

Master's thesis

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

Mari Cecilie Aae

Birds of a Feather Flock Together: Nordic Defense Cooperation in a Globalized World

A Qualitative Case Study on Cyber Defense
within NORDEFCO.

Master's thesis in European Studies
Supervisor: Dr. Pieter de Wilde
Trondheim, May 2018

Mari Cecilie Aae

Birds of a Feather Flock Together: Nordic Defense Cooperation in a Globalized World

A Qualitative Case Study on Cyber Defense within
NORDEFCO.

Master's thesis in European Studies
Supervisor: Dr. Pieter de Wilde
Trondheim, May 2018

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

Abstract

The Nordic region consists of small states eager to cooperate in order to protect its citizens and territory. Since the end of the Cold War, the Nordic states have openly developed a closer cooperation on security and defense policy, and in 2009 the Nordic Defense Cooperation (NORDEF) was established. One increasingly important area of cooperation within this framework is the development of common cyber defense capabilities. Focusing on NORDEF as a regional cooperation, and the use of theories within the global governance approach, this thesis contributes to the discussion on regionalism in the case of cyber defense. By concentrating on motivations for regional cooperation, the thesis argues that the theoretical framework presented has large explanatory power as to why the Nordic states seek closer cooperation on cyber defense capabilities. Realism and constructivism combined can to a large extent explain why Nordic states seek closer regional cooperation despite membership in other systems/organizations working with developing the same policy area.

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my supervisor Pieter de Wilde at NTNU, for your essential feedback, calm conversations and motivational advice. This has kept me engaged and inspired throughout the entire process. Your optimism has pushed me out of my comfort zone, resulting in a thesis I am proud to present. I also want to thank Jannicke Fiskvik for giving me relevant advice when studying security and defense policy, sending me emails with updated research, and being available for discussion when needed.

A special thanks goes to you, Arnhild Myhr Kveli, for going through the last two years with me. Supporting me on my worst days and reminding me that a good dance session solves all problems. Also, Erin Heddeland, thank you so much for all the time you spent proof reading the entire thesis, correcting every comma and spelling mistake. Last, but not the least, I am forever grateful for the support from my family, always helping me and giving me much needed breaks from an intensive process. A special thanks goes to my mom, Cecilie Nilsen, for always believing in me and helping me put my struggles in perspective.

I would also like to thank the informants that have agreed to participate in this project. Being met with positivity and interest have inspired me and provided me with more insight into the topic of the thesis. Your contributions have been extremely valuable!

Finally, to my fellow students at European Studies, thank you for five great years in Trondheim, both on and off campus. Thank you for good discussions and well-needed celebrations of all small victories, making all the long days and intense weekends at the “office” worth it.

Mari Cecilie Aae

Trondheim, May 14th 2018

Contents

ABSTRACT **III**

ACKNOWLEDGEMENTS..... **V**

LIST OF FIGURES **VIII**

ABBREVIATIONS**IX**

1 INTRODUCTION..... **1**

2 THEORETICAL FRAMEWORK **5**

 2.1 GLOBAL GOVERNANCE 5

 2.2 REALISM AND CONSTRUCTIVISM AS ONTOLOGICAL APPROACHES..... 7

 2.2.1 *Realism and the Theory of Forum Shopping*..... 8

 2.2.2 *Constructivism, Socialization and Learning, and the Theory of Historicism*..... 11

 2.3 THE CONCEPT OF REGIONALISM 15

3 QUALITATIVE CASE STUDY **21**

 3.1 CASE STUDY WITH ONE ‘CRUCIAL CASE’ 22

 3.2 METHODOLOGY AND RESEARCH DESIGN 23

 3.3 CASE STUDY IN THE FIELD OF SECURITY AND DEFENSE POLICY 27

4 THE CASE OF CYBER DEFENSE..... **31**

 4.1 CYBER SECURITY AND THE CONCEPT OF CYBER DEFENSE..... 31

 4.2 THE CYBER THREAT IN THE NORDIC REGION..... 34

 4.3 NORDIC RESPONSE TO THE CYBER THREAT 36

 4.4 CYBER DEFENSE WITHIN NORDEFECO..... 37

5 REGIONAL COOPERATION IN A GLOBALIZED WORLD..... **41**

 5.1 CYBER DEFENSE IN THE EU AND NATO..... 42

 5.2 DEFENSE COOPERATION WITHIN NORDEFECO 46

6 CENTRAL FACTORS EXPLAINING REGIONAL COOPERATION ON CYBER DEFENSE WITHIN NORDEFECO..... **53**

 6.1 GEOPOLITICS 53

 6.2 BURDEN-SHARING 56

 6.3 HISTORY OF COOPERATION 58

 6.4 TRUST 63

7 WHY NORDIC COOPERATION? A DISCUSSION OF THE FINDINGS..... **69**

 7.1 NORDEFECO AS A REGIONAL COOPERATION IN A GLOBALIZED WORLD 69

 7.2 CENTRAL FACTORS AND UNDERLYING MOTIVATIONS FOR COOPERATION 72

8 CONCLUDING REMARKS..... **73**

LITERATURE **77**

APPENDIX A – INFORMANTS AND INTERVIEW GUIDES

List of Figures

FIGURE 2.1 RELEVANT THEORIES AND CENTRAL VARIABLES FOR THIS THESIS.....	15
FIGURE 2.2 THE THEORETICAL FRAMEWORK OF THIS THESIS.....	19
FIGURE 3.1 EMBEDDED CASE STUDY DESIGN WITH ONE SINGLE CASE.....	25
FIGURE 3.2 EMBEDDED CASE STUDY DESIGN WITH VARIABLES FOR THIS THESIS.	26
FIGURE 4.1 THE NORDEFECO-STRUCTURE.....	38
FIGURE 4.2 PROCESS FROM STUDY TO ACTIVITY IN NORDEFECO.....	38
FIGURE 6.1 MAIN FINDINGS.....	67

Abbreviations

CAPA	Capabilities
COPA	Cooperation Areas
CSDP	Common Security and Defense Policy
EC	The European Community
EU	The European Union
IMF	The International Monetary Fund
MCC	Military Coordination Committee
NATO	North Atlantic Treaty Organization
NIS	Security of Network and Information Systems
NORDAC	Nordic Armaments Cooperation
NORDCAPS	Nordic Coordinated Agreement for Peace Support
NORDEFECO	Nordic Defense Cooperation
NORDSUP	Nordic Supportive Defense Structures
UN	The United Nations
WTO	The World Trade Organization

1 Introduction

The young man who usually works from the couch in his sweatpants shares the stage with the President of his country. So, I will let you do the deductions of what that means for the state of the world today (Norsk utenrikspolitisk institutt NUPI, 2018).

The Nordic states are increasingly experiencing major threats and real-life consequences of a vulnerable cyber space. The evolvement of cyber threats as real threats has resulted in the need for closer regional cooperation between the Nordic states since it is evident that such hazards are too big and complex for any nation state to handle by themselves. The Nordic Defense Cooperation (NORDEF) is one central forum focusing on developing better cyber defense capabilities as a response to the increased threat posed by foreign hacker groups (O'Dwyer, 2017). Despite initiatives from larger systems and organizations, such as the European Union (EU) and the North Atlantic Treaty Organization (NATO), the Nordic states continue to seek closer cooperation within a regional framework. The development of closer Nordic cooperation on cyber defense, parallel to closer cooperation on the same policy area in larger forums, indicates that regional cooperation still is relevant in an ever-globalized world. An investigation of the motivations for cooperation is needed to understand why the Nordic states find it beneficial to develop cyber defense capabilities in a regional forum. In addition, it is necessary with an understanding of how the Nordic forum differs from other larger systems and organizations such as the EU and NATO.

At the time of writing foreign hacker groups are targeting the military and the Nordic region is suffering from various cyber-attacks and cyber intrusions (Norsk utenrikspolitisk institutt NUPI, 2018). An example is the major cyber-attack from 2017 forcing the shutdown of the Swedish Defense Forces' Caxcis IT System – a system used to plan, manage and monitor military exercises (Defense News, 2017). This example illustrates the severity of cyber-attacks and the urgent need for strong and resilient cyber defense capabilities. As several western democracies claim that their democratic and political processes have suffered from foreign intruders on cyber space, it is evident that the world is changing, and it is time to face the consequences of the digital revolution (Rid, 2016). Thus, the focus of securing cyber space is

larger than ever amongst states, military and politicians. The increased focus of developing cyber defense capabilities is a consequence of various cyber-attacks and intrusions constantly reminding us of the vulnerabilities and weaknesses with cyber space.

Nation states have acknowledged that intergovernmental cooperation on security and defense policy is necessary to meet to challenges with securing cyber space, introducing 'the cyber security dilemma' as a central concept within the field of international relations (Buchanan, 2016). The world is at the time of writing highly dependent on digital solutions, making it necessary to take the concerns about cyber security serious. Despite difficulties finding clear evidence of who is responsible for alleged cyber-attacks, it is apparent that the uncertainty created by such attacks is resulting in a widespread fear among the political elite and the citizens, especially in the Western democratic part of the world. The widespread fear of cyber-attacks is the core of what Buchanan (2016) defines as 'the cyber security dilemma'. The cyber security dilemma derives from the familiar concept in the study of international relations, namely 'the security dilemma', indicating that states inevitably induce fear in other states as they secure themselves. Primarily, scholars of the original security dilemma seek to uncover which structural factors drive the escalatory cycle of the dilemma, and what states might do to foster stability. The security dilemma holds great relevance in cyber security, where it can explain fear caused by network intrusions between states. This thesis contributes to the recent scholarly debate on the cyber security dilemma. Further, the thesis fills a gap in the literature on regional cooperation in the case of cyber defense by aiming at explaining why the Nordic states consider regional cooperation within NORDEFECO as the preferred solution to ensure stability in their region.

The focus of this thesis is on the Nordic states¹ and their cooperation on cyber defense within the newly established cooperation NORDEFECO. NORDEFECO is the result of previous defense cooperation amongst the Nordic states, and is now formally known as a military alliance (Nordic Defence Cooperation, n.d.). By doing a qualitative case study with one case, this thesis aims to answer the research question: *Why are the Nordic states seeking closer cooperation on*

¹ In this thesis, the use of the Nordic states refers to the states Denmark, Finland, Norway and Sweden. Iceland is normally included as a Nordic state, but because Iceland only participates at the policy level of NORDEFECO, it is not included in this thesis (Swedish Armed Forces, 2012). Iceland do not have a military defense force, preventing them in taking part of the military level of NORDEFECO. This legitimize the choice of excluding Iceland in this thesis because of the focus on defense policy (Saxi, 2018).

cyber defense policy within NORDEFECO? In order to fully answer the research question, the analysis addresses the three following sub-questions:

1. What distinguishes the Nordic cooperation on defense policy, and more precisely cyber defense policies, from the cooperation within NATO and the EU?
2. How can Nordic cooperation on cyber defense illustrate the need for stronger regional cooperation in an ever-globalized world?
3. Which factors make Nordic cooperation feasible and realistic?

The thesis problematizes why the Nordic states are developing a forum for Nordic security and defense cooperation when all states have membership in other forums dealing with the same issues, such as the EU and NATO. It finds certain factors distinguishing NORDEFECO from the EU and NATO, such as cultural similarities, geographical proximity, same external threat, and similar interest in developing cyber security capabilities. In addition, the findings of the thesis lead to the conclusion that regional cooperation is the preferred forum for cooperation on cyber defense capabilities, because of its abilities to carry out activities and exercises, thus turning policies into actions. Further, I argue that trust and burden-sharing are the most crucial factors in explaining why the Nordic states seek closer cooperation on ‘high politics’ despite previous set-backs and ‘failures’.

Consisting of eight chapters, the thesis follows a regular structure for papers within the field of political science. The second chapter provides the theoretical framework of the thesis and is an essential chapter because of the deductive character of the project. The chapter combines theories within the global governance approach and regionalism, providing a theoretical understanding helpful when analyzing the empirical material in the following chapters. In addition, chapter two presents a flow chart visualizing the theoretical framework with the relevant concepts and variables for the thesis (see figure 2.2). Chapter three introduces the method selected and provides arguments as to why a qualitative case study is the most fit method for this research project. The following three chapters present the analysis, starting with a presentation of cyber defense as a case and NORDEFECO as a regional cooperation. The continuing two chapters go in depth on the debate of regionalism and globalization, the factors making Nordic cooperation possible, and the underlying motivations to why Nordic cooperation is expanding. The analysis presents the findings and consistently discusses the

findings in relation to theory and previous research. Chapter six then presents a model of the central factors with its underlying motivations for cooperation (see figure 6.1). Chapter seven summarizes the findings and discusses the findings of the three preceding chapters ensuring that enough evidence is provided to sufficiently answer the research question. The final chapter concludes the study and mentions some limitations with the research project, which I hope inspires for further research.

2 Theoretical Framework

With more of a deductive approach to the project, the most relevant starting point is to present the theoretical framework of the thesis. The thesis is not based on a single grand theory, rather it is based on a more precise and complex theoretical framework within the field of global governance. The framework consists of realism and constructivism as two ontological approaches, and central concepts such as forum-shopping, socialization, historicism, and regionalism. The concepts selected for the theoretical framework are chosen because of their relevance to the discourse on intergovernmental cooperation on security and defense policy. Based on these concepts, four relevant variables will be presented, and these are central in the analysis conducted below. The four variables are as follows; 1) geopolitics, 2) burden-sharing, 3) history of cooperation, and 4) trust.

The chapter consists of three sections, with the first focusing on the grand-theory of global governance. As the global governance theory is such a comprehensive theory, it is necessary to narrow it down by selecting two distinct but complementary ontological approaches, and present precise theories within the approaches. This is conducted to meet the criticism of global governance, stating that it is a useless theory because of its broad scope (Hewson & Sinclair, 1999). The final and last section introduces the term ‘regionalism’ and addresses the concept of regions in a globalized world. Together the three sections make up the theoretical framework of the thesis as illustrated by figure 2.2 and it will be central for the analysis and discussion in chapter four, five and six.

2.1 Global Governance

NORDEFECO is an international cooperation where several independent states have created a joint framework for intergovernmental interaction on defense policy. ‘Global governance’ seeks to explain why states choose to collaborate in intergovernmental forums to meet the challenges of the globalized world today. In order to fully understand global governance theory, one must first understand the term governance:

The definition [of governance] develops a clear *distinction between government and governance* in the sense that governance researchers no longer take an interest in government, that is, the existence of a clear hierarchy between state actions and actors, but, on the contrary, in possible bargaining mechanisms between different groups,

networks and sub-systems, mechanisms that disturb and go beyond a clearly established hierarchy between *actors* and *norms* (Saurugger, 2014, p. 106, emphasis added).

The emphasized sections of the definition, being the distinction between government and governance and between actors and norms, are the most relevant parts for the thesis. This indicates that the lines between government and governance, as well as actors and norms are becoming blurred in the contemporary society. Thus, making it challenging to find true answers to how the 'real world' in reality functions. Governance theory addresses this development and is a helpful tool in the attempt to explain the challenges of the globalized world today. In addition, global governance is a relevant theory to account for recent changes within the field of international relations, which is the case of NORDEFECO and the development of cyber defense capabilities.

As a functionalist theory, governance is both used in the study of comparative politics and international relations. Within the field of international relations, governance theory can explain the need for international systems to find solutions to global public policy problems (Saurugger, 2014, p. 103). Governance theory is a relatively new theory first used in the 1980s, and it is a successor of the structural-functional theories used in the 1960s and 1970s. What is similar with the structural-functional theories, is that governance theory also perceive the society as a complex system where different parts of the society contribute to the stability and integration of the society as a whole. By using governance theory, researchers can examine empirical mixtures of the involvement of state and society, as well as looking at the relative success of alternative formats. The public sector continues to remain the principal actor in the field of international relations. Nevertheless, governance theory also includes the influence of non-state actors (Peters & Pierre, 2009). It is evident that globalization changes the dynamics in the international society, and non-state actors are receiving more influence in the global sphere. Hence, non-state actors are gaining more importance, complementing the power of the state as the main actors.

This thesis is a contribution to a more precise approach within the field of global governance by highlighting and explaining the complexity of governance in international cooperation, more specifically in the intergovernmental cooperation NORDEFECO. In the 1990s, the concept 'global governance' emerged in order to understand the global change in the world after the

end of the Cold War. Global governance knows no boundaries, thus it implies studies at global, international, regional and national level. In addition, global governance includes studies on geographic, social, cultural, economic and political levels (Rosenau, 1995). In other words, global governance is an open-ended theory aiming to improve the understanding of various aspects of globalization. This can explain why the theory has been criticized for being “virtually everything”, making it useless because it is too broad and complex to be used as a conceptual tool (Hewson & Sinclair, 1999). However, this criticism could rather be a criticism of how the world has developed, with more globalization and closer ties between social, economic, political and geographic sectors. Today the world is more interdependent than ever, and instead of criticizing the theory of global governance one should instead study more precisely how it can be used as a tool to explain the world as we know it today.

The theory of global governance leads me to investigate in depth the motivation for intergovernmental cooperation by looking at central factors as to why states choose an intergovernmental forum to solve pressing issues, such as cyber defense. One central aspect of globalization and global governance theory is the emergence of new systems and institutions in the international sphere. Today the world has several international institutions trying to meet the challenges of globalization, such as the United Nations (UN), NATO, the World Trade Organization (WTO) and the International Monetary Fund (IMF). As the world moves toward new forms of global governance, the existing international institutions are being questioned and evaluated based on their effectiveness and successful results. Even though international institutions are not always successful, their importance are increasing (Keohane, 1998). As anticipated by Rosenau (1995, p. 20) “[g]lobal governance [...] is likely to consist of proliferating mechanisms that fluctuate between bare survival and increasing institutionalization”. This pose one central question for the thesis: Does the increased institutionalization of Nordic cooperation illustrate an example of bare survival or is it more to it, such as an offensive wish to cooperate? The following section presents four relevant factors influencing the motivation for cooperation based on two distinct ontological approaches.

2.2 Realism and Constructivism as Ontological Approaches

The use of global governance as the general theory for a project opens up for various ontological approaches, such as constructivism and realism. These two approaches are fairly distinctive, with the first being more suitable for explaining cultural globalization and the second for

analyzing economic globalization (Hewson & Sinclair, 1999). However, one can also view these two approaches as combined and interlinked, where increased economic globalization leads to increased cultural globalization and vice versa. By combining the two ontological approaches, it must be acknowledged that globalization is a process consisting of various parts, and that these parts are not developed in different bubbles independent of each other. Rather, one must take into account some of the complexity of the 'real world', and get a better understanding of how one part of the process also has an impact on other parts of the same process. This is in line with the conception of world politics "as all-encompassing" in need of a holistic way of approach (Rosenau, 1992, p. 12). By combining realism and constructivism, the explanatory power of this theoretical framework increases, making the thesis more holistic compared to studies only focusing on either realism or constructivism. Also, to include two distinct ontological approaches gives increased legitimacy to the conclusion of the thesis, stating that realism had larger explanatory power up until 2014. However, from 2014 and onwards constructivism has replaced realism as the ontological approach with most explanatory power.

2.2.1 Realism and the Theory of Forum Shopping

First, the realist approach is known for the perception that world politics is a power struggle with no moral judgements. Within the field of security and defense policy, realism tends to focus on geopolitical relations between states in an anarchic system with no overarching political authority. Actors are the most central element within this approach, and states have for a long time been perceived as the principal actors in the global sphere. The main assumption is that states are self-centered and able to make rational choices based on what serves their own interest the best, following the logic of consequences (Bell, 2017). However, with the global governance theory, the focus on states is changing and when conducting research on economic globalization, one central element is the shift from state power to market power. The more globalized the world becomes the more power belongs to the free market (Hewson & Sinclair, 1999). Even though the state power is being challenged by the market power, economic globalization also leads to closer cooperation between state and non-state actors (Hoffman, 2007). Hence, the main idea of economic globalization is the shift from states as the principal actors in the global sphere to the inclusion of non-state actors. In other words, the influence of non-state actors in the global sphere is increasing as a result of an increasing market power.

This development is distinct to the previous world order where states were the only influential actor in the global sphere.

More specifically, and relevant for this thesis, is to include a theory that can explain why nation states choose certain forums for certain issues, and how a chosen forum is beneficial for the members of that forum. One central theory that provides a rational choice perspective based on the realism approach is the theory of forum shopping. Forum shopping aims at explaining why certain actors choose certain intergovernmental forums to solve pressing issues or to promote its interests. It is an under-researched but highly relevant theory helpful in understanding the dynamics of global governance. Broadly speaking, the theory of forum shopping contributes to the understanding of the influence various forums have on the world order, and how forum shopping can lead to the possibility of a potential restructuring of existing regimes (Murphy & Kellow, 2013).

Economic development is one way of measuring if something is beneficial or not. A forum is beneficial in economic terms if the gains are larger than the costs. In addition, the budget will increase for the forum in accordance with the number of members, opening up for the possibilities to develop competences that are too costly for one single state. Central factors explaining intergovernmental cooperation are comparative advantage and cost-efficiency. Comparative advantage signifies that states in one forum have access to the resources in a specific region, and that they gain especially beneficial conditions for effective production compared to other regions (Røste, 2013, pp. 175-219). It will most likely be economical beneficial for actors in a region to establish a forum so that the region gains from its comparative advantage and increase the cost-efficiency of certain solutions. If a forum in a specific region succeed in making cost-efficient solutions based on their comparative advantage, one could say that the forum is beneficial for its members. Thus, rational reasoning can explain why certain actors choose to be members of a forum, presenting burden-sharing² as the first central factor for cooperation.

