-10/REPORT%20148%20STC%2019%20E%20rev.%201%20fin%20%20-%20NATO%20IN%20THE%20CYBER%20AGE.pdf
- ECS. (2020) WG5: Education, awareness, training, cyber ranges. Retrieved from https://www.ecs-org.eu/working-groups/wg5-education-awareness-training-cyber-ranges
- ENISA. (2019). *ENISA Threat Landscape Report 2018*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
- ENISA. (2019, 15. February). New national strategy for cybersecurity published by Norway. Retrieved from https://www.enisa.europa.eu/news/member-states/new-national-strategy-for-cybersecurity-published-by-norway
- ESPAS. (2019, April). Global Trends to 2030 – Challenges and Choices for Europe. Retrieved from https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/ESPAS_Report2019.pdf
- European Commission. (2017). *Commission Recommendation on coordinated response to large-scale cybersecurity incidents and crises* (2017/1584). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H1584&from=EN
- European Commission. (2020, 20. April). Cybersecurity. Retrieved from https://ec.europa.eu/digital-single-market/en/cyber-security
- European Commission. (2020, 28. February). The EU Cybersecurity Act. Retrieved from https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
- European Council. (2020, 6. March). Cybersecurity in Europe: stronger rules and better protection. Retrieved from https://www.consilium.europa.eu/en/policies/cybersecurity/
- European Parliament. (2019). Cyber: How big is the threat?. Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf
- European Union. (2020, 31. March). The EU in brief. Retrieved from https://europa.eu/european-union/about-eu/eu-in-brief_en
- Forsvaret. (2013). *Etteretningstjenestens vurdering*. Retrieved from https://forsvaret.no/fakta_/ForsvaretDocuments/FOKUS-2013.pdf

- Forsvaret. (2020). *FOCUS 2020: The Norwegian Intelligence Service's assessment of current security challenges*. Retrieved from https://forsvaret.no/presse_/ForsvaretDocuments/Focus2020-web.pdf
- Græger, N. (2019). Veivalg og spenninger i norsk sikkerhetspolitikk: Norges forhold til NATO og EU. *Internasjonal Politikk, 77*(1), 84-94). Retrieved from https://tidsskriftet-ip.no/index.php/intpol/article/view/1625
- Jacobsen, D. I. (2016) *Hvordan gjennomføre undersøkelser?:Innføring i samfunnsvitenskapelig metode* (3rd. Ed). Oslo: Cappelen Damm.
- Johnsen, T. S. (2014). *Norway, NATO and cyber Defence* (01328/2014). Retrieved from https://publications.ffi.no/nb/item/asset/dspace:2441/14-01328.pdf
- Johnsen, R. (2013) Cyberkrigføring og Forsvarets operative evne. *Internasjonal Politikk, 71*(2), 241-251. Retrieved from https://www.idunn.no/ip/2013/02/cyberkrigfoering_og_forsvaretsoperative_evne
- Kveberg, T., Johnsen, S. T. (2013). *Cyberdomenet, cybermakt og norske interesser* (FFI report (02712/2013) Retrieved from https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/1022/13-02712.pdf?sequence=1&isAllowed=y
- Langø, H. I., Sandvik, K. B. (2013). Cyberspace og sikkerhet. *Internasjonal Politikk, 71*(2), 221-228. Retrieved from https://www.idunn.no/file/pdf/60693172/cyberspace_og_sikkerhet.pdf
- Lewis, J. A. (2015). *Tallinn Paper: The Role of Offensive Cyber Operations in NATO´s Collective Defence* (8/2015). Retrieved from https://www.ccdcoe.org/uploads/2018/10/TP_08_2015_0.pdf
- NATO. (2020, 17. March). Cyber defence. Retrieved from https://www.nato.int/cps/en/natohq/topics_78170.htm
- NATO. (2018). Final Planning Conference held for NATO Cyber Coalition 2018. Retrieved from https://shape.nato.int/news-archive/2018/final-planning-conference-held-for-nato-cyber-coalition-2018
- NATO. (2019, February). NATO Cyber Defence. Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf
- NATO. (2018, 29. October). Trident Juncture 2018. Retrieved from https://www.nato.int/cps/en/natohq/157833.htm
- NATO. (2014. 5. September). Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the north Atlantic Council in Wales. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_112964.htm
- NATO. (2019, 21. July). What is NATO. Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/191021-WhatIsNATO_en.pdf
- Pernik, P. (2014). Improving Cyber Security: NATO and the EU. *International Centre for Defence Studies*. Retrieved from https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf
- Pernik, P. (2018). *Preparing for Cyber Conflict: Case Studies of Cyber Command*. Retrieved from https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf

- Regjeringen. (2019). *Gjennomføringsforordning 2018/151 om spesifisering av NIS-direktivet artikkel 16 nr. 1 og nr. 4.* Retrieved from https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2019/sep/gjennomforingsforordning-2018151-om-spesifisering-av-nis-direktivet-artikkel-16-nr.-1-og-nr.-4-/id2673244/
- Regjeringen. (2017). *International cyber strategy for Norway*. Retrieved from https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategy_2017.pdf
- Regjeringen. (2019). *List of measures – National Cyber Security Strategy for Norway.* Retrieved from https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/list-of-measures--national-cyber-security-strategy-for-norway.pdf
- Regjeringen. (2019). *National Cyber Security Strategy for Norway.* Retrieved from https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf
- Regjeringen. (2014, 13. December). Norway and the EU. Retrieved from https://www.regjeringen.no/en/topics/european-policy/Norways-relations-with-Europe/norway-eu/id684934/
- Secret Service. (2019). Threat levels. Retrieved from https://www.mi5.gov.uk/threat-levels
- Štitilis, D., Pakutinskas, P. & Malinauskaité. (2016). EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security Journal, 30* (4), 1151-1168. Retrieved from https://link.springer.com/article/10.1057/s41284-016-0083-9
- Tzu, S. (2020) *The Art of War – Sun Zis Krigskunst*. (Yang, H, H, L. Trans.). Oslo: Hegnar Media
- University of Oslo. (2012). Protocol Modifying and Completing the Brussels Treaty. Retrieved from https://www.jus.uio.no/english/services/library/treaties/01/1-10/protocol-brussels-treaty.xml

NTNU

Norwegian University of
Science and Technology