² Burden-sharing indicates that states establish a cooperation to share the costs of a certain development. In the case of this thesis one can argue that the Nordic states decided to establish NORDEFECO so that they could share the burden of developing a strong and resilient defense sector. When states share the burden of a specific problem they also share the potential gains once a solution is found, such as certain cyber defense capabilities. I will come back to the discussion of burden-sharing in chapter six.

Even though economic factors are central in rational choice theory, it is important to keep in mind that political factors also play a key role. Forum shopping addresses both economic and political conditions and claims that nation states strategically select the international venue most likely to promote their specific policy preferences. Hence, nation states are still the main actors in this theory. The actors use different strategies in order to select the best forum for promoting their preferences, with the goal of promoting a decision favoring their interests: “In forum-shopping, the shopper strategically selects the venue to gain a favorable interim decision for a specific problem” (Alter & Meunier, 2009, p. 17). This indicates that nation states are able to make rational decisions and strategically select the ‘right’ forum, based on an evaluation of potential costs and benefits both in economic and political terms.

For states, forum shopping is an important part of the strategic search for advantage by having issues dealt with in an appropriate arena. Global governance is not only spread over various functional issue-based areas, but also over numerous regional arenas. In particular cases there are strength in numbers making large forums beneficial, while in other settings small forums are ideal following the possibility to exert more influence on the decisions being made. In addition, some systems are limited in membership based on geographical and/or functional issues. One notable example of a small geographical forum is the Nordic Council with its five members; Denmark, Sweden, Finland, Iceland and Norway (Kellow, 2012). Further NORDEFECO is an example of a forum limited in membership based on both geographical and functional issues. The focus of geography introduces the second central factor for cooperation that is geopolitics.

Based on the theoretical approach of realism and the theory of forum shopping, two central variables can explain why the Nordic states seek closer cooperation within the NORDEFECO framework. The two variables are based on a rational choice way of thinking where power struggle and economic considerations are in focus. Geopolitics represents the realist approach with the perception of world politics as a power struggle, and that membership in NORDEFECO is closely linked to geography. Burden-sharing, as the second variable, represents the shift in world politics as a result of economic globalization, and that membership in NORDEFECO are also based on rational and economic considerations, such as cost-efficiency and comparative

advantage. These two variables will be combined with two variables from the constructivist approach, as illustrated by figure 2.1 presented below.

2.2.2 Constructivism, Socialization and Learning, and the Theory of Historicism

The second approach used in this thesis is constructivism. In the field of international relations, constructivism is a relatively new approach focusing on world politics as socially constructed. According to Wendt (1999, p. 1), there are two central principles of constructivism: 1) “[T]he structures of human association are determined primarily by shared ideas rather than material forces, and 2) the identities and interests of purposive actors are constructed by these shared ideas rather than a given nature”. Based on these two principles, it is evident that this approach is fundamentally different from that of realism. Instead of rational reasoning for actions, constructivism argues that shared ideas can explain why actors choose to interact with each other and develop collaborations. Following, these shared ideas influence the micro-level by constructing the identity and interests of individual actors. Constructivism seeks to explain processes at both the macro- and micro-level. Albeit, the focus of this thesis is only on the macro-level.

Instead of making rational decisions based on self-interests, scholars of constructivism believe actors make decisions based on shared ideas and norms. Constructivism can be understood as a critique of structural realism stating that ideas must be considered alongside material forces in any empirical analysis. Based on this way of thought, “whether a system is conflictual or peaceful is a function not of anarchy and power but of the shared culture created through discursive social practices” (Copeland, 2006, p. 1). Such understanding of constructivism indicates that globalization can be explained by shared ideas and a common culture, also called norms. Norms are the most central element in this approach, and these have the capacity to change. The importance of shared ideas and norms can explain why constructivism often is linked to the explanation of cultural globalization.

Grounded in a constructivist perception of international relations, the actor makes decisions based on a logic of appropriateness, not on a logic of consequences as suggested by the realist approach. Making decisions based on what is appropriate require socialization of states that leads to the internalization of new roles or the establishment of group norms. Socialization can

be defined as “a process of inducting actors into the norms and rules to a given community” (Checkel, 2005, p. 804). When following a logic of appropriateness, the actor bases its decision-making on what is expected from a group following the norms and rules of that specific group. These groups can develop and become institutions, and these institutions can either be promoters or sites of socialization. Further it is important to note that states entering a new institutional arenas are in no sense free agents: they are embedded in multiple domestic and international contexts (Checkel, 2005). This makes the development of new institutions complex, with different influencing factors at all levels.

Since the focus of this thesis is at the macro-level, the main actor is the state. The aim is to understand how learning and socialization contribute to the explanation of why nation states seek closer cooperation on policy areas that are considered to be ‘high politics’³. This leads to the introduction of one central aspect within constructivism that is the undertheorized perspective of an intergovernmental socialization and learning process, where interaction triggers the internalization of norms. As a common culture has the ability to evolve and change, the “‘member states’ perception of their own political interests evolve due to an international socialization process” (Saurugger, 2014, p. 152). This view fits under the analytic perspective of social constructivism because it follows a logic of appropriateness. Defense policy is a policy area in international relations where states often are hesitant to agree on intergovernmental cooperation. This can be explained by the difficulties many countries face when having to trust other countries on issues regarding security and defense policy (Buchanan, 2016). Based on this challenge, it is interesting to go in depth on how socialization can build trust, and how the process of socialization and learning can be important for states agreeing to closer cooperation on issues which falls under the category of high politics.

Trust-building factors are essential in order to understand NORDEFECO, and requires further elaboration. Trust in international relations is difficult to measure and explain, and it is not a given that more socialization leads to more trust. Trust-building is a time consuming process requiring socialization and learning, where the involved states recognize the value and benefits with intergovernmental cooperation. According to Andrew Kydd (2000, p. 399) trust is first

³ High politics are political areas that are vital for the very survival of the state. Defense policy is an example of a sector falling under the category of high politics.

built by small steps generating reassurance: “[T]rust reassurance can be produced by small opening cooperative gestures, and [...] this can lead to full cooperation between trustworthy actors”. Trusting other states is a demanding task that include taking risks and being aware of potential dangers in a such a relationship. Thus, trust is closely linked to fear, and only by going beyond “cheap talk”, trust is built by making the trustworthy actor do something that the untrustworthy actors would hesitate to do (Buchanan, 2016; Kydd, 2000). Even though trust-building is a difficult and long process, some factors make the process easier. Small states find it easier to trust each other because both parts will “benefit from security guarantees provided by other states” (Buchanan, 2016, p. 163). Further, a good working relationship and communication mechanisms between the parties involved facilitate the process. When ensuring communication mechanisms, it is crucial that the states involved in a cooperation have access to all the relevant information from the other states, and that no parties intentionally hide vital information from others. Last, albeit not least, it is easier to build trust in forums with fewer members facing the same threat (Buchanan, 2016, pp. 163-169). Trust is the third central variable in this thesis, helpful in explaining why the Nordic states are developing closer intergovernmental cooperation on high politics, and more specifically on defense policy.

To fully understand NORDEFECO, it is necessary to look closer at the past and how previous Nordic cooperation has been central in explaining NORDEFECO as we know it today. As mentioned above, socialization and learning is a long process. In order to get a better understanding of the establishment and development of an international institution, one central factor to study is the history leading up to such a development. The historicist approach is a theory focusing on the role of history in global governance (Hewson & Sinclair, 1999). The historicist approach seeks to create stronger ties between the literature on international relations and the historical literature, with the aim of drawing lines from the past to the present. Going back to the past to gain a better understanding of the process leading up to the present is valuable, and can be perceived as a complementary factor to the element of norms. When applying this approach the aim is to “emphasize the distinctiveness of social phenomena in history” (Cello, 2017, p. 240). Hence, the fourth and last variable included in this thesis is the historical perspective providing a new dimension as to why the Nordic states are developing a Nordic forum dealing with security and defense policy.

Based on the theoretical approach of constructivism and the theories of socialization and historicism, it is necessary to limit the scope of such a comprehensive approach by focusing on the two variables mentioned above; trust and history of cooperation. These variables will be central in the analysis and contribute to answering the research question. Trust is chosen as one variable following its close link to the development of norms as a result of socialization and learning. Group norms create stability and predictability which are crucial factors in building a trusting relationship in the international sphere; a sphere usually perceived as an anarchic system characterized by self-interest and rational behavior. History of cooperation is chosen as the fourth variable, and it is a central factor in order to fully understand the development of NORDEFECO. Since the constructivist approach focuses on the long process of developing a logic of appropriateness, it makes the historical perspective crucial to understand the 'status quo'. Represented by the historicist approach, the focus of the fourth variable is therefore on linking the past to the present.

To summarize, the two ontological approaches selected for the theoretical framework are indeed possible to combine despite of a longstanding belief that they are competing approaches. Because of the fundamental disagreement between the two distinct logics, the aim of the thesis is to find out if one of these logics can explain NORDEFECO better, or if they have the most explanatory power combined. By including both realism and constructivism, as illustrated by figure 2.1, the theoretical framework provides a more objective approach to the analysis.

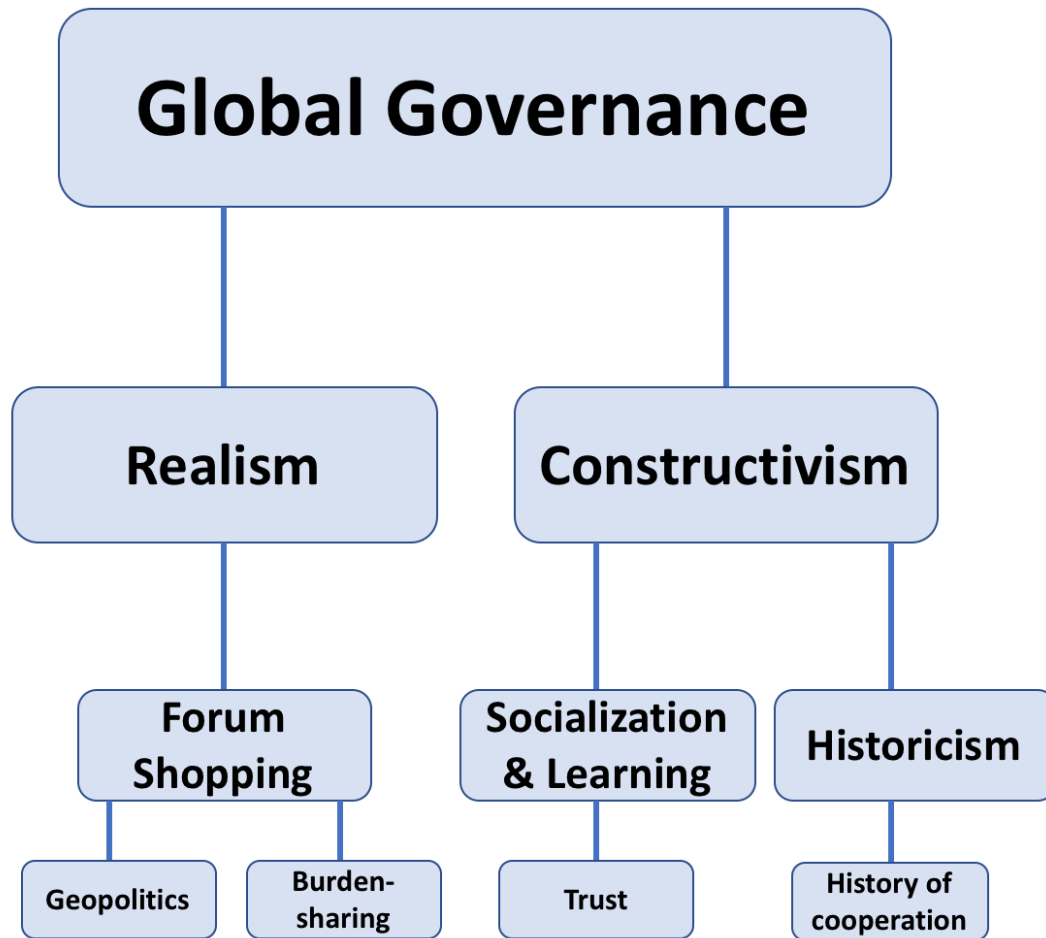


Figure 2.1 Relevant theories and central variables for this thesis.

In the light of this approach, I will now present the third and final part of the theoretical framework focusing on the contested concept of ‘regionalism’. I have chosen to include this concept since NORDEFECO can be viewed as a regional cooperation, and it contributes to the discussion on the correlation between globalization and regionalism.

2.3 The Concept of Regionalism

The literature on regionalism in general, and security regionalism specifically, is an important contribution to the analysis because it leads me to study the development of NORDEFECO in a global context. To address the question asked at the end of section 2.1. about the increased institutionalization of Nordic cooperation, it is beneficial to look closer at the concept of regionalism. NORDEFECO is perceived as a regional cooperation, not an international institution, and it is therefore necessary to include more extensive literature on the role of

regions in international relations. The distinction between globalization and regionalism is a central element in global governance theory, and one cannot explain the development of a regional cooperation by only using general literature on global governance. As stated by Rosenau (1995, p. 16) “the world is too disaggregated for grand logics that postulate a measure of global coherence”. In order to understand the disaggregated world, it is necessary with focus on more precise logics, such as the concept of regions and security regionalism.

First, a definition of regionalism is needed, in addition to a better understanding of the concept of regions. The focus of the thesis is on regions with a space embracing two or more national economies, also called a macro-region (Rosenau, 1995). Albeit, there are no clear definition of what constitutes a macro-region. According to Russett (as quoted in Mansfield & Solingen, 2010, p. 146) a region is defined as a group of countries with “geographic proximity, social and cultural homogeneity, shared political attitudes and political institutions, and economic interdependence”. This definition is in line with the argument in the section above, stating that both realism and constructivism are relevant approaches to explain intergovernmental cooperation. Even though many scholars argue that geographical proximity is a condition for a region, other scholars argue that one can speak of regions in non-geographical terms as well. In this thesis, the understanding of regions is based on the definition by Russett requiring geographic proximity. This is in line with the description of a region as “patterns of interaction that span established political boundaries and at the same time remain within a delimited geographic space” (Rosenau, 1995, p. 25).

The concept of regions also introduces an important distinction between the term ‘regionalism’ and ‘regionalization’. This distinction is a result of the ontological disagreements of what constitutes a region. First, regionalism is known as the political process marked by cooperation and policy coordination. Regionalization on the other hand is known as an economic process with trade and investments. This distinction can be explained by another different, but related understanding of the distinction where the focus of regionalism is on the macro-level and is a top-down approach, while regionalization begins at the micro-level and is a bottom-up approach (Mansfield & Solingen, 2010). Because of the research question of the thesis, the most relevant term in this context is the term of regionalism. According to Pempel (2005, p. 19), “regionalism involves primarily the process of institution creation. It occurs most conspicuously when nation-states come together through top-down activities—deliberate projects involving

government-to-government cooperation”. Regional institutions are created in order to deal with transnational problems that several nations have in common. When states agree to establish a regional cooperation, it is a rational decision to reduce costs and further their self-interests at the same time as the states agree to mutually bond, which enhances the level of trust among the member states (Pempel, 2005, p. 19). Based on this, it is evident that both the realist approach and the constructivist approach are highly relevant when studying regionalism.

Since it is established that regionalism is the most relevant concept for the thesis, one should be aware of the difference between “old” and “new” regionalism, and that regionalism is a dynamic concept. Old regionalism is more concerned with economic integration and peace where the nation-state is seen as the problem, rather than the solution. This reflects the functionalist, and later on the neofunctionalist, way of thought in Europe up until the 1970s. In the 1970s, Europe, and more specifically the European Community (EC), experienced a period of ‘Eurosclerosis’, marking the beginning of the term ‘new’ regionalism. The central phenomenon in new regionalism is globalization, and the challenges posed by a world that is becoming more and more interlinked. Because of the complexity of globalization, regions developed in recent time are the result of a more comprehensive, multidimensional process where also non-state actors are central. Similar to the process of globalization, the regions are constantly changing and they have to be understood as subjects in the making. Also, it is important to keep in mind that the development of regions is not a one-way process because some regions might fail and disintegrate (Hettne, 2005). Based on the distinction between old and new regionalism, it is evident that the development of regions is more complex and comprehensive today than before the 1970s. First regionalism was a central concept in the field of political economy and peace studies, and it just recently became a central concept within the field of international relations. This can be explained by the fact that economic issues and peace were central during the old regionalism, but during the development of new regionalism issues such as security have emerged, which is more related to the field of international relations and defense studies.

Despite the fact that security policy is high politics, recent developments indicate that it might be beneficial and/or necessary for a group of states to establish regional cooperation to ensure the security and the stability of a certain state and the region it belongs to. Security regionalism is a relatively new concept within the field of regionalism. Nevertheless, it is now considered

as a genre of its own (Hettne, 2005). The focus in security studies is “on the safety of the state, its society, and its core values from physical harm and military coercion by external sources” (Morgan, 1997, p. 21). Accordingly, when establishing security regions the aim is to protect its members from physical harm and military coercion. This is often the case if the security of a given state cannot be guaranteed by themselves. For a regional cooperation on security issues to be successful, the members of such a region should hold a high level of interdependence on security, in addition to geographical proximity. In the words of Buzan (1991, p. 190), security regionalism is relevant for a “group of states whose primary security concerns link together sufficiently closely that their national securities cannot realistically be considered apart from one another”.

Even though the world is becoming more and more globalized, this does not necessarily lead to less regional cooperation. Regionalism is without doubt a highly debated concept with various definitions, interpretations and sub-categories. However, it will be a valuable concept in this thesis due to the link between regionalism and globalization. The literature on regionalism contributes to a better understanding of why states seek closer regional cooperation on defense policy despite increased effort in larger international institutions working with the same policy area. By using the theoretical framework of global governance as illustrated by figure 2.2, this thesis addresses the question whether more globalization imply more or less regionalism.

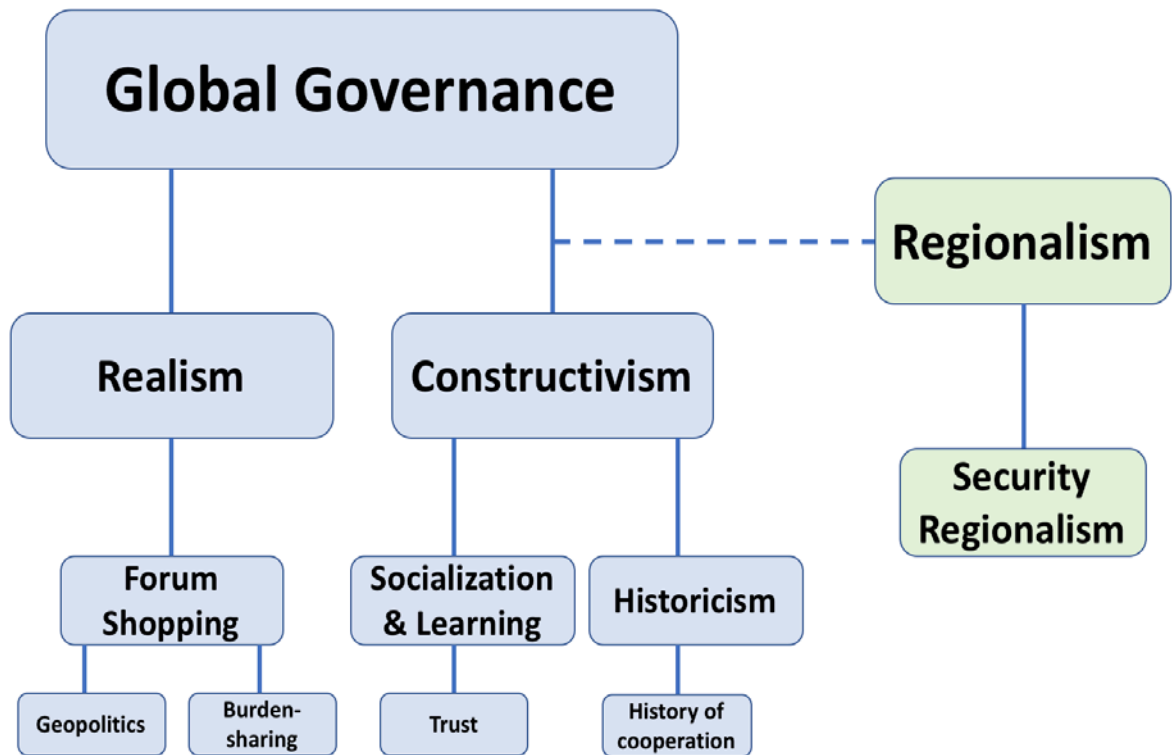


Figure 2.2 The theoretical framework of this thesis.

By looking closer at the Nordic cooperation on defense policy within NORDEFECO, I argue that when it comes to high politics such as security and defense policy, regional cooperation is often the most obvious choice. I will do so by using the case of cyber defense and the four independent variables; 1) geopolitics, 2) burden-sharing, 3) history of cooperation and 4) trust. Before presenting the analysis, an elaboration of the selected method and its methodological challenges is needed. The next section presents the case study method and the research design of this thesis, in addition to fundamental challenges when doing research on security and defense policy.

3 Qualitative Case Study

This thesis is a qualitative case study with the purpose to “gain better understanding of the whole by focusing on a key part” (Gerring, 2007a, p. 1). The focus of the thesis is on the cooperation NORDEFECO, and the aim is to gain better understanding as to why Nordic states are seeking closer cooperation within this intergovernmental framework. I am then asking a ‘why’ question about a contemporary event over which I, as the investigator, have little or no control (Yin, 2003, p. 9). In order to answer the research question, I have chosen the case of a policy field, more specifically the cooperation on cyber defense. Cyber defense is a relatively new phenomenon in the field of international relations, and little research is conducted on NORDEFECO as an intergovernmental forum for cooperation. In other words, by using the case of cyber defense, the aim is to get a better understanding of NORDEFECO as a whole.

The case of cyber defense is a relatively new case that requires limitations in time, space, subject of analysis, and problem. The timeframe of the study is from 2009, when the Nordic states established NORDEFECO with a Memorandum of Understanding, up until 12th of April 2018 when the last interview for this research project was conducted (The Ministry of Defence of the Kingdom of Denmark, The Ministry of Defence of the Republic of Finland, The Ministry of Foreign Affairs of Iceland, The Ministry of Defence of the Kingdom of Norway, & The Government of the Kingdom of Sweden, 2009). A case study also requires a given space that will be investigated. The space for this case study is more of an abstract space, namely the cyber space. This is a different space than the ‘real’ world, but it does indeed affect what happens in the ‘real’ world. Further, the chosen subject of analysis is NORDEFECO as an intergovernmental cooperation where representatives from the Defense Secretaries represent each member state (Nordic Defence Cooperation, n.d.). Hence, the level of analysis is mainly the international level, or more specifically the regional level, and the aim is therefore to explain a system, instead of opening up the ‘black box’ of each member state (Singer, 1961). The problem of the thesis is *why* the Nordic states have established a Nordic cooperation on cyber defense, when all the member states are members of either the EU or NATO, or both systems/organizations, whom also work with developing stronger and better cyber defense capabilities.

Inspired by the work of Stephen Van Evera (1997), I will conduct a case study analysis in order to find out the impact of omitted variables. The case of cyber defense within NORDEFECO is a

challenging case, consequently it is a need to look at several variables for why a closer institutional framework is being developed. This includes theory building, which in this thesis consists of a conceptual framework based on theories within the global governance approach as presented in chapter two. The conceptual framework will be compared to the empirical material gathered from interviews, official documents, previous research and other relevant information, and its explanatory power will be evaluated based on this comparison.

3.1 Case Study with One ‘Crucial Case’

Because of the complexity of the case chosen for the thesis, the thesis will not be a large-*n* study. Rather I will conduct a qualitative case study with only one single case. It is important to note that the purpose of the study is not external validity, instead the purpose is to develop a deeper understanding of one specific occurrence, which in this case is the development of a Nordic cooperation on defense policy (Gerring, 2007b). Following this, a qualitative case study with one case is the most fit method in order to answer the research question posed in the introduction.

The aim of the thesis is to provide sufficient evidence supporting the argument that a combination of realism and constructivism can to a larger extent explain the development of cyber defense capabilities in NORDEFECO over time, than what would be the case with a theoretical framework only consisting of one ontological approach. The case chosen for this thesis is central in the evaluation of the explanatory power of the theoretical framework, and should according to Gerring (2007b) be labelled a ‘crucial case’. The role of theory is relevant when doing a case study with one crucial case, and this thesis provides room for further theory building. When it comes to case study as a method, the main goal is to gain knowledge of ‘real world’ events, being a rather challenging task, especially when it is not clear what the ‘real world’ is (Moses & Knutsen, 2012, p. 118). By combining two distinct ontological approaches the thesis provides a nuanced explanation of real world events.

Even though case study has been considered as one of the weakest methods within the field of social science, it has large explanatory power. With help from theoretical approaches, case studies’ main focus is to answer *why* certain actions takes place (Evera, 1997). One central challenge with the case chosen for this thesis is that it is crucial in a somewhat weaker sense,

indicating that the case cannot be explained precisely by one single theory (Gerring, 2007b). In other words, the main goal of a case study with a ‘weak’ crucial case should be to answer the why-question, not the if-question. Also, by using open-ended theories from the global governance approach and regionalism, the aim is to conduct a ‘heuristic case study’ providing room for theory building (Eckstein, 1975, p. 104, as cited in; Moses & Knutsen, 2012). Global governance and regionalism are both theories and concepts in development, open for change and expansion.

3.2 Methodology and Research Design

Case-study in general, and single-case study specifically, is a highly criticized method in social science because of its methodological challenges. In order to understand the strengths and weaknesses of the case study as a method, it is necessary with a clear distinction between ‘method’ and ‘methodology’:

[M]ethod refers to research techniques, or technical procedures of a discipline. Methodology, on the other hand denotes an investigation of the concepts, theories and basic principles of reasoning on a subject. The methodology of the social sciences, then, is to be understood simply as philosophy of science applied to the social sciences (Moses & Knutsen, 2012, p. 5).

Based on the definition, methodology is a broader and more challenging term than one specific method, and it can be illustrated as a toolbox (e.g. methodology) with many different tools (e.g. methods). Research within the field of social science is influenced both by the ontological and epistemological positions of the author, making it impossible to conduct fully objective studies. However, this does not indicate that research within social science is meaningless. Instead, it strongly suggests that it is need for discussion amongst scholars within the same field to encourage students and researchers to “embrace a broader, more pluralistic approach to knowledge” (Moses & Knutsen, 2012, p. 6). One central question every scholar has to ask himself/herself is how do we know?

When using theory or a theoretical framework in a crucial case study it will be a limited to none external validity. Therefore, one cannot expect the result of this thesis to have a high degree of generalizability (Gerring, 2007b). Despite the challenge with external validity, it is possible to ensure that the internal validity is high by having control over the variables used in the study.

Even though this is possible, it is challenging to control the variables in qualitative research (Moses & Knutsen, 2012, p. 60). In general, ensuring external and internal validity is difficult in social and political research, and not only a challenge for case studies. However, the challenge with external validity might be larger in case studies than in other qualitative research designs. As external validity is nearly impossible in single case studies, the question that arises is how to ensure a high degree of internal validity?

In order to strengthen the internal validity of this project, the case study is in need of an accepted research design. Internal validity refers to the control of variables used in a research project (Moses & Knutsen, 2012, p. 60). A high degree of internal validity is a result of reduced uncertainties “so that causal inference is possible” (Gerring, 2007a, p. 151). The design of this case study is a single case with multiple units of analysis, also called an embedded case study design. In the analysis, attention is given to four sub-units which are important devices to ensure that the case study stay on track and does answer the research question. Also, by including sub-units the insight into the single case is enhanced, resulting in a more extensive analysis (Yin, 2003, pp. 39-46). Figure 3.1 is a general illustration of an embedded case study design (Yin, 2003, p. 40). The dotted lines between the context and the case indicate that the boundaries between the case and the context are to some extent blurred:

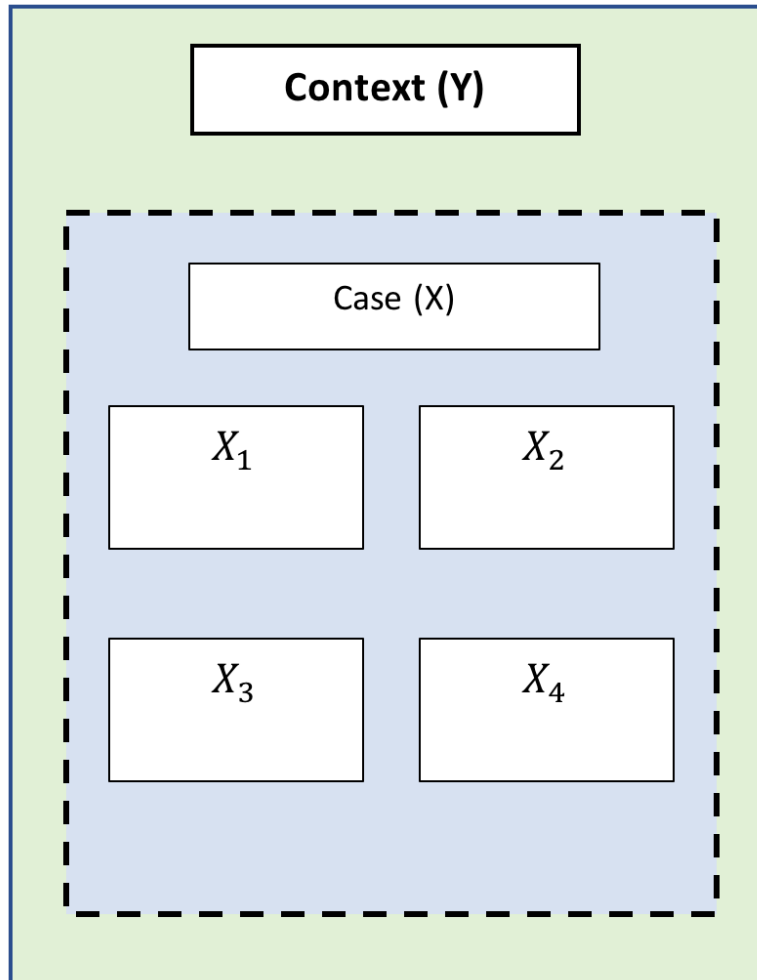


Figure 3.1 Embedded case study design with one single case.

Unfortunately, an embedded case study design has some challenges. By including four sub-units there is a risk that the larger aspect of the case is being ignored by the failing to return to the larger unit of analysis. If the four independent variables prevents the researcher from returning to the larger case, the case study itself will shift its orientation (Yin, 2003). This will complicate it further by making it difficult to explain the context. In order to avoid such mistakes, it is important to constantly be reminded of the purpose of study, being to explain NORDEFCO and the larger case of cyber defense. Doing this will ensure that the nature of the case study stay constant. Another central challenge with ensuring internal validity in a case study is the difficulties with holding all else constant when investigating the correlation between the variables of interest (Gerring, 2007a, p. 157). As this is not an experimental study, it is impossible to ensure that peripheral factors are held constant. Making it important to keep in mind that other factors than the ones included in this thesis can influence the result. Therefore, I will encourage other students and/or researchers to tackle the same research question with different independent variables, in order to validate the results of this thesis.

The analytic strategy chosen for this thesis is the inclusion of complementary explanations based on the theoretical propositions (Yin, 2003, pp. 109-115). These complementary explanations are the four independent variables mentioned above, which will be analyzed and discussed in chapter six. In figure 3.2 , you will find the variables making up the analysis in the embedded case study design.

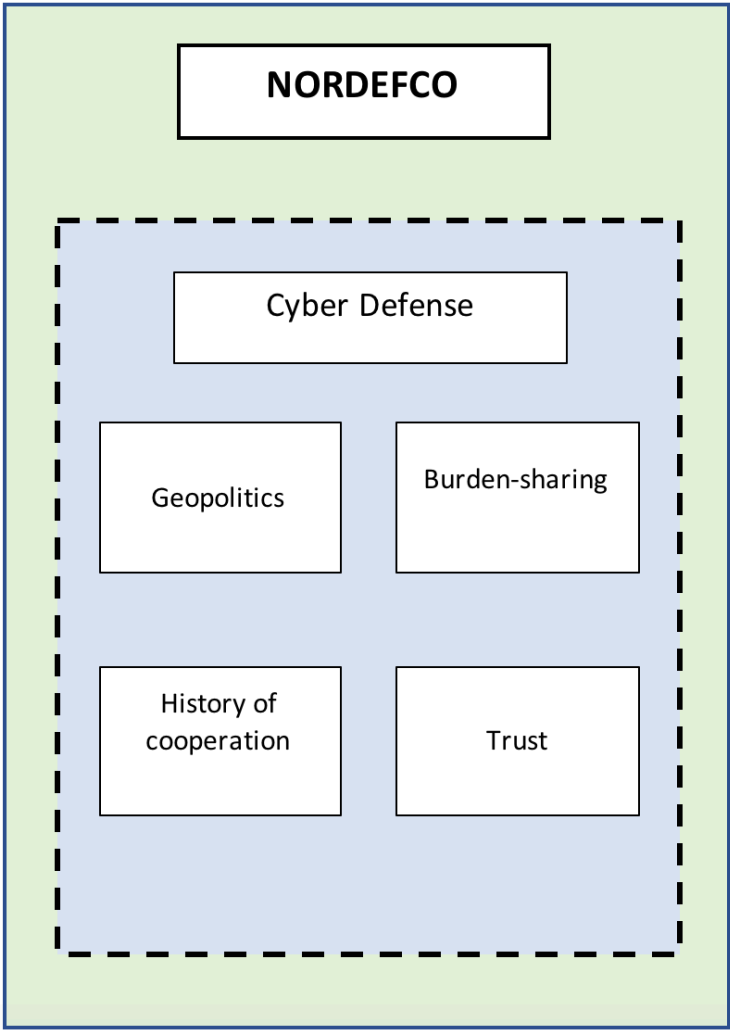


Figure 3.2 Embedded case study design with variables for this thesis.

Even though an embedded case study design is challenging the internal validity of the project, it is important to remember that the aim of the thesis is to contribute to the literature on why Nordic states seek closer regional cooperation on cyber defense. Hopefully this contribution can trigger more research and perhaps be used at a later stage in combination with a more formal research design. In other words, this case study should be considered as an exploratory case study. The research project is solved with the perception of research as a process where knowledge is developed in small steps toward a greater goal, as suggested by Tjora (2012). This

thesis is then hopefully a small step towards more research on regional cooperation on cyber defense, within the field of international relations.

There are different ways to approach the aspects of explanatory factors for why the Nordic states seek cooperation in NORDEFECO. Two central, but distinct, aspects are the behavior of the actors in such a cooperation, and the motivation or reasons for why it happens. This thesis will focus on the second aspect. Motivation can both be dependent and independent variables (Singer, 1961). In this thesis motivation will be treated as independent variables, as illustrated by figure 3.2. By looking closer at four different, albeit complementary factors for cooperation, the aim is to find the underlying motivations for cooperation and give an answer to which is/are the most evident factor(s), and motivation(s), for cooperation. I have selected four independent variables because a limited number of explanatory factors makes it possible to go in detail on each of them. Thus, the reader gets a better understanding of how these four factors can be linked to the explanation of why the Nordic states seek closer cooperation on defense policy within NORDEFECO.

3.3 Case Study in the Field of Security and Defense Policy

It is important to keep in mind that foreign- and security policy is closely interlinked, and that each member state's main priority is to secure its citizens from external threat. This thesis will not focus on the foreign policy aspect, therefore I will not go in depth on each state and their diverging interests (Moravcsik, 1997). Instead, the focus will be on how states act in the global sphere, represented by the states' respective defense ministers. Within the field of research on foreign and security policy it has for a long time been argued that the state is the main actor in the global society, and that both internal and external sovereignty is crucial for independent states (Fermann, 2013). However, the sovereignty of a state is restricted in the global sphere by various factors. As mentioned in chapter two, the world is changing at a fast pace because of globalization and digital solutions, making it necessary for scholars within social and political science to adapt to these changes. By using the theory of global governance and regionalism this thesis highlights the need to view international relations through 'new theoretical lenses'.

The research question is difficult to answer mainly because of three major challenges; 1) NORDEFECO is a cooperation focusing on defense policy, 2) it is a fairly new cooperation with

a short history, and 3) cyber defense is a new policy area with several uncertainties. The first challenge makes it difficult to find trustworthy empirical evidence because most of the relevant information is kept secret. Second, such a new cooperation makes it difficult to find historical documents. Last, but not the least, there is not much research done in the field of political science on cyber defense. In order to meet these challenges, the theoretical framework presented above will be central in the analysis as a compensation for lack of empirical evidence.

Out of the three challenges, I believe the largest challenge for the thesis is the lack of clear empirical evidence. However, the thesis includes empirical material from various sources which shed light on the unique strength of case study as a method. Case studies do have the “ability to deal with a full variety of evidence [...] beyond what might be available in a conventional historical study” (Yin, 2003, p. 8). This way of doing research can be compared to the combining of methods, and fits under the category of triangulated investigation within the method of qualitative case study (Read & Marsh, 2002, p. 237). In other words, this qualitative case study combines different empirical evidence in order to fully answer the research question, strengthening the validity of project.

Even though most of the information regarding security and defense policy is kept secret, there are some official documents available. One important source is the annual reports published by NORDEFECO, with the first report published in 2010 up until the latest report published in 2018. In addition to this, it is relevant to use the official documents on the long-term agreements for defense policy of the respective states, and their national official cyber security strategies published by the governments. Also, the EU’s official cyber security strategy published by the European Commission is used. To complement the primary sources in form of official documents, the thesis also includes secondary sources in the form of articles from newspapers, information from various web pages, in addition to relevant podcasts and video files when necessary.

To get more insight in the underlying motivations for cooperation, I chose to conduct elite interviews with one national representative, two national bureaucrats and one Norwegian Lieutenant-Colonel, all with close ties to NORDEFECO. In addition to this, I conducted one interview with a Norwegian Senior Staff Officer working as an advisor to the chief of the

Norwegian Cyber Defense Force, a division in the Norwegian Armed Forces. In total the selection consists of five informants, and the interviews were conducted as semi-structured interviews with room for digression (Tjora, 2012). Because this thesis has more of a deductive approach, the interviews were conducted at the end of the project. The first interview was scheduled to the 15th of March 2018 and the last interview was scheduled to the 12th of April the same year. This is in line with the advice given by Richards (1996, p. 201) and Lilleker (2003, p. 212) to conduct the interviews in the end of the research project, ensuring that I had enough knowledge of the topic before approaching competent people working close with the topic of the thesis.

The informants were found and contacted based on the snowball method, with one informant leading to the next one (Tjora, 2012, p. 230). Therefore, I asked at the end of each interview, except the last one, if they knew of anyone else who could be relevant to contact for the research project. When selecting informants, it was important that the informant was either connected to NORDEFECO or to the case of cyber defense. The selection of informants ended up with consisting of one national representative only connected to NORDEFECO, and not cyber defense, and one representative only connected to cyber defense and not to NORDEFECO. The two national bureaucrats and the Norwegian Lieutenant-Colonel were connected to both NORDEFECO and cyber defense, with one working in the Finnish Ministry of Defense, while the two others are working in the Norwegian Ministry of Defense. All interviews except one were conducted in Norwegian, which were the native tongue of the informants, and the interview with the Finnish bureaucrat was conducted in English. Since most of the interviews were scheduled short time in advance with little time to prepare, they were conducted over the phone. This gave me time to focus on preparing the interviews instead of spending time on travelling and other logistical challenges. The interview with the two informants in the Norwegian Ministry of Defense was the only interview planned well in advance, giving me time to be well prepared and travel to Oslo to conduct the interview in person. All interviews were recorded and transcribed within 48 hours after the interview found place.

The analysis is a result of the empirical evidence gathered and found during a period of four months, from January 2018 until April 2018. I used NVivo to categorize the material retrieved, and this gave me an overview of a great deal of different empirical evidence. It is highly likely that my personal and professional background have affected the interpretations made in the

analysis. A consequence of this is that the subjectivity of the thesis is relatively high, and this might undermine the reliability of the project. It is not guaranteed that a later investigator would derive the same conclusions based on the findings presented in the analysis. However, subjectivity is a common challenge when doing qualitative research. To meet this challenge the thesis follows the path of deduction and my interpretations will be legitimized by the theoretical framework presented in the previous chapter. As Singer (1961, p. 88) already has pointed out; “who is to say that empirical observation [...] is any better than informed deduction [...]?”.

To sum up, the thesis is a qualitative case study with one crucial case within the field of security and defense policy. This poses both methodological and empirical challenges, hence it is necessary for the reader to be critical of the findings in this thesis. However, by having a clear research design and a comprehensive theoretical framework that legitimizes the findings, the results presented below do have a value. The next chapters present the analysis of the empirical material in relation to previous research and already stated theory, before ending with a discussion of the findings presented in the analysis.

4 The Case of Cyber Defense

As presented in the chapter above, the case selected for this thesis is the case of cyber defense within the NORDEFECO framework. Cyber defense is a relatively new branch within the defense sector, but it is increasingly making its way into policy and strategy conversations (Norsk utenrikspolitisk institutt NUPI, 2018). As a result, the policy field of cyber defense is evolving, and it is evident that various countries have different ways of handling challenges posed by the cyber space. In addition to national initiatives on cyber defense, several international organizations are working on establishing a common cyber defense policy across state borders (Justisdepartementet, 2017, p. 29). Despite the efforts of several international organizations, such as the EU and NATO, the Nordic states have also established a regional cooperation on cyber defense within the NORDEFECO framework (Norwegian Armed Forces, 2011). The first section of this chapter elaborates on the academic relevance of cyber defense as a case and introduces central terms relevant when studying such a case.

4.1 Cyber Security and the Concept of Cyber Defense

There is not much research done within the field of political science and international relations on the case of cyber defense. Cyber security is a relatively new topic within political science in need for further research focusing on the political aspect of the phenomenon. Nevertheless, there is some academic research conducted in the field, some of which will be presented in this section.

First, cyber security is a concept requiring further elaboration and limitation in order to use it in a valuable manner. A broad definition of cyber security is “a property of cyberspace to be able to resist intentional and unintentional unwanted incidents – to respond and recover to avoid death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment” (Johnsen, 2015). According to this definition, cyber security is comprehensive because the society today increasingly relies on digital solutions, creating a strong dependence to the cyber space. Also, the second relevant factor for this definition is the highlighting of the severity of digital threats. Cyber space can be perceived as a different ‘room’ than the ‘real’ world, but what happens in cyber space has the capacity to cause great damage to the ‘real’ world. The fact that the lack of cyber security can lead to severe damages enforces the need of a strong and resilient cyber defense. Since the concept of cyber security is complex,

this thesis is limited to the military aspect of the term, more specifically the concept of cyber defense.

Despite the fact that cyber defense is a relatively new concept, there are some relevant published works to be aware of. First, cyber defense is in this thesis defined as a state's initiatives to defend itself from cyber-attacks or cyber intrusions, in order to protect its citizens and territory. Even though the concept is closely interlinked with cyber offense, it is important to be aware of the distinction between defense and offense studies. While defense studies tend to focus on initiatives made to defend a state or a region, offense studies focus on explaining offensive operations. In other words, defense studies aim at explaining what states do to protect its citizens and territory. Offense studies, on the other hand, aim at explaining what states do to conduct operations with the aim to harm other actors or take over territory. Previous research has argued that cyber space has favored the offense side. Meaning that it is easier to conduct offensive operations such as cyber-attacks and cyber intrusions, than to develop defense capabilities defending cyber space from such attacks and intrusions. However, recent scholars suggest that cyber space favors the defense side, indicating that it might be easier to build a strong and resilient cyber defense than to develop cyber 'weapons' (Slayton, 2017). This thesis meets the debate of the cyber offence-defense balance by contributing to the less developed research topic of cyber defense.

A central challenge when studying cyber defense is how to balance the positive and negative force of machines. Making it possible to take advantage of the benefits with digital solutions, at the same time as limiting the negative consequences of the dependence created by the same phenomenon. To gain a better understanding of cyber defense as a concept, it is need for an introduction to the historical development of machines. After all technology and machines are not new wonders, as Thomas Rid (2016) importantly reminds us of. Turning to history, machines and technological solutions have for a long time been viewed as magic and a myth, but in the 1940s machines became reality and cybernetics became science. Machines have throughout its existence been a helpful tool. At the same time it has brought new challenges to the fore: "The machines were always a positive and negative force at the same time, utopian and dystopian at once, although most of the time optimism dominated" (Rid, 2016, p. 348).

The optimism of machines has resulted in a second industrial revolution driven by technological solutions. However, one should be wary of this optimism as history has shown that the rise of machines has encountered various set-backs. One of these set-backs can be explained by the process where machines has created a new and distinct 'room', parallel to 'room' of the 'real' world, without a system regulating the behavior of the actors. In other words, the digital domain is a domain without policies and established rules (Buchanan, 2016). Since the Second World War, governments and militaries have a history of dominating the use of computers. This is changing, and recently citizens and non-state actors challenge the dominance of governments, increasing the need for a regulated digital domain. One central threat causing tensions around the world, both for governments and their military, and for citizens and non-state actors, is the relatively new threat of hacking (Rid, 2016). The exploitation of the lack of regulations and rules, such as hacking, have introduced the term cyber warfare.

To understand cyber warfare one must understand how cyber warfare is linked to hybrid warfare. Also it is crucial to understand that the cyber threat is a part of the broader concept of hybrid threat, with hacking as one unconventional mean used to pursue a larger objective. The possibility of cyber warfare is one of the negative forces with the rise of the machines causing a widespread fear of cyber-attacks and other cyber intrusions. Cyber warfare is in this thesis defined as the use of technology to harm other states or organizations by attacking them on the cyber domain or intrude in foreign networks. Hence, cyber-attacks and cyber intrusions are two central means in cyber warfare. Further, cyber warfare should be linked to the existing literature on the development of hybrid warfare, consisting of hybrid threats. Hybrid warfare is a warfare blending conventional and unconventional tactics, a result of the emerging fusion of war forms blurring the lines between regular and irregular warfare. Hybrid warfare opens up for the use of various unconventional weapons such as nuclear weapons or hacking (Hoffman, 2007). Consequently, hybrid threats can be defined as "those posed by adversaries with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives" (European Parliament, 2015, p. 1). Since cyber warfare is a new type of warfare, more research on cyber defense is needed in the studies of politics and international relations.

The increased fear of the severe consequences of cyber intrusions and cyber-attacks has resulted in an urgent need for a strong and resilient cyber defense for the states in the Western part of the world. To meet the need for a strong and resilient cyber defense, the Nordic states are now

working together developing cyber defense capabilities. Ethics, norms, and the ways of dealing with the critical issues of cyber security are questions which need to be agreed upon in a cooperation between institutions, militaries, states and international organizations. On the political level there is a desire to move towards concrete and practical cyber cooperation (Rantapelkonen & Salminen, 2013). By combining the case of cyber defense with the study of NORDEFECO as a regional cooperation, this thesis fills a gap in the literature on how states adapt to new and rising challenges such as ensuring a safe and open cyber space.

4.2 The Cyber Threat in the Nordic Region

The digital revolution is changing the society to a substantial extent and technological wonders are constantly introduced to citizens, private companies, and politicians. This dependence makes relevant actors extremely vulnerable for potential cyber intrusions, and highlights the great weakness of the digital revolution (Rid, 2016). Artificial intelligence is one result of the digital revolution, and its fast development is both impressive and frightening at the same time. The reason why the development to some extent is frightening, is somewhat the same reason as why cyber intrusions are a major threat; there is no established system to control or govern the cyber space (NRK Nyheter og politikk, 2018). In other words, the technological development has enhanced faster than the political development, and today the consequences of this is disclosed by people, organizations or states taking advantage of the lack of control in the cyber space. One of the most recent examples is the Facebook case, and how much influence metadata has on important events in the real world (Adams, 2018). Cambridge Analytica, the company buying personal information from Facebook, managed to misuse their access to personal information and provided a new tool in democratic election campaigns. Allegedly, both Donald Trump in the US presidential election of 2017 and the Leave side in the EU Referendum in 2016 used this tool to influence voters (Rosenberg, Confessore, & Cadwalladr, 2018; Scott, 2018). In addition, the Facebook case illustrates how much power private actors have in the world today, and that the liberal democracy is threatened by this shift (Hewson & Sinclair, 1999). Consequently, the digital revolution has resulted in an instant need for a strong and resilient cyber defense, enabling states to protect its territory and its people from actors abusing the vulnerabilities caused by a less regulated cyber space.

Since the Nordic region is one of the most digital advanced regions in the world, the fear of intrusion in cyber space is high. Also, the Nordic states and its citizens are highly dependent on

digital solutions, which indicate that potential cyber-attacks or intrusions can cause a great deal of harm to the region and/or its citizens (Turvallisuuskomitea, 2013). Based on this it is evident that the states in the Nordic region have strong incentives for developing cyber defense capabilities. In addition, the threat of cyber-attacks has proven to be a real risk for several of the Nordic states. According to FireEye⁴, Sweden, Finland, Denmark and Norway have been victims of cyber espionage, and foreign hacker groups are now targeting the Nordic military (Norsk utenrikspolitisk institutt NUPI, 2018). The extensive cyber-attack forcing the shutdown of the Swedish Defense Forces' Caxcis IT System is one example of foreign hacker groups targeting and influencing the Nordic military (Defense News, 2017). This clearly illustrates the real life consequences of cyber intrusions. As a country valuing their neutrality as a non-member of NATO, Sweden is now increasing their budgetary funding to strengthen its cyber defense capabilities, prioritizing cooperation with like-minded countries in the Nordic region, the EU and other global partners, such as NATO (Justisdepartementet, 2017, p. 31). This strongly suggests that one single state cannot deal with the cyber threat alone and supports the predictions of security regionalism. Regional cooperation on security policy is needed as the ensuring of one nation states' security cannot realistically be considered separate from other states (Buzan, 1991).

The example listed above highlights the major threat for the Nordic region within cyber security, namely cyber espionage. Cyber espionage can be used to gather information from various sectors and in the Nordic region the political, military and industrial sectors are especially vulnerable. Relevant for this thesis is military espionage where intruders are looking for strategic documents, such as plans for military exercises. Intruders are often looking for highly classified documents, and by getting access to such competing actors can be one step ahead in their strategic military planning (Norsk utenrikspolitisk institutt NUPI, 2018). Although information-sharing is an important element to build trust, it is also a threat if the information is shared with the wrong actors (Buchanan, 2016). If sensitive information land in the hands of wrong people or actors, it can weaken the position of an actor or cause great damage to a project or a region. One example is the Russian annexation of Crimea in 2014. It has been argued that Russia strategically used cyber intrusions to destabilize Ukraine as a country and 'shape the battlefield', before troops were sent in (Institute of International

⁴ FireEye is a private company based in the USA, focusing on hands-on and front-line expertise and intelligence in order to protect their customers from the impact and consequences of cyber-attacks (FireEye Inc., 2018).

Relations Prague, 2017). It is highly unlikely that a Russian annexation will happen in the Nordic region, but the example illustrates the strategy Russia allegedly uses, and how one country with long history of strategic espionage has managed to transfer their expert knowledge of espionage to the new digital arena. Even though a Russian annexation of the Nordic region is unlikely, one should not underestimate the power of cyber ‘weapons’, and the fatal consequences potential cyber-attacks might have for a region.

4.3 Nordic Response to the Cyber Threat

The recently published national cyber security strategies of the Nordic states are results of the increased severity of the cyber threat. These strategies explain cyber security and why it is essential with more focus on strengthening this in the years to come. All countries acknowledge the fact that international cooperation is essential in order to meet the challenges ensuring a safe cyber space. Nordic, European and global cooperation are essential for all countries, as a result of the global aspect of the cyber space. The four cyber security strategies are somewhat similar in the sense that all strategies highlight Nordic cooperation as a complementary effort to the initiatives by the EU and NATO. Further, it is evident that all countries will prioritize Nordic cooperation (Forsvarsministeriet, 2014; Justis- og beredskapsdepartementet, 2017; Justisdepartementet, 2017; Turvallisuuskomitea, 2013). To illustrate, the Swedish cyber security strategy states that “[c]ooperation on the conditions in Sweden’s neighborhood has a particular priority, for example within the framework of the Swedish-Finish, the Nordic and the Nordic-Baltic cooperation”⁵ (Justisdepartementet, 2017, p. 30, my translation). The findings from these strategies verify the statement that globalization has made the world more interdependent than ever before, also in the defense sector, and the use of global governance theory is therefore needed in order to understand this development.

Even though the national cyber security strategies are similar, there are also some differences among the Nordic states. Finland is standing out as the state with highest ambitions for the development of their national cyber security. While all strategies state that developing cyber security and cyber defense is a priority, the Finish strategy presents the aim of making Finland a leading nation in this area (Turvallisuuskomitea, 2013). Hence, indicating that Finland is the most motivated state, and this can explain why Finland took the lead role in the initiative phase

⁵ Original phrase: “Samarbeten kring förutsättningarna i Sveriges närområde har särskild prioritet, t.ex. inom ramen för det svensk-finska, det nordiska och det nordisk-baltiska samarbetet” (Justisdepartementet, 2017).

of a cooperation on cyber defense within the NORDEFECO-framework (Swedish Armed Forces, 2012). When being aware of the Russian threat on the digital sphere, this high motivation for a secure cyber space might not come as a surprise. As I will come back to in chapter six, Finland has complex historical ties with Russia, in addition to being the Nordic state with the longest frontier towards Russian territory.

4.4 Cyber Defense within NORDEFECO

In the NORDEFECO-structure, cyber defense is relevant at all levels, from highest with the Ministers of Defense all the way down to the lowest with different Cooperation Areas (COPAs)⁶. Despite the relevance for the whole system, cyber defense is mostly dealt with at the lowest level (Norwegian bureaucrat, 2018). However, the chiefs of defense have acknowledged that NORDEFECO also cooperate on cyber defense capabilities, which means that it has officially made its way up to the level of Military Coordination Committee (MCC-level) (Norwegian Lieutenant Colonel, 2018). Below, figure 4.1 illustrate the NORDEFECO-structure (Finnish Ministry of Defence, 2018, p. 4):

⁶ The COPAs ensure the allocation of resources from the national organizations to activities within NORDEFECO, and they serve as a bridge between the MCC-structure and the national chains of command (Norwegian Armed Forces, 2011).

NORDEFECO Structure

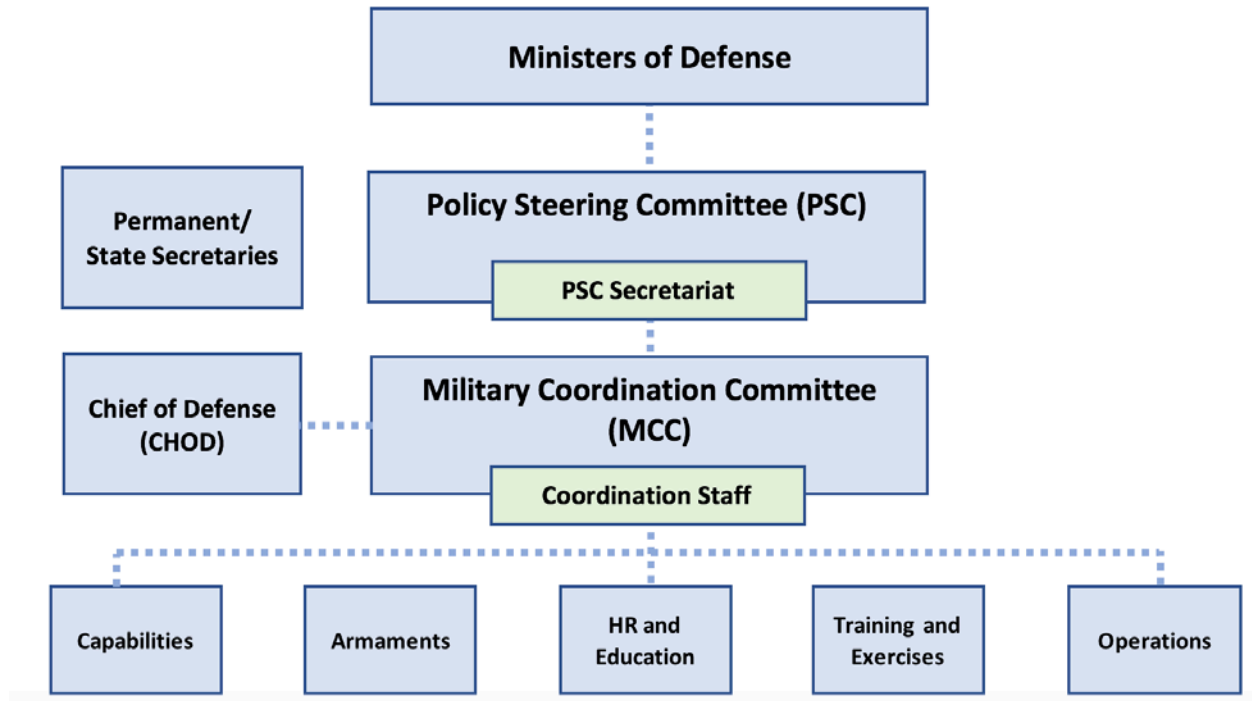


Figure 4.1 The NORDEFECO-structure.

To initiate a study is the normal starting point for any cooperation within the NORDEFECO-framework. The process of developing an idea to an activity or exercise, as illustrated by figure 4.2, starts with a study that is being developed into a project, and in the end it is implemented as an activity (Norwegian Armed Forces, 2011, p. 9). The first mentioning of cyber defense in relation to NORDEFECO was in the NORDEFECO Annual Report of 2011 where it is stated that the “[t]he MCC has decided that the study for 2012 will be on ‘Cyber defense in Nordic countries and challenges for cyber security’. This study will be led by Finland” (Swedish Armed Forces, 2012, p. 16).

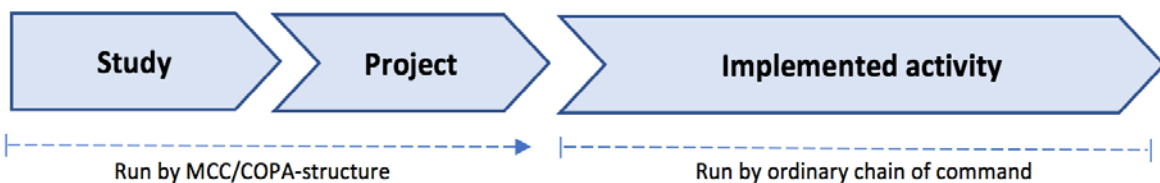


Figure 4.2 Process from study to activity in NORDEFECO.

After the first mentioning of cyber defense in 2011, it has been referred to in all the succeeding reports (Danish Ministry of Defence, 2017; Defence Command Denmark, 2013; Defense

Command Finland, 2014; Finnish Ministry of Defence, 2018; The Ministry of Defence Sweden, 2016; The Norwegian Ministry of Defence, 2015). In 2013 cyber defense was for the first time mentioned under one of the COPAs indicating that the study had turned into a project (Defense Command Finland, 2014). Now, cyber defense is formally under what is called COPA Capabilities (CAPA), which is the division focusing on addressing the Nordic states' development plans, in addition to identifying areas of capability cooperation (Danish Ministry of Defence, 2017). Further in this thesis, when referring to NORDEFECO's work on cyber defense, I will refer to the capability sector in general instead of only the COPA CAPA section. This, because cyber defense is not only relevant for the COPA CAPA section, but also relevant for the whole NORDEFECO-structure as previously mentioned.

Further, it is worth disclosing that cyber defense experienced increased focus in NORDEFECO after the Russian annexation of Crimea in 2014. In 2015 cyber defense was mentioned as one of the focus areas within the Nordic-Baltic cooperation (The Ministry of Defence Sweden, 2016; The Norwegian Ministry of Defence, 2015). The cooperation among NORDEFECO and the Baltic countries Latvia, Lithuania and Estonia have increased over the years focusing on certain areas of cooperation at both political and military level. One result of this cooperation is a joint Nordic-Baltic Statement highlighting "improved situational awareness, exercises, increased cooperation within the area of cyber defense, international operations and capacity building, as well as armaments and centers of excellence and other hubs of knowledge" (The Ministry of Defence Sweden, 2016, p. 22). The inclusion of the Baltic states supports the argumentation favoring larger forums, and highlights the fact that the institutional development is constantly changing (Checkel, 2005; Kellow, 2012). Also, since the Baltic region is geographically close to the Nordic region, this strengthens the argument that geography is essential in any regional cooperation (Mansfield & Solingen, 2010; Rosenau, 1995).

In short, this chapter has elaborated on the severity of cyber threats, and how cyber intrusions can lead to damaging consequences for a state or a region. Some of the Nordic states have been victims of cyber intrusions, as illustrated by the Swedish example. As a response to the severity of cyber intrusions, and the grand effects of cyber-attacks, all Nordic states have increased its focus on cyber security. It is now a common interest in the Nordic region for developing a strong and resilient cyber defense. NORDEFECO is one actor working with developing cyber defense capabilities, and it is a regional cooperation limited in members and to certain issues,

as illustrated by figure 4.1. The next chapter elaborates on NORDEFCO as a regional cooperation in a globalized world with other central organizations and systems, also working with developing cyber defense capabilities.

5 Regional Cooperation in a Globalized World

One central part of the analysis is how NORDEFECO illustrates an example of a closer regional cooperation in a globalized world, as a result of the challenge with keeping its territory and citizens safe from foreign threats. Regionalism is a highly relevant concept in order to understand the world we live in today, as mentioned in chapter two. Even though the world is becoming increasingly globalized, this does not necessarily indicate that regional cooperation is less common. In fact, regional cooperation might become even more important in the globalization process, as states realize that they cannot deal with today's security issues alone. Thus, the globalization process also affects the development of security and defense policy leading to the need of more regional cooperation. One area within security and defense policy dependent on regional cooperation is the area of cyber defense. As confirmed by a Finnish bureaucrat (2018) "first of all cyber is not, and cyber threats are not limited to only one nation. So due to the nature of cyber threats, cyber security requires cooperation of different actors, not only nationally but also internationally". Hence, security regionalism is a relevant concept, indicating that the nation state alone cannot guarantee the security of its territory and its citizens. This leads to various nation states' desire and need for closer regional cooperation in order to safeguard itself (Buzan, 1991). The following chapter focuses on explaining the complexity with globalization by analyzing the initiatives by the multilateral cooperation in the EU and NATO, and discloses where NORDEFECO fits in as a complementary regional forum for the Nordic states.

Continuing, the chapter seeks to address the question whether the development of a regional cooperation on cyber defense within NORDEFECO indicates that the Nordic states are not fully satisfied with the development on cyber defense within the EU and NATO. In other words, it seems NATO and the EU are not meeting the Nordic states' urgent need for a strong and resilient cyber defense. Consequently, my assumption is that the Nordic states would not have focused on cyber defense within NORDEFECO had they been satisfied with the development in NATO and the EU. This assumption was confirmed by a national representative, commenting on the motivation for a deeper Nordic cooperation on cyber defense: "It is difficult to cooperate on [cyber defense]. So, in a way, the fact that we are struggling to get started with a cooperation

in NATO and the EU is an additional motivation”⁷ (Norwegian Lieutenant Colonel, 2018, my translation). This phrase leads me to investigate the initiatives of the EU and NATO on cyber defense, and how NORDEFECO complements the process in these two larger systems/organizations. Based on the argumentation above, Nordic cooperation on cyber defense is perceived as a result of lacking achievements from larger multinational cooperation.

5.1 Cyber Defense in the EU and NATO

Even though the focus of the thesis is on the regional cooperation among the Nordic states, one must not forget that international organizations and systems also work intensively with the development of an international framework on cyber defense. By including more of a global perspective to the development of a common cyber defense, the understanding of NORDEFECO and its room to maneuver increases. Since the world today is heavily globalized it is not possible to explain regional cooperation without including the broader global context (Checkel, 2005). The cyber threat is a global threat and it is therefore not surprising that cyber defense is high on the agenda in several international organizations and systems.

The Nordic states are embedded in multiple international contexts and NORDEFECO must maneuver within these constraints. This explains why the aim of NORDEFECO is to complement the work of NATO and the EU and not to compete with it. NORDEFECO’s room to maneuver when it comes to developing cyber defense capabilities is limited by the states’ existing membership in other international organizations and institutions. In addition to the regional cooperation NORDEFECO, the EU and NATO are two central systems/organizations also working with cyber defense. They are relevant to include because the EU represents a larger European cooperation, while NATO represents the Western tradition for security policy since the end of the Second World War. In addition, the Nordic states are members of at least one of these two organizations, indicating that the Nordic states also work with developing closer cooperation on cyber defense at the global level. The memorandum of understanding of NORDEFECO signed by the Nordic states acknowledge “any obligation that may follow from the Participants’ membership in the European Union (EU) and/or the North Atlantic Treaty

⁷ Original phrase: «Fordi dette er veldig vanskelig å samarbeide om. Så det er på en måte en tilleggs motivasjon da, at vi ser at vi sliter med å komme i gang med samarbeid i NATO og EU på dette området» (Norwegian Lieutenant Colonel, 2018).

Organization (NATO)” (The Ministry of Defence of the Kingdom of Denmark et al., 2009). This strengthens the theoretical prediction that global governance is complex and that states entering new institutional arenas are not free agents (Checkel, 2005). To understand how membership in the EU and/or NATO limits or compliments the work done in NORDEFECO, there is a need for a general review of what the EU and NATO are performing on cyber defense.

For the EU to be able to fulfill its objective of a Digital Single Market, it is crucial that the Union has a strong and resilient cyber defense (European Commission, 2013). The EU is known for its expertise in pooling and sharing, and it is to a large extent also becoming an actor of its own in the international sphere, representing its 28, soon to be 27, member states. The EU’s Global Strategy of 2016 has increased the Union’s focus on a common foreign policy, with more of a transformative agenda (Sjursen, 2017, pp. 451-455). The Global Strategy, similar to global governance theory, is complex and includes various important areas for the development of the EU as a global actor. One central area is the development of a common security and defense policy in order to protect the EU and its citizens (The European Union, 2018). Because of the increased threat of cyber-attacks and other cyber intrusions, the development of a common European cyber defense is high on the agenda in the EU, as a new branch within the defense sector.

Despite the fact that the EU has a less developed defense sector, one of the top priorities when it comes to cyber security is to establish common cyber defense policy and capabilities. The EU has a cyber security strategy, similar to that of the Nordic states, addressing the challenges and vulnerabilities that follows the development of cyber space. The strategy “outlines the EU’s vision in this domain, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU’s online environment the safest in the world” (European Commission & High Representative of the European Union for Foreign Affairs and Security Policy, 2013, p. 3) A common European cyber defense will be developed by an EU-organization with the name Common Security and Defense Policy (CSDP) (European Commission & High Representative of the European Union for Foreign Affairs and Security Policy, 2013, p. 5). How this should be conducted is however unclear at the time of writing this thesis. Albeit, one concrete result of the increased focus on cyber security in the EU is the Directive on Security of Network and Information Systems (the NIS Directive), that is also to be implemented in the EEA Agreement (EØS-notat, 2016).

Cyber threats are today challenging the development of the single market and therefore the EU experiences the necessity of common European rules regarding ICT-security. In July 2016 the EU member states agreed on the NIS directive with the aim to tackle hybrid threats, and it will be integrated into domestic legislation in May 2018. This directive is a result of the strategy launched by the EU Commission on cyber security called *An Open and Secure Cyberspace*. The directive has three main motives; 1) to better the conditions of competition in a globalized world, 2) contribute to economic growth in Europe, and 3) create trust to digital solutions (EØS-notat, 2016). According to this, the NIS directive is a reactive action strengthening the argument that the mechanism of 'bare survival' is indeed relevant in contemporary global governance (Rosenau, 1995). Continuing, it highlights the challenge brought forward by Rid (2016) about the digital revolution and the lack of policies securing the digital system, making the users question the security of such solutions. This indicates that Europe is in need of common rules in order to increase the level of trust to digital solutions, among its citizens.

The initiatives on developing a strong and resilient cyber defense in the EU cannot be viewed separate from the similar initiatives made in NATO. Earlier it was easy to understand the difference between the EU and NATO. However, now partly because of the challenges with cyber security these two systems are becoming more interlinked. In addition to the increased focus on cyber defense in the EU, NATO is also working on establishing a strong and resilient cyber defense. The EU is aware of the work NATO is doing on cyber defense, and in order to avoid duplication, the EU strategy states that the Union should "explore possibilities on how the EU and NATO can complement their efforts to heighten the resilience of critical governmental defense, and other information infrastructures on which the members of both organizations depend" (European Commission & High Representative of the European Union for Foreign Affairs and Security Policy, 2013, p. 11). NATO has acknowledged this cooperation and after a meeting between the two parts in December 2017, it was clear that "cyber defense is one of the areas where NATO and the EU are working closer together than ever" (North Atlantic Treaty Organization, 2017a). This highlights the complexity with global governance and proves that the lines between central actors in the global arena are becoming blurred (Saurugger, 2014). The two systems/organizations have to closely cooperate in order to build a strong and resilient cyber defense. This is a good example of the complexity with global

governance and that international institutions are required to always change and adapt to the surrounding conditions (Keohane, 1998; Wendt, 1999).

The most relevant aspect of NATO for this thesis is the so-called smart defense, that “is a cooperative way of thinking about generating modern defense capabilities that the Alliance needs for the future. [...] That means harmonizing requirements, pooling and sharing capabilities, setting priorities and coordinating efforts better” (North Atlantic Treaty Organization, 2017b). Cyber defense is part of NATO’s core task of collective defense, and the organization has affirmed that international law applies in cyber space in the same manner as it applies in the ‘real’ world. The main focus of NATO, at least in the public, is to protect its own networks indicating that building a strong cyber defense has priority, not building a ‘cyber army’ (North Atlantic Treaty Organization, 2018). Again this is an example of a reactive action, where the mechanism of ‘bare survival’ is present by responding to the increased cyber threat by developing defense capabilities (Rosenau, 1995). Projects under the umbrella of NATO’s smart defense cover a wide range of efforts and address the most critical capability requirements, including cyber defense capabilities. NORDEFCO is known for being smart defense in practice, indicating that the institutional development of NATO’s smart defense has succeeded and its importance has increased and is now being implemented in other intergovernmental cooperation (Keohane, 1998; National representative, 2018). Thus, regional cooperation draw advantages of already established strategies in larger international institutions.

Since all the Nordic states are well integrated in both the EU and/or NATO, who both work intensively with developing a common cyber defense policy, the parallel development of the same policy area within NORDEFCO is a puzzle. As mentioned above, the Nordic countries are linked to at least one of the two larger forums for cooperation. As small countries in a globalized world, these memberships are important for the states because it gives them increased influence in the world order (Kellow, 2012). For Norway and Denmark, NATO has been the main actor for security and defense policy, while the EU is perhaps becoming the main partner for Finland and Sweden. This is illustrated by statements from the informants in this project. The Norwegian Senior Staff Officer (2018, my translation) said that “regarding good

cooperation it is of course the Alliance. And it is with the Alliance we [Norway] have our primary focus”⁸. Further the Finnish bureaucrat (2018) stated that:

[W]hen Finland joined the EU in the 90s, that was very much a political sign that we are part of West. [...] Finland wanting to be part of a security arrangement, which the EU is. Not necessarily that strong on the defense side, but in general, in broad meaning, the EU is also a security arrangement, not only an economical arrangement, but also a security arrangement for Finland.

Despite membership in the EU, Denmark is not a member of the EU’s defense policy because of an opt-out (Danish Ministry of Defence, 2018). Norway on the other hand is not a member of the EU, but has several agreements with the Union on security and defense policy, such as contributing with military and civilian forces and participating in international operations led by the EU (NOU 2012:2, 2012, p. 724). Thus, one can argue that Norway is more closely linked to EU’s security and defense policy than what is the case with Denmark. Sweden and Finland as the two other Nordic states are EU members and are actively taking part in the development of a common European defense policy. Also, Sweden and Finland are close partners with NATO, making NATO a relevant organization for the non-NATO members as well (Wivel & Marcussen, 2015).

5.2 Defense Cooperation within NORDEFECO

Despite the initiatives by the EU and NATO, the Nordic states are seeking closer Nordic cooperation on cyber defense, where they also want to include the Baltic states in a somewhat larger regional cooperation. According to NORDEFECO, the initiatives taken within this framework is not competing initiatives to that within NATO and the EU. Rather cooperation in NORDEFECO aim at strengthening NATO’s smart defense and EU’s pooling and sharing (Swedish Armed Forces, 2012). A national representative to NORDEFECO put it this way:

Based on my understanding of NATO’s smart defense, and pooling and sharing, one could say that NORDEFECO itself is a practical example of smart defense and pooling

⁸ Original phrase: «Altså når det gjelder godt samarbeid så er det selvfølgelig alliansen. Og det er jo der vi har primærfokuset vårt» (Norwegian Senior Staff Officer, 2018).

and sharing. There are in no way, any competing, or any misunderstandings on this issue⁹ (National representative, 2018, my translation).

Based on this statement it is evident that the cooperation in NORDEFECO in fact seeks to strengthen the work of NATO and the EU. By providing a practical example of NATO's smart defense and EU's pooling and sharing, NORDEFECO can be perceived as a solution to the issues with turning policies on cyber defense into concrete results and implementation. NORDEFECO is working with practical cooperation activities, and by completing different activities they learn what is successful and where the potential for improvement lies. When it comes to cyber defense, NORDEFECO is testing out a strategy with low ambitions and gradual habituation (Norwegian Lieutenant Colonel, 2018). This is in line with the theory of socialization and learning (Saurugger, 2014).

The Nordic states are easily satisfied when it comes to cooperation within the area of defense policy. Also, one hopes that small successes will result in grand effects (Norwegian Lieutenant Colonel, 2018). There are two central reasons to why the ambitions for a common Nordic cyber defense is low, and why the EU and NATO is struggling with developing practical examples of joint cyber defense capabilities. First, one obstacle is that the information in this area is highly classified, and states most often want to avoid sharing confidential information with one another. Second, it is difficult to discuss cyber defense without disclosing sensitive information, which requires some sort of confidentiality and a level of trust to the one receiving such sensitive information (Norwegian Lieutenant Colonel, 2018). Nobody wants to talk about their vulnerabilities, in fear of other actors exploiting these weaknesses. In addition, sharing sensitive information requires that the participating actors trust each other sufficiently to be comfortable with disclosing confidential information. This confirms the theoretical prediction that states often are hesitant to intergovernmental cooperation on defense policy (Buchanan, 2016). I will come back to the issue of trust in the next section.

Despite the low ambitions for common Nordic cyber defense capabilities, the Nordic states have managed to start some sort of cooperation within the field, giving them first-hand

⁹ The original phrase: «Sånn som jeg ser for meg NATOs smart defense, og pooling og sharing, så er NORDEFECO i seg selv et eksempel på smart defense og pooling and sharing. Det er på ingen måte noen konkurrerende eller noe misforståelser mellom dette her» (National representative, 2018).

knowledge of how such a cooperation could be developed functionally. According to the informants working in the Norwegian Ministry of Defense, intergovernmental cooperation on cyber defense should start with procuring individuals from various states to cooperate. One must start from the bottom and build personal relations and individual cooperation before one can take it to a more institutional level. The NORDEFECO strategy is based on this thought, and they are now working with establishing interpersonal relations so that such relations can make the implementation of certain policies and activities easier at a later stage. As a result of certain initiatives, NORDEFECO has succeeded in getting people from various Nordic countries to sit together and make common activities on the topic of cyber defense. This might seem like a simple task, but it is also a success because it creates relations among Nordic individuals based on good will and positive attitudes towards cooperation (Norwegian Lieutenant Colonel, 2018). Based on this information, institutional development at the macro-level requires initiatives at the micro-level where individuals are central. Thus, making personal experience the first building block for the development of common Nordic cyber defense capabilities. This highlights the importance of constructivism as an ontological approach where both the micro- and macro-level are central in understanding the institutional development of NORDEFECO (Wendt, 1999).

To understand the institutional development of the connection between the micro- and macro-level, it is important to understand how good interpersonal relations are established and developed. In order to establish good personal relations, as the foundation of a larger institutional cooperation, culture and geography are two central elements. Cultural equality and geographical proximity makes the development of good personal relations feasible which again facilitates institutional cooperation. Hence, culture and location are important elements when establishing and developing a regional forum dealing with defense cooperation. The fact that the Nordic states have a fairly similar culture and are located right next to each other, makes Nordic cooperation on cyber defense feasible and realistic (Norwegian Lieutenant Colonel, 2018). As of now, the Nordic states have accomplished some results illustrating a common approach to the development of cyber defense capabilities. One practical example of an activity of closer Nordic cooperation on cyber defense within the NORDEFECO-framework is the development of national Computer Emergency Response Teams, led by Finland, aiming at improving Nordic defense against cyber-attacks (The Norwegian Ministry of Defence, 2015). Also, the Nordic states cooperate on education and research within the field of cyber defense

with the Cyber Defense Study, sponsored by Finland, as one concrete example (Rantapelkonen & Salminen, 2013; Swedish Armed Forces, 2012). To summarize, the institutional development of cyber security capabilities is dependent on initiatives on the micro-level with good interpersonal relations being essential for the further development of cooperation. The NORDEFECO strategy is based on this type of development, where smaller personal forums might lead to greater projects in the future (Kydd, 2000). As mentioned in chapter two, the focus of this thesis is not the micro-level, however, these findings introduce an interesting perspective for later research.

The Nordic states are not able to stand alone in the defense of cyber-attacks and cyber intrusions. By providing clear examples of initiatives and activities on intergovernmental cooperation on cyber defense, NORDEFECO represents a regional forum based on security regionalism. In line with the theory of security regionalism, it is evident that Nordic states have high interdependence when it comes to cyber security, and also holds a geographical proximity (Buzan, 1991). As stated by one of the informants, the Nordic states are “similar when it comes to culture and technology”¹⁰ (Norwegian Lieutenant Colonel, 2018, my translation). Later in the interview the Lieutenant-Colonel stated that one factor for cooperation is that “the possibility of being able to use land right next to us, [...] gives new opportunities, and this is mutual. So geography is a factor, definitively”¹¹ (Norwegian Lieutenant Colonel, 2018, my translation). These findings, in addition to the central challenge with how the national boundaries are blurred in cyber space, indicate that the best way to secure the region and its citizens is through intergovernmental cooperation. This was confirmed by the Norwegian Senior Staff Officer (2018, my translation):

Anyways, I do agree with you that international cooperation is crucial. [...] There are political dimensions with standing together too, but also a military operational dimension where one can cooperate in order to control parts of the cyber domain. This to prevent an intruder, or an aggressor so to speak, to get comfortable in that domain¹².

¹⁰ Original phrase: «vi er ganske like kulturelt og teknologisk» (Norwegian bureaucrat, 2018).

¹¹ Original phrase: «så kan du si at det å kunne bruke land som ligger ved siden av oss, som en del av..., det åpner nye muligheter, og det er gjensidig da. Så geografi er også en faktor, helt klart» (Norwegian bureaucrat, 2018).

¹² Original phrase: «Uansett, så er jeg derimot enig med deg at internasjonalt samarbeid vil være avgjørende. [...] Det er politiske dimensjoner ved å stå sammen og, men også en sånn militær operativ dimensjon der man kan samarbeide om å kontrollere deler av cyberdomenet. For å forhindre at en motstander, en aggressor da, kan ta seg til rette der» (Norwegian Senior Staff Officer, 2018).

This proves that international cooperation is wanted both from the political dimension and the military dimension because it will strengthen the defense capabilities of each state. This can explain why the Nordic states are seeking practical solutions within NORDEFECO as to how one can best build cyber defense capabilities.

When it comes to the development of cyber defense capabilities, it seems as the states prioritize having influence of the decisions being made, indicating that smaller forums are preferred. By highlighting relevant issues in the context of regional cooperation, such as culture and geography, it is evident that the NORDEFECO-structure is an example of both a rational cooperation, and a cooperation based on socialization and learning (Alter & Meunier, 2009; Bell, 2017; Checkel, 2005; Kellow, 2012; Saurugger, 2014). The results from Nordic cooperation, as presented above, is a good illustration of how both a common culture and geographic proximity facilitate intergovernmental cooperation, and this is where NATO and the EU differ from NORDEFECO. Both NATO and the EU are larger forums with various diverging cultures, in addition to covering large geographic areas. These factors make it difficult for the two organizations/systems to find common ground between its members on sensitive issues, such as cyber defense. As a consequence, it is comprehensible that the states in these large organizations are not comfortable with discussing their weaknesses and vulnerabilities. Based on the theory of forum shopping, the development of a common cyber defense in the EU, NATO and NORDEFECO is an example of a situation where smaller forums are preferred based on the achievements of NORDEFECO (Kellow, 2012). Additionally, the element of trust is evident when it comes to being comfortable with sharing relevant information required for such a cooperation. Hence, NORDEFECO might be the best forum to realize cyber defense capabilities needed to protect the territory and the citizens of the Nordic region.

This chapter illustrates how NORDEFECO can be understood as a practical example of NATO's smart defense and EU's pooling and sharing. Continuing to argue in favor of why a smaller Nordic region is preferred in cooperation on highly sensitive issues. The findings from this chapter leads me to conduct a more thorough analysis of relevant factors as to why NORDEFECO is to some extent succeeding in providing a practical example of NATO's smart defense and EU's pooling and sharing. Some central factors have been mentioned in this chapter, and these will be further elaborated on in the next chapter. By looking at the four central

variables presented in figure 3.2 , the next chapter should be perceived as a complementary chapter going in depth in explaining the motivation for why Nordic states are seeking closer institutional cooperation on cyber defense within the NORDEFECO-framework.

6 Central Factors Explaining Regional Cooperation on Cyber Defense within NORDEFECO

By focusing on the four independent variables of 1) geopolitics, 2) burden-sharing, 3) history of cooperation, and 4) trust, this chapter sheds light on the underlying motivations for why the Nordic states have chosen a Nordic forum in the development of common cyber defense capabilities. As argued above, a small regional forum such as NORDEFECO is to be preferred when states are required to cooperate on sensitive issues. However, what the preceding chapter does not elaborate on is the motivation for why the Nordic states have chosen a Nordic forum to deal with defense policy, and more precisely cyber defense capabilities.

6.1 Geopolitics

Geopolitics as an independent variable, based on the ontological approach of realism, introduces the importance of geography for members in a forum. Since NORDEFECO is a forum limited in membership based on geography, it is relevant to look closer at how their geographic positioning affects their initiatives on cyber defense. The Nordic states have the same geopolitical environment, and as stated by Forsberg (2013, p. 1175) “[g]eography is commonly seen as a reason why the Nordic countries should work together”. However, geography does not automatically lead to cooperation. In order for geopolitics to be a motivation for cooperation, it is essential that the potential members of a forum understand geography as a factor tying them together (Forsberg, 2013, p. 1178). Hence, it is necessary to disclose whether the Nordic states understand geography as a factor binding them together.

There are no empirical evidence indicating that geography was the most crucial factor in the first years of Nordic cooperation in NORDEFECO. From 2009 up until 2014 it is evident, based on the material analyzed for this thesis, that the most central factor for cooperation was cost-efficiency. However, a critical juncture in this development happened in 2014 when Russia aggressively invaded Ukraine leading to the annexation of Crimea. This event is perceived by the West as a result of the strengthening of Russian military capabilities, with the aim of restoring its status as a Great Power (Bukkvoll & Åtland, 2015). For the Nordic states this event was both frightening and provoking, making it necessary to explicitly show their support to the Western liberal democracy and international law. Russia violated international law by taking control over another state’s territory and by upholding the annexation it is evident that this was intentional, requiring a response from the international society (FN-Sambandet, 2017). As a

consequence of the Russian annexation of Crimea, the Nordic states were forced to reconsider their security policies and with it, also their relationship with Russia. Thus, leading to an increased importance of geopolitics as a factor tying the Nordic states closer together in NORDEFECO:

2014 has been an eventful year for Nordic defense cooperation. Russia's annexation of Crimea and its intervention in Eastern Ukraine have changed the European security landscape, with implications also in our own region, and we have discussed how we can adapt our defense policies to this new situation. The Nordic nations are reconsidering their security policies and their relationship with Russia (The Norwegian Ministry of Defence, 2015).

At the time of writing this thesis, the situation continues to be tense, and Russia's developments of espionage and intrusions in the cyber domain is understood as a real threat for the Nordic states:

It [e.g. cyber intrusions] is used to influence the population both through, let's call it, information operations, but also through coercive power, destruction, the loss of electricity and so on. We see that it [e.g. cyber intrusions] is being used in new ways following the development where it [IT infrastructure] plays a greater role and a more fundamental role in keeping the machinery of our society going¹³ (Norwegian Senior Staff Officer, 2018, my translation).

The informant also explicitly refers to the Russian annexation of Crimea as an example of the severe consequences of hybrid warfare, as cyber warfare tools was used to disturb the public authorities.

Swedish and Finnish participation in NORDEFECO is one example of a stronger alliance to the West. Russia's recent aggressive foreign policy in its neighboring countries have to some extent caused a shift forcing the more 'neutral' states of Finland and Sweden to show stronger support to the West. It can be argued that Finland and Sweden have undermined its neutrality since the end of the Cold War with Swedish and Finnish membership in the NATO program Partnership for Peace. Also EU memberships contribute to weaken the Swedish and Finnish neutrality

¹³ Original phrase: «Det brukes for å påvirke befolkningen både gjennom, kall det da, informasjonsoperasjoner men også gjennom tvangsmakt, ødeleggelse, bortfall av strøm også slike ting. Vi ser at det har fått en ny anvendelse i takt med at det har fått en større rolle og en fundamental rolle i å holde samfunnsmaskineriet i gang» (Norwegian Senior Staff Officer, 2018).

policy (Saxi, 2018, p. 91). One can then ask the question if Sweden and Finland ever were neutral? Compared to Norway and Denmark, I would suggest that Sweden and Finland are neutral to some extent based on their choice to remain outside the NATO alliance. In other words, Finland and Sweden are neutral in the sense that they do not have the same ties to the USA, as is the case with Norway and Denmark. This important element indicates that Nordic cooperation still is relevant and have an effect, and that NATO is not the best forum for promoting Swedish and Finnish security and defense interests. Nevertheless, one should not underestimate the alternative partnership Sweden and Finland have with NATO. It is evident that these two states are experiencing how important it is with partners and alliances in such turbulent times: “The core motivation for Finland’s defense cooperation is realizing that we as part of West, we are interdependent” (Finnish bureaucrat, 2018). Also, in the Swedish long term agreement on defense policy it says that “Sweden continues to building security together with its partners” (Swedish Ministry of Defence, 2015, p. 5). Based on these findings, there is reason to believe that aligning with the West is the priority of Sweden and Finland, despite potential negative reactions from Russia.

Another element strengthening the explanatory power of the geopolitical variable is the inclusion of some Baltic states in the Nordic cooperation on cyber defense. Efforts have been made to develop the Nordic-Baltic cooperation since the establishment of NORDEFECO. In later years, cyber defense has evolved as one of the key areas of cooperation among the Nordic states along with the Baltic states Estonia, Latvia and Lithuania (Danish Ministry of Defence, 2017; Defence Command Denmark, 2013; Defense Command Finland, 2014; Finnish Ministry of Defence, 2018; Norwegian Armed Forces, 2011; Swedish Armed Forces, 2012; The Ministry of Defence Sweden, 2016; The Norwegian Ministry of Defence, 2015). Even though the Nordic and the Baltic states are economically, historically and politically distinct, they have one thing in common, they all have Russia as a close neighbor. This finding strengthens the theoretical presumption that states strategically select forums with members holding the same interests and threats as themselves. Thus, it could be of similar interest for the Nordic and Baltic states to build a stronger and resilient cyber defense mainly because of the increased threat from Russia (Alter & Meunier, 2009). Following, it is evident that geography is relevant in regional cooperation supporting the definition of regionalism that requires geographic proximity (Mansfield & Solingen, 2010).

Despite these findings, I would not argue that geopolitics is the most dominant factor for Nordic defense cooperation based on its lack of focus in the first five years of its existence. Also, the digital revolution and globalization decreases the necessity of geographical proximity. The inclusion of the Baltic states can be explained by other factors as well, introducing the next variable for investigation, namely burden-sharing.

6.2 Burden-Sharing

When states decide to join forces to solve common issues and deal with shared challenges it is evident that some sort of burden-sharing is happening. The Nordic states are small states in a global context and it is therefore natural that they are aware of the benefits of intergovernmental cooperation: “Small countries, in particular, cannot afford not to cooperate” (Forsberg, 2013, p. 1174-1175). Also, as stated by one of the founding fathers of NORDEFECO Sverre Diesen (as quoted in Saxi, 2018, p. 92, my translation), NORDEFECO was the result of “the acceptance that small nations such as Norway [...] can no longer alone bear the increasingly growing costs of a complete military defense”¹⁴. Consequently, economically speaking it is indeed strength in numbers, and because of the growing costs of functioning and resilient defense capabilities, some sort of burden-sharing is a motivation for closer cooperation.

In economic terms, one central element of burden-sharing is cost-efficiency. Cost-efficiency has been the most central aspect of NORDEFECO ever since its establishment, and the aim has always been, and still is, to find cost-efficient solutions (Danish Ministry of Defence, 2017; Defence Command Denmark, 2013; Defense Command Finland, 2014; Finnish Ministry of Defence, 2018; Norwegian Armed Forces, 2011; Swedish Armed Forces, 2012; The Ministry of Defence Sweden, 2016; The Norwegian Ministry of Defence, 2015). The national defense departments always have to manage with restricted amount of resources, making it necessary to localize the most effective ways to use it. Furthermore, based on the information gathered from the interviews, it is evident that cost-efficiency is one of the main motivations for cooperation: “Of course, one of the motivations, if I go down my list which I wrote down, is cost-savings” (Finnish bureaucrat, 2018). Cost-efficiency is a relatively easy way of measuring

¹⁴ Original phrase: «å akseptere at små nasjoner som Norge [...] ikke lenger kan bære de strekt voksende kostnadene ved et komplett militært forsvar alene» (as quoted in Saxi, 2018, p. 92)

the benefits of a cooperation, and it is based on a rational reasoning making it difficult to question.

Based on economic theory, cost-efficiency is dependent on comparative advantage which can explain why the Nordic states are including the Baltic states in the cooperation on cyber defense (Røste, 2013). The Nordic region is one of the most digitalized regions in the world. In addition, Estonia is a forerunner when it comes to developing cyber defense capabilities, strengthening the argument of the importance for a region to employ its comparative advantage (Norsk utenrikspolitisk institutt NUPI, 2018). The Nordic states are becoming increasingly dependent on digital solutions and this dependence requires increased knowledge of the cyber space, introducing the power of knowledge:

So it is, just because we are so similar that one in theory can find something of interest to us. So to speak, we can [...] in the best case scenario, share heads. Competence is definitively an important factor in this case. It does not have to be like, let's say the submarine for example, but it is all the underlying factors that are relevant. So it is how we plan, how we develop all of this. Not necessarily the object so to speak, without us necessarily knowing what the object of cyber defense is. But if we say that it is a super computer or something similar, then we do not have to talk about that at all, but about everything else¹⁵ (Norwegian Lieutenant Colonel, 2018, my translation).

If you then, well in the example of the submarine there are not many possibilities for cooperation, but there are possibilities in the support-system, [...], in other words to produce everything you need to get the object to function well in a war. Then you need things such as logistics, education, training and everything else that support the capability. And this is perhaps 70-80% of the costs too. It is actually there the great effects lie¹⁶ (Norwegian Lieutenant Colonel, 2018, my translation).

¹⁵ Original phrase: «Så det er, nettopp fordi vi er så like så kan i teorien en finne som kan noe være interessant for oss. Altså, så vi kan i beste fall, i verste fall, i beste fall, dele hoder. Kompetanse er helt klart en viktig faktor her. Så det må ikke være sånn, ja kall det ubåten da, men det er alt det underliggende. Så det er hvordan vi planlegger, hvordan vi utvikler alt dette her. Ikke nødvendigvis denne tingen da, uten at vi nødvendigvis vet helt hva et cyberforsvars ting er. Men hvis vi sier at det er en sånn supercomputer eller noe sånt da, så trenger vi ikke nødvendigvis å snakke om det i det hele tatt, men om alt det andre» (Norwegian Lieutenant Colonel, 2018).

¹⁶ Original phrase: «Hvis du da, her er det kanskje ikke så mye å samarbeide om med selve ubåten, men det er i understøttelsen, altså det å styrke-produsere, altså det å produsere alt det du trenger for å få denne til å virke ordentlig i krig. så trenger du ting som logistikk, utdanning, trening og alt det andre som understøttet kapabiliteten.

These quotes strengthen the argument that burden-sharing is one of the most central motivations for cooperation on cyber defense within NORDEFECO. Also, it highlights how it is possible to cooperate on sensitive issues by focusing on the underlying issues, rather than the capability itself. It is evident that burden-sharing is not only about sharing the material costs, it is also about the sharing of knowledge and competence. When it comes to cyber defense, the sharing of competence is crucial because it is such a new phenomenon which requires more research and knowledge in order to develop well-functioning capabilities.

Not surprisingly the empirical evidence leads towards burden-sharing with cost-efficiency being the most important motivation for cooperation. Political decisions is less likely to be criticized if they have economic legitimation, illustrating the benefits of cooperation with numbers and concrete results. Nevertheless, it is not a given that NORDEFECO has resulted in cost-efficient solutions, even if it has been the most crucial motivation. The next section elaborates on the historical development of NORDEFECO by looking closer at the results of Nordic defense cooperation and whether it has resulted in cost-efficient solutions. In addition, an interesting aspect of the findings presented above is the importance of sharing of knowledge and information. This results in a fruitful discussion in the two following sections about the assumption stating it is not a given that states are positive to share knowledge and competence with other states.

6.3 History of Cooperation

To understand the present it is also necessary to understand the past. Today, closer Nordic defense cooperation might seem like an obvious development, however this has not always been the case. During the Cold War, the Nordic states had distinct security policies which have been described as the ‘Nordic balance’, resulting in any potential defense cooperation being highly unlikely. Norway and Denmark joined NATO in 1949, Sweden remained neutral, and Finland aimed at neutrality, but was restrained by close ties to the Soviet Union. These varying orientations made an open Nordic cooperation on security and defense policy unthinkable according to the previous Norwegian Defense Minister, Thorvald Stoltenberg (Saxi, 2018).

Og dette er jo kanskje 70-80% av kostnadene også. Det er der egentlig de store effektene ligger» (Norwegian Lieutenant Colonel, 2018).

Despite an unthinkable open Nordic defense cooperation, a parallel development of a Nordic cooperation on civil issues was in progress during the Cold War. As a result, in 1952 the Nordic states established the Nordic Council, an inter-parliamentary cooperation on areas not concerning security and defense policy. The Nordic states also had a close cooperation within the United Nations (UN), in addition to the development of a confidential operative military cooperation between the NATO-members Norway and Denmark and the 'neutral' Sweden. During the Cold War this cooperation was kept secret from the Soviet Union. When the Cold War ended, it became clear to the dissolving Soviet Union that Sweden and Finland would approach the West. Finland also made it clear to the Soviet Union that they no longer would uphold the Treaty of Friendship, Cooperation and Mutual Assistance, a treaty dating back to 1948. Thus, Finnish and Swedish partnership with NATO could now be out in the open without fear of the response from the newly established Russian Federation. Continuing, the Nordic states could at that time start the development of a Nordic cooperation on security and defense policy (Saxi, 2018). This led to the development of various Nordic forums within the security- and defense sector, and in 2009 these forums were comprised. More specifically, in 2009 the forums of NORDAC (Nordic Armaments Cooperation), NORDCAPS (Nordic Coordinated Agreement for Peace and Support) and NORDSUP (Nordic Supportive Defense Structures), turned into NORDEFECO (Wivel & Marcussen, 2015, p. 217).

Based on history, it is evident that the Nordic states have been eager to cooperate, also on security and defense policy, ever since the end of the Second World War. Albeit, it could not fully be realized until the end of the Cold War, with the fall of the Soviet Union. The findings above illustrate that despite distinct security policies, some Nordic states managed to find ways to cooperate already during the Cold War. Even though this cooperation had to be conducted in secrecy, it laid the foundation for closer cooperation after the end of the Cold War. In addition, the close ties between the Nordic states from cooperation in other forums during the Cold War, such as in the Nordic Council and in the UN, resulted in a good working relationship. Further leading to the facilitation of the development of a Nordic defense cooperation when this became possible. This strongly suggests that the end of the Cold War and the fall of the Soviet Union is a social phenomenon in history, making it possible for the Nordic states to develop a closer cooperation on security and defense policy (Cello, 2017).

The open initiatives for a closer Nordic cooperation on defense policy after the end of the Cold War was welcomed both by the political elite of each state, and by the citizens of the region (Saxi, 2018). This support was rather obvious, knowing the historical development from the Second World War. In 2009, the famous “Stoltenberg-rapport”¹⁷ was launched with ambitious proposals for further Nordic defense cooperation, increasing the level of ambition for a deeper and more comprehensive defense cooperation (Forsberg, 2013, p. 1162). Even though the thought of a closer Nordic defense cooperation received support in the initiating phase, it suffered various set-backs and resistance when suggestions were made on how to realize such cooperation. In Denmark for example, Nordic defense cooperation was unofficially perceived as a waste of time: “The key to a closer Nordic cooperation lays within the framework of the larger cooperation in NATO and the EU [...] Forget all about mini-NATO [e.g. Nordic defense cooperation]”¹⁸ (quote by Uffe Ellemann-Jensen in Saxi, 2018, p. 93, my translation). This indicates that Nordic defense cooperation was restrained by membership in NATO and the EU, confirming the theoretical understanding that states entering new institutional arenas, or forums, are embedded in multiple domestic and international contexts and are therefore not free agents (Checkel, 2005). At the time, it seemed as NATO and the EU were preferred forums for the Danes.

Information gathered from the interviews strengthens the argument of restrained membership. The representatives in the Norwegian Ministry of Defense mentioned certain set-backs for Nordic defense cooperation:

[A]t the same time we have observed that the cooperation have experienced some set-backs. The case of combat aircraft is one of them. Norway chose F35, even if Jas-Gripen, as one of the Swedish aircrafts, was one of the candidates. That could have been interpreted as unfortunate, and then we also had this Archer, an artillery cooperation, that failed a couple of years ago, and this created some challenges¹⁹ (Norwegian bureaucrat, 2018, my translation).

¹⁷ A report written by the well-known Norwegian statesman Thorvald Stoltenberg as ordered by the Nordic foreign ministers (Forsberg, 2013, p. 1162).

¹⁸ Original phrase: “Nøglen til et tættere nordisk samarbejde ligger inden for rammerne af et større samarbejde i NATO og EU [...] glem alt om mini NATO” (Saxi, 2018, p. 93).

¹⁹ Original phrase: «men samtidig har vi sett at samarbeidet har gått på noen smeller. Kampflysaken var ett av dem. Norge valgte F35, hvor Jas-Gripen var et, som et av det svenske flyet, var en av kandidatene. Det kunne bli oppfattet som uheldig, også hadde vi denne Archer, dette artilleri-samarbeidet, som stranda for noen år siden, og det skapte noen utfordringer» (Norwegian bureaucrat, 2018).

But it is, in a way, what the NORDEFECO-setting lacks inasmuch any material setting, there is a lack of the good examples of cases where one really cooperate all the way through. So to speak, that one adopt exactly the same systems²⁰ (Norwegian Lieutenant Colonel, 2018, my translation).

These findings strengthen the argument of nation states not being free agents, where Norway in the case of combat aircrafts, chose the American F35 instead of the Swedish Jas-39 Gripen NG. The Swedish prime minister at the time, Frederik Reinfeldt, declared that he was “disappointed and surprised” and further he characterized the decision as “a set-back for our ambitions to further develop Nordic solutions”²¹ (as quoted in Saxi, 2018, p. 93, my translation). This indicates that Norway, in this situation chose NATO and American friendship, over Swedish neighborhood and partnership. Consequently, such decisions undermine Nordic defense cooperation because, as I will come back to in the next section, it is not what you say that is of most importance, it is what you do that matters.

Despite the resistance and various difficulties with Nordic defense cooperation, NORDEFECO was established in 2009, shortly after the launch of the “Stoltenberg-rapport”. In the first years of the cooperation, NORDEFECO did not achieve the economic aim of cost-efficiency, and the benefits of intergovernmental cooperation was not as expected. Continuing, as highlighted above, the cooperation experienced various set-backs, mainly because of commitment to other central forums for security and defense policy. However, in 2015 a critical juncture happened that revived the cooperation in NORDEFECO. The defense sectors in each state demanded an increase in the states’ defense budget. Consequently, the defense budgets in Norway, Sweden and Finland increased largely due to this, also instigated by the increased security threat posed by Russia (Saxi, 2018). To conclude, it is evident that NORDEFECO failed to create cost-efficient solutions for the defense sector. In the end, the only solution was to increase the national budgets making the Nordic states able to develop the necessary capabilities, such as cyber defense capabilities.

²⁰ Original phrase: «Men det er jo på en måte det at man mangler jo i NORDEFECO-settingen da for såvidt, i enhver materiell setting, så mangler man de gode eksemplene på at man virkelig samarbeider tvers gjennom. Altså det at man adopterer klin like systemer» (Norwegian Lieutenant Colonel, 2018).

²¹ Original phrase: «skuffet og overrasket», «et tilbakeslag for våre ambisjoner om å utvikle nordiske løsninger» (as quoted in Saxi, 2018, p. 93).

Although the cooperation suffered a tough start with several set-backs and ‘failures’, NORDEFECO today is a cooperation mainly characterized by friendship, pragmatism and incrementalism (Saxi, 2018, p. 95). NORDEFECO being characterized by pragmatism and incrementalism explains why the ambitions for the development of common cyber defense capabilities are low, and that the Nordic states are satisfied with small accomplishments. Cyber defense within NORDEFECO is an example of the adjustments conducted in the cooperation and how the Nordic states have learned from previous mistakes. As stated by one of the informants, NORDEFECO is “almost like a marriage”²² (Norwegian bureaucrat, 2018, my translation). This indicates that the cooperation does have pitfalls, and it has happened – and will most likely happen again – that certain things go wrong. However these set-backs does not put the entire cooperation in danger. Most likely the Nordic states will continue the cooperation after similar set-backs in the future, and learn from the mistakes made, similar to any marriage. This is what is unique with such a close regional cooperation that has existed for a long time and holds close historical ties.

Based on the findings presented in this section, it is evident that NORDEFECO did not reach its aim of cost-efficient solutions. This strongly suggests that there are other factors and motivations ensuring that the Nordic cooperation remains. The long history for cooperation is an additional factor holding Nordic cooperation together despite various set-backs and the failure of cost-efficient solutions. However, historical ties are not sufficient to understand why the Nordic states seek closer cooperation on cyber defense. The Nordic states have close historical ties with many different nations, and it is therefore crucial to understand what distinguishes the relationship amongst the Nordic states from the relationships with other states. Continuing, the element of friendship amongst the Nordic states and the comparison of NORDEFECO with a marriage, introduces trust as the last variable for this thesis. For any well-functional friendship and/or marriage, trust is essential. The next section therefore elaborates on the element of trust in NORDEFECO.

²² Original phrase: «Det blir nesten som et ekteskap [...]» (Norwegian bureaucrat, 2018)

6.4 Trust

Measuring the level of trust among certain actors is a challenging task, and it is not the aim of this section. Instead, this section aims at researching whether trust is a central factor in explaining NORDEFECO and, if so, how one can best build trust in an intergovernmental cooperation working with sensitive issues such as defense policy. It is not a given that members in an intergovernmental cooperation trust each other, especially not with sensitive and confidential information. However, for a cooperation to be successful and to accomplish results, trusting each other is helpful as it facilitates the process leading up to results (Norwegian Armed Forces, 2011).

Trust was already mentioned in the first annual report of NORDEFECO, strongly suggesting that trust has been a crucial factor for the cooperation since its establishment. Also, it stated that a high level of trust was observed already in the first year of NORDEFECO's existence: "Concrete results will be generated by trust, patience and joint commitment. I have, therefore, with great satisfaction, noticed the high level of commitment and trust between our Nordic colleagues" (Norwegian Armed Forces, 2011). With this as the starting point of the cooperation, it is evident that in the case of NORDEFECO trust is a dominant factor:

[M]uch of this secrecy is based on trust, so in the best case scenario everyone know more than they are willing to talk about, but that is fine because it is mutual. So, a great deal of security is about the possibility for me to provide you with something of value, but with the understanding that you will not pass this on to anyone else [...]²³ (Norwegian Lieutenant Colonel, 2018, my translation).

This statement proves that trust is helpful in a cooperation dealing with sensitive issues, such as defense policy and development of capabilities. For the parties to be willing to share relevant information, one must trust that the receiving part does not share sensitive information with anyone else. When such a trusting relationship is built, it will facilitate the information-sharing, and different parties of a cooperation can take advantage of the information provided by others. This confirms the theoretical understanding that socialization and learning leads to group norms and a logic of appropriateness (Checkel, 2005; Copeland, 2006). Given that the Nordic states have experienced on several occasions that it is beneficial to share information, knowledge, and

²³ Original phrase: «Fordi mye av dette hemmeligholdet er basert på tillit, så i beste fall vet alle mer enn de vil snakke om, men det er helt greit. Fordi det er gjensidig. Så veldig mye sikkerhet dreier seg om at jeg kan gi deg noe, men det er under forutsetning om at du ikke gir det videre [...]» (Norwegian Lieutenant Colonel, 2018).

competence, even though it might be confidential or sensitive, it is likely that they will repeat it. Thus, a common culture has been developed and a norm of sharing sensitive information and best practice with each other has been established (Copeland, 2006; Saurugger, 2014). Because much of the cooperation in NORDEFECO is based information-sharing, trust is an essential factor: “There has to be enough trust to make this information-sharing effective (Finnish bureaucrat, 2018).

NORDEFECO is to a large extent based on information-sharing and dialogue, which are two elements that require trust (Buchanan, 2016). As mentioned earlier, cost-efficiency was the most central motivation for NORDEFECO up until 2014, according to the annual reports and the statement by Sverre Diesen. Therefore, rational reasoning and potential economic benefits can to a great extent explain the first phase of Nordic defense cooperation. However, in 2014 there was a shift of focus in NORDEFECO and dialogue gained more focus than cost-efficiency (The Ministry of Defence Sweden, 2016). The finding that dialogue is gaining importance in the cooperation is an indication of a less rational reasoning compensated with an increased focus on socialization and learning. Consequently, dialogue and socialization has become an equally important motivation, or even perhaps a greater motivation, for the further development of NORDEFECO. As a result, this year the Norwegian chairmanship has ambitions of creating more room for dialogue and discussion in order to find common solutions to central challenges within the defense sector (Norwegian bureaucrat, 2018). Such a development is closely linked to trust, and socialization is a prerequisite for trust-building, as stated by the Finnish informant; “trust is built when these actors know each other” (Finnish bureaucrat, 2018).

NORDEFECO does have the foundation for a successful trust-building process because of the shared culture, values and identity that exist among the Nordic states and its citizens (Forsberg, 2013, p. 1175). In other words, the Nordic region is a region with essential similarities helpful when building trust. Also, the Nordic states are able to “speak the same language”, in the sense that they have an understanding of each other’s interests and their fundamental equalities and differences, which facilitate the process of trust-building. Such an understanding, in addition to the ability to communicate, is something that improves with time, and therefore the historical ties elaborated above further facilitate Nordic cooperation. Also, the Nordic states are aware of their varying needs and plans, making it easier to find either common solutions or come to terms

with the decision of one or two states' choosing to stay outside Nordic cooperation on certain issues (Norwegian bureaucrat, 2018). As nicely formulated by the Finnish informant:

We have had a lot of capability projects starting in COPA CAPA, where one of the nation's say that 'well that is not relevant for us', and that is fully OK. It's fair, it's open, it's honest, and it's frank, and that does, and that actually enhances the trust (Finnish bureaucrat, 2018).

This is in line with the theory stating that good working relationship and communication mechanisms between the parties involved facilitate the trust-building process. Also, these findings support the claim that small states find it easier to trust each other because they "benefit from security guarantees provided by other states" (Buchanan, 2016). Based on this argumentation it is evident that Nordic defense cooperation indeed has the foundation needed for the further development of a trusting relationship. Continuing, the fact that high level of trust was observed already in the first year of cooperation is a sign of a cooperation strongly linked to trust.

NORDEFECO is an example of a cooperation benefitting from a trusting relationship that facilitates the development of capabilities in the category of high politics, such as cyber defense capabilities. Even though dialogue and socialization are central in the trust-building process there is one crucial element for trust-building that has not been mentioned yet, and that is the realization of common activities and exercises:

When we go further in this [e.g. trust], I think exercises are the emerging priority in the cooperation, so exercises become another central element. It is kind of a deeper information-exchange. And exercises facilitate a form where we can, or we see that exercises are the best way to share experiences, knowledge and know-how, and techniques and tactics and procedures (Finnish bureaucrat, 2018).

[A] great deal of the trust also comes [...] with these practical cooperation activities as you can see. Such as cyber defense, and frankly much else²⁴ (Norwegian bureaucrat, 2018, my translation).

²⁴ Original phrase: «Og mye av den tilliten den kommer jo også [...] med disse praktiske samarbeidsaktivitetene kan du se da. Sånn som cyber defense, og egentlig veldig mye annet» (Norwegian bureaucrat, 2018).

This illustrates that to build trust it is also necessary to achieve some results in the form of activities and exercises. It is not until the discussions have led to a result that one truly discloses whether the other parties were trustworthy, “there are lots of sayings that talking is good, but you know, what you do is gold” (Finnish bureaucrat, 2018). This might be the greatest distinction between NORDEFECO on the one hand, and the EU and NATO on the other hand. One could argue that the two latter organizations are more concerned with talking, while NORDEFECO is more concerned with doing, referring to the statement that NORDEFECO is a practical example of EU’s pooling and sharing and NATO’s smart defense (National representative, 2018). As a result of this difference, a successful cooperation in NORDEFECO requires more trust than a successful cooperation in the EU or NATO. Also, the practical focus of NORDEFECO and the high level of trust among the Nordic states can explain why NORDEFECO has succeeded in the accomplishment of some activities developing cyber defense capabilities, while the EU and NATO are struggling to get started with a cooperation within this area (Norwegian Lieutenant Colonel, 2018). This leads me to the conclusion that trust is indeed a crucial factor for regional cooperation, and it is one of the most central factors for the development of a closer Nordic cooperation on defense policy within the NORDEFECO-framework.

To conclude, the argumentation of the four sections strongly suggests that trust and burden-sharing are the two most central factors for why the Nordic states seek closer institutional cooperation on defense policy. In the case of cyber defense, it is evident that cost-efficiency, in addition to dialogue and exercises, are essential elements to build a strong and resilient cyber defense within the NORDEFECO-framework. Figure 6.1 illustrates the main findings of this section by giving a simple presentation of the different motivations for cooperation, including the factors each motivation originates from.

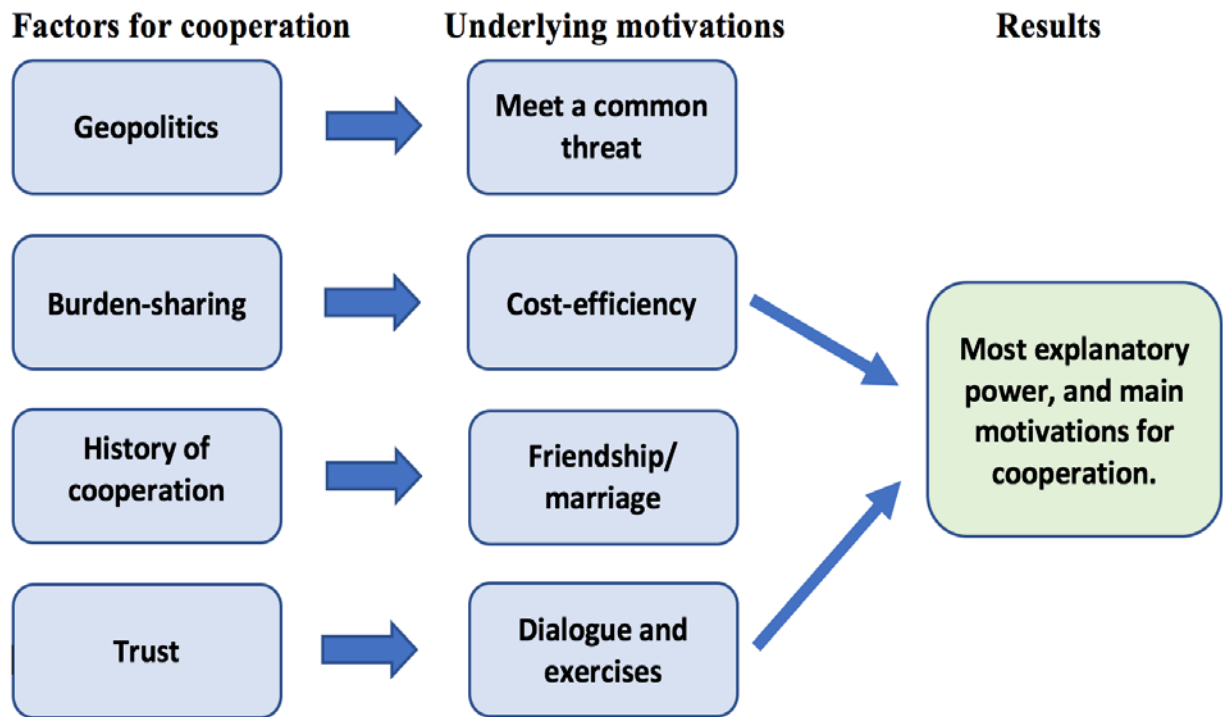


Figure 6.1 Main findings.

7 Why Nordic Cooperation? A Discussion of the Findings

The analysis presented above has addressed the three sub-questions posed in the introduction:

1. What distinguishes the Nordic cooperation on defense policy, and more precisely cyber defense policies, from the cooperation within NATO and the EU?
2. How can Nordic cooperation on cyber defense illustrate the need for stronger regional cooperation in an ever-globalized world?
3. Which factors make Nordic cooperation feasible and realistic?

By addressing these three questions, the analysis as a whole provides sufficient evidence, from theory, empirical material and previous research, to fully answer the research question of why the Nordic states are seeking closer cooperation on defense policy within NORDEFECO. Before presenting the conclusion of the thesis, it is necessary to provide a discussion of the findings presented in the analysis, elaborating how these provides sufficient evidence needed to answer the research question.

7.1 NORDEFECO as a Regional Cooperation in a Globalized World

The EU and NATO are, similar to NORDEFECO, working intensively with developing strong and resilient cyber defense capabilities. As argued in this thesis, NORDEFECO should be perceived as a provider of practical examples on how cyber defense capabilities could be developed. The EU and NATO on the other hand, provide more general and overall policies and guidelines for such defense capabilities. The aim of NORDEFECO is not to compete with the development of defense policy within NATO and the EU. However, when it comes to high politics it is evident that smaller regional forums is preferred because it involves the sharing of restrictive or confidential information. This supports the claim of the theoretical presumption of security regionalism and the importance of trust in a cooperation aiming at the realization of activities and exercises (Buchanan, 2016; Buzan, 1991; Kydd, 2000). These findings illustrate that even though the EU, NATO and NORDEFECO have different roles regarding the development of cyber defense capabilities, small forums have better conditions for realizing such capabilities, which ultimately should be the main goal of all forums. Also, the struggles with developing common cyber defense capabilities indicate that most initiatives can be categorized as initiatives of 'bare survival' responding to an increasing threat, not an offensive wish to cooperate (Rosenau, 1995). However, NORDEFECO's success with the implementation of some activities suggests that the Nordic states have showed a more offensive wish to cooperate in recent years.

NORDEFECO is more of an informal cooperation, being compared to a friendship and/or a marriage characterized by a good working relationship all the way down to the individual level. It is evident that these factors facilitate the process of developing cyber defense capabilities, which require actors to be open about their vulnerabilities and weaknesses. Also, NORDEFECO consists of members with equal fundamental values and similar interests, in addition to an understanding of various restrictions from membership in other forums. The EU and NATO on the other hand are formal systems/organizations consisting of many members with varying interests and different fundamental values. Making it difficult to build a trusting relationship between the members. The challenges with building trusting relationships in the EU and NATO affect the level of honesty between the participants, creating difficulties for the members to disclose their vulnerabilities and weaknesses. The issues with disclosing sensitive information might be explained by the fear that others, at the receiving end, will exploit these vulnerabilities and weaknesses. Based on this argumentation, there is a close link between fear and trust, confirming the theoretical understanding of trust presented in chapter two (Buchanan, 2016). As a result, this discussion strengthens the argument presented in the analysis, stating that NORDEFECO as a smaller regional forum is the preferred forum for its members to deal with sensitive issues, such as the development of cyber defense capabilities. This finding supports the claim made by Kellow (2012) that successful forums can be limited by geography and issues, even though the world is becoming more globalized.

When it comes to cyber defense capabilities one must start one place with developing knowledge and competence. Based on the evidence presented in this thesis, a small forum as NORDEFECO might be the best place to start. Since the EU and NATO are struggling with detecting how to build common cyber defense capabilities, it has resulted in the Nordic states becoming impatient and not satisfied with the pace of the progress so far within the EU and NATO. It has therefore led to a wish to further develop more concrete activities and exercises within the NORDEFECO-framework, to speed up the process of developing a strong and resilient cyber defense in each nation. The fact that NORDEFECO consists of five states, and only four at the military level, makes the process from developing policies, to implementation and real-life activities shorter. It is easier to get five or four relatively equal states to agree on certain issues than to get 28 or 29 states to agree on the same issues. When it comes to sensitive issues, such as cyber defense, it is self-evident that developing capabilities in smaller forums is easier,

than what is the case with larger forums. However, one challenge in small forums is the limited budget, which have been a problem for NORDEFECO, making it difficult to develop cost-efficient solutions. This challenge was partly solved in 2015 when the national defense budgets increased. Also, it is no help having a large budget, if there are no activities to spend the resources on. By being able to implement activities, the results of smaller forums can be beneficial for larger forums. When capabilities have been developed in smaller forums, the results can at a later stage be shared with larger forums, assuming small forums are open to share their experience and best practice to the larger forums.

In addition to the abovementioned aspects, geography has been introduced as a central element tying the Nordic states closer together. The Nordic states are geographically close to each other, enhancing the sense of belonging to the Nordic region and supporting the understanding of regionalism as a concept requiring geographic proximity (Mansfield & Solingen, 2010; Rosenau, 1995). To compare, the EU and NATO covers large geographical areas, making it difficult to create a sense of belonging to their entire territories. Even though cyber space is in another 'room', geography is still relevant because it facilitates cooperation by making it easier to meet in person to discuss central challenges on the cyber space. Such meetings, at the micro-level, are central in the development of closer institutional cooperation at the macro-level, as argued in chapter five.

When having a cooperation with members who are physically close to each other, it also facilitates realization of activities and exercises. This can explain why NORDEFECO is aiming at delivering practical examples of EU's pooling and sharing, and NATO's smart defense. Further, as argued in chapter six, the realization of activities and exercises enhance the level of trust among the members of a cooperation. It is therefore reason to believe that the Nordic states have a more trusting relationship to each other, than to other states in the EU and NATO. Such a trusting relationship can explain why NORDEFECO has been able to realize some activities promoting the development of common cyber defense capabilities, at the same time as the EU and NATO are struggling to get a similar cooperation on cyber defense started.

7.2 Central Factors and Underlying Motivations for Cooperation

The four central factors analyzed in chapter six prove that Nordic cooperation on cyber defense is feasible and realistic. In addition, the findings presented in figure 6.1 strengthen the argument that the best place to start with the development of cyber defense capabilities is in a regional forum, such as NORDEFECO. The conclusion of the chapter is that burden-sharing and trust are the two factors with most explanatory power. Cost-efficiency was the most important motivation for the establishment of NORDEFECO, and the Nordic-Baltic cooperation represents the political economic theory of comparative advantage. Trust on the other hand, represented by dialogue and exercises, has become the most central motivation since 2014. In the unstable world we witness at the time of writing this thesis, it is essential for nation states to have trustworthy allies and partners.

Even though these two factors have most explanatory power, the following two are also central in understanding why the Nordic states are seeking closer cooperation on defense policy. Geopolitics gained importance after 2014 when it became evident that the Nordic states needed to stay together and oppose unacceptable Russian behavior in the international sphere. Continuing, as mentioned in chapter four, the issue of how to meet cyber threats gained importance in NORDEFECO after 2014, placing the development of cyber defense capabilities high on the agenda in the cooperation. The increased importance on developing cyber defense capabilities also increased the importance of the Nordic-Baltic cooperation, with geography as a major link binding the two regions together. In addition, history of cooperation is crucial in order to understand how the Nordic states could develop a defense cooperation shortly after the end of the Cold War, and why the cooperation is characterized as a friendship and/or as a marriage. Also, history of cooperation is eminent to understand why severe set-backs and 'failures' have not caused NORDEFECO to dissolve. Despite a bumpy road, NORDEFECO has continued its development towards a better and deeper defense cooperation amongst the Nordic states, and it is expected to be further developed in the future.

8 Concluding Remarks

The aim of this thesis has been to answer the question of why Nordic states are seeking closer cooperation on defense policy within NORDEFECO. This is to better understand the development of global governance and why regional forums still are relevant in an ever-globalized world. By focusing on the case of cyber defense the scope of the thesis has been limited, making it possible to go in depth on one certain issue and still include a general discussion of NORDEFECO as a whole. Through analysis of NORDEFECO as a cooperation and cyber defense as a newly developed issue of cooperation, this thesis has argued that regional forums are preferred in the case of cooperation on high politics such as security and defense policy.

The theoretical understanding of global governance, in addition to the empirical evidence gathered from various sources, allows me to conclude that Nordic states seek closer cooperation on defense policy within NORDEFECO because of a various set of factors. First, regional cooperation is in this case preferred when dealing with defense policy. Elements such as cultural similarities, geographical proximity, same external threat, and similar interest in focusing on cyber security are central in understanding why the Nordic states prefer a Nordic forum for cooperation in the development of cyber defense capabilities. Further, when looking at the variables of 1) geopolitics, 2) burden-sharing, 3) history of cooperation, and 4) trust, it is evident that the four variables combined (see figure 6.1) can to a large extent explain Nordic cooperation. Continuing, burden-sharing and trust have greater explanatory power than geopolitics and history of cooperation as to why the Nordic states still aim at closer Nordic cooperation on defense policy. Focusing on these four variables gave room to investigate the underlying motivation for cooperation. Indicating that cost-efficient solutions, increased dialogue and the realization of exercises are the most central motivations for Nordic defense cooperation in NORDEFECO.

Even though the four independent variables have large explanatory power combined, this does not necessarily mean that other factors are not relevant as well. Intergovernmental cooperation is a complex topic with several explanatory factors, indicating that one must be open for the possibility of influence from other factors. Also, cyber defense is a complex and relatively new policy area which requires further research with the inclusion of other factors. One interesting

suggestion for further research would be to focus on the balance between public and private actors.

Despite the fact that other factors would be relevant to include, the findings presented and discussed in this thesis provide a detailed and elaborated answer to the research question, as summarized in the preceding chapter. The analysis strengthens the theoretical framework of the thesis, providing empirical evidence supporting the theoretical framework presented in chapter two. In other words, this thesis contributes to theory building by providing a theoretical framework useful to analyze and explain why Nordic states seek closer cooperation on defense policy in NORDEFECO. This indicates that a combination of realism and constructivism proved to be a useful tool when analyzing the empirical material gathered for the project. In other words, the theoretical framework for the thesis is useful when aiming at analyzing NORDEFECO and cyber defense as a case. For further research it would be relevant to use the same theoretical framework on other regional forums and investigate whether the theoretical framework still is useful or if it should be changed.

When combining constructivism and realism, it is evident that this thesis is favoring a holistic approach to theory building where both realism and constructivism contribute to the understanding of why Nordic states seek closer cooperation on cyber defense policy. The different ontological approaches have varying explanatory power. As argued in this thesis realism had highest explanatory power from 2009 up until 2014, with burden-sharing as the most crucial factor for cooperation. In 2014 a critical juncture happens resulting in constructivism replacing realism as the ontological approach with the greatest explanatory power, and trust replaces burden-sharing as the most crucial factor for cooperation.

For further research it would be relevant to look closer at the micro-level, as suggested by the constructivist approach, with focus on how individuals cooperate on cyber defense within the NORDEFECO-framework. The findings presented in this thesis highlight the micro-level as an interesting perspective for further investigation by introducing the importance of good interpersonal relations for further institutional development. It would be beneficial to find out if individuals working directly with developing cyber defense capabilities have the same

understanding of NORDEFECO as the political and military elite. In other words, a project focusing on the micro-level would be a fitting continuation of this thesis.

Literature

- Adams, T. (2018, 24.03.). Facebook's week of shame: the Cambridge Analytica fallout. *The Guardian*. Retrieved from <https://www.theguardian.com/technology/2018/mar/24/facebook-week-of-shame-data-breach-observer-revelations-zuckerberg-silence>.
- Alter, K. J., & Meunier, S. (2009). The Politics of International Regime Complexity. *Perspectives on Politics*, 7(1), 13-24. doi:10.1017/S1537592709090033
- Bell, D. (2017). Political realism and international relations. *Philosophy Compass*, 12(2), 1-12. doi:10.1111/phc3.12403
- Buchanan, B. (2016). *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. New York: Oxford University Press.
- Bukkvoll, T., & Åtland, K. (2015). Russlands kriger i Georgia og Ukraina: Konsekvenser og lærdommer for Norge. In T. Heier & A. Kjølberg (Eds.), *Norge og Russland: Sikkerhetspolitiske utfordringer i nordområdene* (pp. 85-95). Oslo: Universitetsforlaget.
- Buzan, B. (1991). *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era* (2nd ed.). Boulder, Colo: Lynne Rienner.
- Cello, L. (2017). Taking history seriously in IR: Towards a historicist approach. *Review of International Studies*, 44(2), 236-251. doi:10.1017/S0260210517000432
- Checkel, J. T. (2005). International Institutions and Socialization in Europe: Introduction and Framework. *International Organization*, 59(4), 801-826. doi:10.1017/S0020818305050289
- Copeland, D. C. (2006). The constructivist challenge to structural realism: A review essay. In S. Guzzini & A. Leander (Eds.), *Constructivism and International Relations: Alexander Wendt and his critics* (pp. 1-20). Abingdon: Routledge.
- Danish Ministry of Defence. (2017). *NORDEFECO Annual Report 2016: «Promoting security through cooperation»*. København: Danish Ministry of Defence. Retrieved from <http://www.nordefco.org/files/Design/NORDEFECO%20Annual%20Report%202016.pdf>.
- Danish Ministry of Defence. (2018, 03.08.2018). EU - The Danish Defence Opt-Out. Retrieved from <http://www.fmn.dk/eng/allabout/Pages/TheDanishDefenceOpt-Out.aspx>.
- Defence Command Denmark. (2013). *NORDEFECO Military Coordination Committee Annual Report 2012*. The Danish chairmanship of the Nordic Military Coordination Committee. Retrieved from <http://www.nordefco.org/files/Design/NORDEFECO%20Annual%20Report%202012.pdf>.
- Defense Command Finland. (2014). *NORDEFECO Annual Report 2013*. The Finnish chairmanship of the Nordic Military Coordination Committee. Retrieved from <http://www.nordefco.org/files/AR2013.pdf>.
- Defense News. (2017, 27.02.2017). Sweden to scale up cyber defense funding. *Defense News*. Retrieved from <https://www.defensenews.com/2017/02/27/sweden-to-scale-up-cyber-defense-funding/>.
- Eckstein, H. (1975). Case Study and Theory in Political Science. In F. I. Greenstein & N. W. Polsby (Eds.), *Strategies of Inquiry. Handbook of Political Science* (Vol. 7, pp. 79-137). Reading, MA: Addison-Wesley.
- European Commission. (2013, 16.04.2018). Cybersecurity. Retrieved from <https://ec.europa.eu/digital-single-market/en/cyber-security>.
- European Commission, & High Representative of the European Union for Foreign Affairs and Security Policy. (2013). *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*. Brussels: The European Union Retrieved from https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.
- European Parliament. (2015). *Understanding hybrid threats.*: European Parliament. Retrieved from [http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA\(2015\)564355_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf).
- Evera, S. V. (1997). *Guide to Methods for Students of Political Science*. Ithaca; New York: Cornell University Press.
- EØS-notat. (2016). *NIS-Direktivet*. EØS-notatbasen Retrieved from <https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet/id2483374/>.
- Fermann, G. (2013). Utenrikspolitisk praksis. Handlingsrom, interesser, virkemidler. In G. Fermann (Ed.), *Utenrikspolitikk og norsk krisehåndtering* (pp. 47-88). Oslo: Cappelen Damm AS.
- Finnish bureaucrat (2018, 12.04.2018). [Interview 4: Semi-Structured Phone Interview].
- Finnish Ministry of Defence. (2018). *NORDEFECO Annual Report 2017*. Helsinki: Finnish Ministry of Defence.
- FireEye Inc. (2018). Why FireEye? Retrieved from <https://www.fireeye.com/company.html>
- FN-Sambandet. (2017, 17.08.2017). FN-pakten. Retrieved from <https://www.fn.no/Om-FN/Avtaler/FN-pakten>.
- Forsberg, T. (2013). The rise of Nordic defence cooperation: a return to regionalism? *International Affairs*, 89(5), 1161-1181.
- Forsvarsministeriet. (2014). *National strategi for cyber- og informationssikkerhed: Øget professionalisering og mere viden*. København: Regeringen. Retrieved from <http://www.fmn.dk/TEMAER/CYBERSIKKERHED/Pages/national-strategi-for-cyber-og-informationssikkerhed.aspx>.
- Gerring, J. (2007a). *Case Study Research: Principles and Practices*. New York: Cambridge University Press.
- Gerring, J. (2007b). Is There a (Viable) Crucial-Case Method? *Comparative Political Studies*, 40(3), 231-253.
- Hettne, B. (2005). Beyond the 'new' regionalism. *New Political Economy*, 10(4), 543-571. doi:10.1080/13563460500344484
- Hewson, M., & Sinclair, T. J. (1999). The Emergence of Global Governance Theory. In M. Hewson & T. J. Sinclair (Eds.), *Approaches to Global Governance Theory* (pp. 3-22). Albany: State University Press of New York Press.
- Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies.
- Institute of International Relations Prague (Producer). (2017, 24.01.2018). Mark Galeotti: Russia's Hybrid War: What Does it Really Mean, And How Should the West Respond? [Videofilm] Retrieved from https://www.youtube.com/watch?v=M1INBEAR_2M&t=3007s.
- Johnsen, S. O. (2015). A comparative study of the Norwegian Cyber Security Strategy vs strategies in EU and the US-emerging cybersafety ignored. In L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio, & W. Kröger (Eds.), *Safety and Reliability of Complex Engineered Systems* (pp. 3485-3492). London: Taylor & Francis Group.
- Justis- og beredskapsdepartementet. (2017). *IKT-sikkerhet: Et felles ansvar*. (Meld. St. 38 (2016-2017)). Oslo: Regjeringen. Retrieved from <https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/>.

- Justisdepartementet. (2017). *Nationell strategi för samhällets informations- och cybersäkerhet*. (Skr. 2016/17:213). Stockholm: Regeringskansliet. Retrieved from <http://www.regeringen.se/rattsdokument/skrivelse/2017/06/skr.-201617213/>.
- Kellow, A. (2012). Multi-level and multi-arena governance: the limits of integration and the possibilities of forum shopping. *International Environmental Agreements: Politics, Law and Economics*, 12(4), 327-342. doi:10.1007/s10784-012-9172-3
- Keohane, R. O. (1998). International institutions: can interdependence work? . In R. O. Keohane (Ed.), *Power and Governance in a Partially Globalized World* (pp. 27-38). London: Routledge.
- Kydd, A. (2000). Overcoming Mistrust. *Rationality and Society*, 12(4), 397-424.
- Lilleker, D. G. (2003). Interviewing the Political Elite: Navigating a Potential Minefield. *POLITICS*, 23(3), 207-214.
- Mansfield, E. D., & Solingen, E. (2010). Regionalism. *Annual Review of Political Science*, 13, 145-163. doi:10.1146/annurev.polisci.13.050807.161356
- Moravcsik, A. (1997). Taking Preferences Seriously: A Liberal Theory of International Politics *International Organization*, 51(4), 513-553. doi:10.1162/002081897550447
- Morgan, P. M. (1997). Regional Security Complexes and Regional Orders. In D. A. Lake & P. M. Morgan (Eds.), *Regional Orders: Building Security in a New World* (pp. 20-42). University Park, PA: The Pennsylvania State University Press.
- Moses, J. W., & Knutsen, T. L. (2012). *Ways of Knowing: Competing Methodologies in Social and Political Research*. (2nd. ed.). Hampshire: Palgrave Macmillan.
- Murphy, H., & Kellow, A. (2013). Forum Shopping in Global Governance: Understanding States, Business and NGOs in Multiple Areas. *Global Policy*, 4(2), 139-149. doi:10.1111/j.1758-5899.2012.00195.x
- National representative (2018, 15.03.2018). [Interview 1: Semi-Structured Phone Interview]. Nordic Defence Cooperation. (n.d.). The basics about NORDEFECO. Retrieved from <http://www.nordefco.org/the-basics-about-nordefco>.
- Norsk rikskringkasting (2018) (Producer). (2018, 18.01.2018). Krig og fred: Når kommer robotkrigen? [Podcast] Retrieved from https://radio.nrk.no/podcast/krig_og_fred/nrkno-poddkast-26572-129596-18012018020000.
- Norsk utenrikspolitisk institutt NUPI (Producer). (2018, 25.01.2018). Cyber Intelligence and Nordic Security. [Video File] Retrieved from <https://www.youtube.com/watch?v=3DE8xBR8a0o>.
- North Atlantic Treaty Organization. (2017a, 08.12.2017). NATO and the European Union deepen cooperation on cyber defence. Retrieved from https://www.nato.int/cps/en/natohq/news_149848.htm?selectedLocale=en.
- North Atlantic Treaty Organization. (2017b, 20.02.2017). Smart Defence. Retrieved from https://www.nato.int/cps/ua/natohq/topics_84268.htm.
- North Atlantic Treaty Organization. (2018, 19.02.2018). Cyber defence. Retrieved from https://www.nato.int/cps/en/natohq/topics_78170.htm.
- Norwegian Armed Forces. (2011). *NORDEFECO Military Level Annual Report 2010*. Oslo: The Norwegian chairmanship of NORDEFECO Military Coordination Committee. Retrieved from <http://www.nordefco.org/Files/AR2010.pdf>.
- Norwegian bureaucrat (2018, 03.04.2018). [Interview 2: Semi-structured interview].
- Norwegian Lieutenant Colonel (2018, 03.04.2018). [Interview 2: Semi-structured interview].
- Norwegian Senior Staff Officer (2018, 11.04.2018). [Interview 3: Semi-Structured Phone Interview].

- NOU 2012:2. (2012). *Utenfor og innenfor: Norges avtaler med EU*. Oslo: Departementenes servicesenter, Informasjonsforvaltning Retrieved from www.regjeringen.no/no/dokumenter/nou-2012-2/id669368/sec1.
- O'Dwyer, G. (2017). Nordic states join together to bolster cyber defenses. *DefenseNews*. Retrieved from https://www.defensenews.com/international/2017/10/06/nordic-states-join-together-to-bolster-cyber-defenses/?utm_source=Sailthru&utm_medium=email&utm_campaign=DFN%20DNR%2010/6/17&utm_term=Editorial%20-%20Daily%20News%20Roundup.
- Pempel, T. J. (2005). Introduction: Emerging Webs of Regional Connectedness. In T. J. Pempel (Ed.), *Remapping East Asia: The Construction of a Region* (pp. 1-30). Ithaca, NY: Cornell University Press.
- Peters, B. G., & Pierre, J. (2009). Governance Approaches. In A. Wiener & T. Diez (Eds.), *European Integration Theory* (2nd. ed., pp. 91-104). Oxford: Oxford University Press.
- Rantapelkonen, J., & Salminen, M. (Eds.). (2013). *The Fog of Cyber Defence*. Helsinki: National Defence University.
- Read, M., & Marsh, D. (2002). Combining Qualitative and Quantitative Methods. In D. Marsh & G. Stoker (Eds.), *Theory and Methods in Political Science* (2nd. ed., pp. 231-248). Hampshire: Palgrave Macmillan.
- Richards, D. (1996). Elite Interviewing: Approaches and Pitfalls. *POLITICS*, 16(3), 199-204.
- Rid, T. (2016). *Rise of the Machines: The Lost History of Cybernetics*. Victoria: Scribe Publications.
- Rosenau, J. N. (1992). Governance, order, and change in world politics. In J. N. Rosenau & E.-O. Czempiel (Eds.), *Governance without government: order and change in world politics*. Cambridge: Cambridge University Press.
- Rosenau, J. N. (1995). Governance in the Twenty-first Century. *Global Governance*, 1(1), 13-43.
- Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, 17.03.2018). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. Retrieved from <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.
- Røste, O. B. (2013). *Politikk og økonomi for statsvitere* (2 ed.). Oslo: Gyldendal Norsk Forlag.
- Saurugger, S. (2014). *Theoretical Approaches to European Integration*. Hampshire: Palgrave Macmillan.
- Saxi, H. L. (2018). Nordisk forsvarssamarbeid etter den kalde krigen: Fra avståelse til integrasjon og havari. *FORTID*, 1, 90-97.
- Scott, M. (2018, 27.03.2018). Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower. *POLITICO Europe Edition*. Retrieved from <https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook/>.
- Singer, J. D. (1961). The Level-of-Analysis Problem in International Relations. *World Politics*, 14(1), 77-92. doi:10.2307/2009557
- Sjursen, H. (2017). Principles in European Union Foreign Policy. *International Relations and the European Union*.
- Slayton, R. (2017). What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment. *International Security*, 41(3), 72-109. doi:10.1162/ISEC_a_00267
- Swedish Armed Forces. (2012). *NORDEFco Military Level Annual Report 2011*. Stockholm: The Swedish chairmanship of the Nordic Military Coordination Committee. Retrieved from http://www.nordefco.org/Files/nordefco_ar_lo-res.pdf.

- Swedish Ministry of Defence. (2015). *Sweden's Defence Policy 2016-2020*. Retrieved from https://www.government.se/globalassets/government/dokument/forsvarsdepartementet/sweden_defence_policy_2016_to_2020.
- The European Union. (2018). European Union Global Strategy: Security and Defence. Retrieved from <https://europa.eu/globalstrategy/en/security-defence-0>.
- The Ministry of Defence of the Kingdom of Denmark, The Ministry of Defence of the Republic of Finland, The Ministry of Foreign Affairs of Iceland, The Ministry of Defence of the Kingdom of Norway, & The Government of the Kingdom of Sweden. (2009). *Memorandum of Understanding between the Ministry of Defence of the Kingdom of Denmark and the Ministry of Defence of the Republic of Finland and the Ministry for Foreign Affairs of Iceland and the Ministry of Defence of the Kingdom of Norway and the Government of the Kingdom of Sweden on Nordic Defence Cooperation*. Helsinki.
- The Ministry of Defence Sweden. (2016). *NORDEFECO Annual Report 2015*. Regeringen. Retrieved from https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/internationellt/nordefco-annual-report-2015_webb.pdf.
- The Norwegian Ministry of Defence. (2015). *NORDEFECO Annual Report 2014*. The Norwegian chairmanship of NORDEFECO. Retrieved from http://www.nordefco.org/Files/NORDEFECO_arsrapport_2014.pdf.
- Tjora, A. (2012). *Kvalitative Forskningsmetoder i praksis*. (2nd. ed.). Oslo: Gyldendal Norsk Forlag.
- Turvallisuuskomitea. (2013). *Finland's Cyber security Strategy*. Helsinki: Turvallisuuskomitea. Retrieved from <https://www.turvallisuuskomitea.fi/index.php/fi/yhteiskunnan-turvallisuusstrategia-yts>.
- Wendt, A. (1999). *Social Theory of International Politics*. Cambridge: Cambridge University Press.
- Wivel, A., & Marcussen, M. (2015). In the Shadow of History? Explaining the (lack of) Europeanisation of Nordic Security and Defence Policies. In C. H. Grøn, P. Nedergaard, & A. Wivel (Eds.), *The Nordic Countries and the European Union: Still the Other European Community?* (pp. 206-225). Abingdon; N.Y.: Routledge
- Yin, R. K. (2003). *Case Study Research: Design and Methods* (3rd ed. Vol. 5). Thousand Oaks, CA: Sage Publications, Inc.

Appendix A – Informants and Interview Guides

Four interviews, with five informants in total, were conducted for this research project. The interviews were conducted with informants of the political and military elite, and they were therefore conducted as elite interviews.

Interview one – one informant:

- **National representative:** Informant who is national representative to NORDEFECO.

Interview two – two informants:

- **Norwegian bureaucrat:** Informant who is a national bureaucrat working with NORDEFECO and the capability sector in the Norwegian Ministry of Defense.
- **Norwegian Lieutenant Colonel:** Informant who is a national military official working with NORDEFECO and cyber defense capabilities in the Norwegian Ministry of Defense.

Interview three – one informant:

- **Norwegian Senior Staff Officer:** Informant working as a Senior Staff Officer in the Norwegian Cyber Defense.

Interview four – one informant:

- **Finnish bureaucrat:** Informant who is a national bureaucrat and has worked with NORDEFECO up until two years ago in the Finnish Ministry of Defense. He now works as a Senior Staff Office in the Finish Ministry of Defense and is still to some extent involved in NORDEFECO.

Interview with National Representative to NORDEF

1. Kan du begynne med å si noe om bakgrunnen for samarbeidet NORDEF?
 - a. Hvorfor ble det opprettet?
 - b. Hvorfor har det blitt mer institusjonalisert?

2. NORDEF er kjent for å kombinere NATOs smart defense og EUs pooling and sharing, kan du utdype hvordan et slikt forsvarssamarbeid foregår, rent praktisk?
 - a. Hvordan samarbeider dere?
 - b. Hvordan deles informasjon?
 - c. Hvordan fordeles ressursene?
 - d. *Hvordan kommuniserer dere?*

3. Ut ifra din mening, hvordan vil du si relasjonen er mellom de nordiske landene i samarbeidet?
 - a. Er det noen som er mer aktive enn andre?
 - b. Merkes det at ulike land er medlem av ulike organisasjoner (NATO, EU)
 - c. Har noen bedre samarbeid internt enn andre? Mindre allianser?
 - d. *Formelt/uformelt?*
 - e. *Hvem deltar i hva?*

4. Etter din vurdering, hva vil du si er de viktigste faktorene for Nordisk forsvarssamarbeid?
 - a. Hva er sentrale utfordringer det jobbes med?
 - b. Hvilke områder prioriteres?

5. Som norsk representant, kan du si noe om hvilke motivasjoner Norge har for økt forsvarssamarbeid i NORDEF?
 - a. Hvordan kombineres dette samarbeidet med medlemskap i NATO?

6. Siden Norge nå har formannskap i NORDEF, kan du si noe om prioriteringene for samarbeidet det kommende året?

Interview with Norwegian bureaucrat and Norwegian Lieutenant Colonel

Punkt 1: Motivasjon for samarbeid

1. Som norsk representant, kan du Trond si noe om hvilke motivasjoner Norge har for økt forsvarssamarbeid i COPA CAPA?
2. Ole, kan du si noe om hvilke motivasjoner Norge har for økt digitalt forsvarssamarbeid?

Punkt 2: Faktorer for samarbeid

3. Etter deres vurdering, hva vil dere si er de viktigste faktorene for Nordisk forsvarssamarbeid på cyberforsvar?
4. I den første årlige rapporten til NORDEFECO blir tillit nevnt som en viktig faktor for samarbeidet. I senere rapporter nevnes det at det er viktig å bygge tillit til hverandre for å videreutvikle samarbeidet. Etter deres vurdering, hvordan preger tillit samarbeidet?

Punkt 3: Samarbeid i praksis

5. NORDEFECO er kjent for å kombinere NATOs smart defense og EUs pooling and sharing, kan dere utdype hvordan et slikt forsvarssamarbeid foregår rent praktisk? (I COPA CAPA og innenfor cyberforsvar.)
6. Ut ifra deres mening som norske representanter, hvordan kan tillit bygges i NORDEFECO, rent praktisk?

Punkt 4: Relasjoner mellom landene i samarbeidet

7. Ut ifra deres forståelse, hvordan er relasjonen mellom de nordiske landene i COPA-CAPA samarbeidet?

Telephone interview, April 11th 2018

**Interview with Norwegian Senior Staff Officer in the Norwegian Cyber
Defense Division**

1. Hva er din nåværende rolle i cyberforsvaret?

2. Hvordan foregår samhandling mellom det norske cyberforsvaret og lignende avdelinger/etater i andre land?

3. Kan du si noe om trusselbildet i Norge nå, med tanke på cybertrusler?
 - a. Hvor viktig anser du internasjonalt samarbeid for å kunne lykkes i å sikre landet mot disse cybertruslene?

4. Hvordan samarbeider cyberforsvaret med forsvarsdepartementet om etableringen av et sterkt og robust cyberforsvar innenfor NORDEFECO-rammeverket?

5. Hvor langt har Norge kommet i etableringen av et cyberforsvar, sammenlignet med andre nordiske land?

Interview with Finnish bureaucrat

Motivation for cooperation

1. As a previous Finish representative working with COPA CAPA in NORDEFECO, can you elaborate on the motivation Finland has for increased defense cooperation within the capability sector?

2. Because cyber defense is under the COPA CAPA division, do you know the motivation for why Finland is seeking closer Nordic cooperation on cyber defense?

Central elements for cooperation

3. Based on your opinion, what are the most central elements for Nordic cooperation on cyber defense?

4. In the first annual report of NORDEFECO, trust is being mentioned as an important element for the cooperation. In later reports, it is mentioned that it is necessary to build trust to each other, in order to further develop the cooperation. Based on your understanding, how important is trust for this cooperation?

5. If trust is important, based on your understanding as a previous Finish representative, how should one best build trust in NORDEFECO, in practical terms?

Relations among the countries in the cooperation

6. Based on your understanding, how are the relations between the Nordic countries in NORDEFECO?
 - a. Do Finland have stronger relationship with one or two of the Nordic countries?

7. One Norwegian representative mentioned that more dialogue between the Nordic countries in the capability sector is needed. From your experience, are there any relevant forum for discussion and dialogue on capability issues?
 - a. How important is dialogue to build trust?