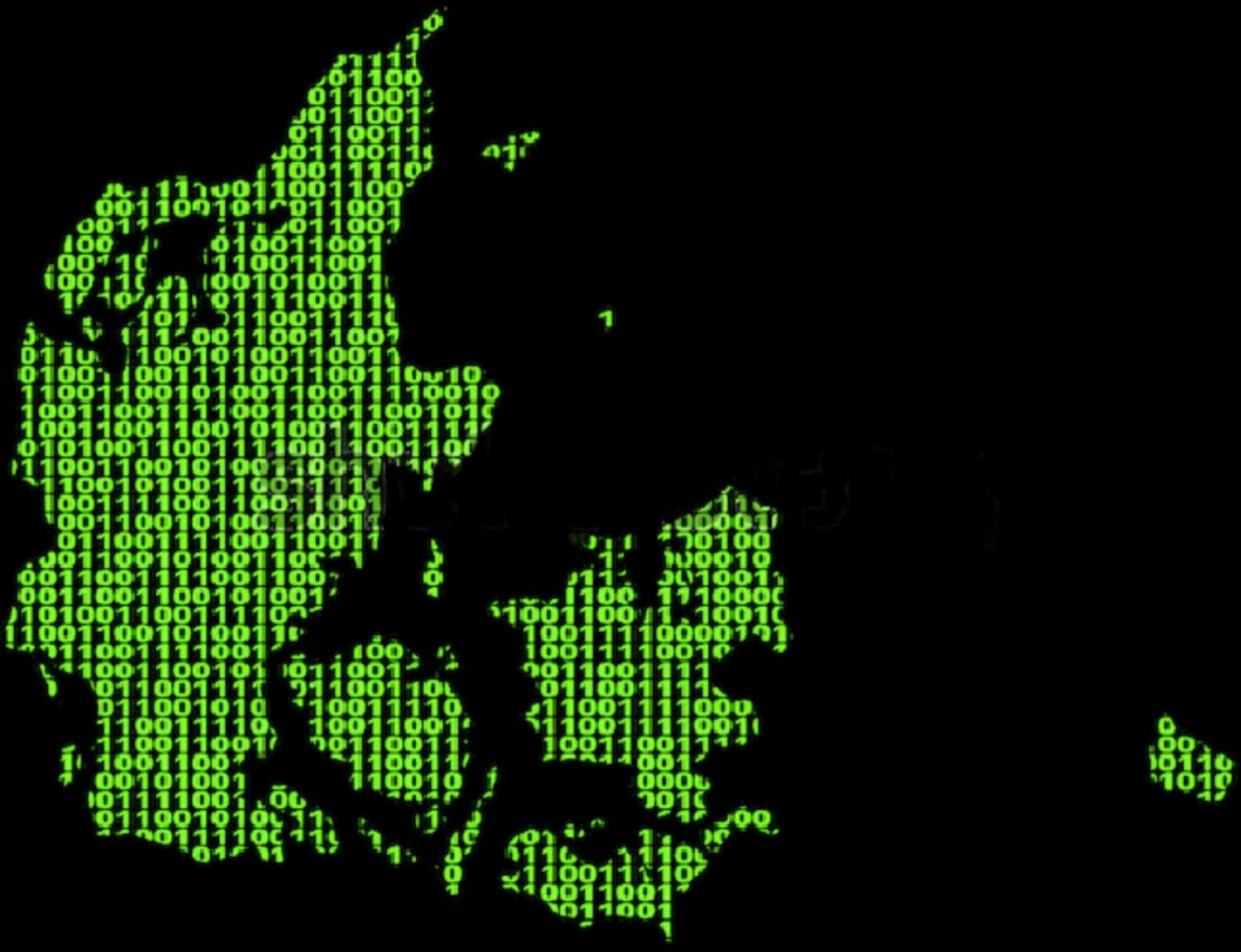
Small states in cyberspace:

A case study of Danish cybersecurity policy in the EU and NATO

Fadi Assi, Jacob Brink Hansen, Jacob Munch Jensen and Jens Lie Stokbro



MASTER THESIS: DEVELOPMENT & INTERNATIONAL RELATIONS SUMMER 2020

Aalborg University, Supervisor: Søren Dosenrode

1 Abstract

With Denmark as its case, this thesis joins an already exciting conversation in the social sciences about the increasing challenges small states face in cyberspace. The thesis explores Denmark as a small state in relation to NATO and the EU. Collectively, the evidence gathered in this thesis explores the undefined role of small states in the realm of cyberspace and proves that cyberspace contains new security issues and dynamics in the international system. Small state issues are often not accounted for in conventional studies on cybersecurity. In an attempt to cover some of these issues, this thesis will explore Danish cybersecurity strategies paying special attention international cooperation on cybersecurity. The thesis discovers that Denmark in the globalized cybersecurity sphere has multiple options and challenges. Denmark has, however, been passive in defining a balance between NATO, the EU and domestic policies that have seen Denmark dismiss opportunities in both organizations. Though neither NATO nor the EU can guarantee Danish cybersecurity, NATO and especially the EU provide an array of initiatives through which Denmark can compensate for its relative weakness by cooperating on expertise and intelligence sharing, capacity development and emergency response entities to cyberattacks, but due to a high domestic political risk for the Danish government of backing referendums on lifting opt-outs on the ASFJ and Defence, Denmark has been reluctant to pursue the possibility of engaging in deep EU cooperation on cybersecurity.

KEYWORDS: *Cybersecurity; Small State; Denmark; NATO; The EU; Cyberpolicy; Danish AFSJ and Defense opt-outs; Alliances; International Institutions; Norm-building; Cyberspace*

2 Acknowledgments

Firstly, we would like to thank our supervisor, Dr. phil. Søren Dosenrode of the Faculty of Social Sciences at Aalborg University. Søren, with his open door and insightful mind, was a great contribution to our work when we needed guidance. Søren allowed us to make this our project whilst keeping us on track and helping steer us towards the target when we were deviating from the course. Secondly, we would like to thank The Danish Foreign Policy Society for the collaboration. We want to send a special thanks to the employees of The Danish Foreign Policy Society for their guidance and openness.

We would further like to extend a special thanks to Lise-Lotte Terp, Jakob Gudiksen, Ulrik Pram Gad and Jeppe Teglskov Jacobsen, who, at an early stage of our project, helped us narrow and develop our project idea. In addition, we would like to thank Egon Kidmose, Postdoc, from The Technical Faculty of IT and Design at Aalborg University for helping us getting a technical insight into the subject and Lene Wacher Lentz, Assistant Professor at the Faculty of Social Sciences at Aalborg University for giving us an insightful introduction to the legal aspects of our subject. Our meetings and correspondences with all six have been instrumental for the way we have chosen to conduct our thesis.

We would likewise like to thank all experts and politicians, who were involved in the project through official and unofficial interviews helping us getting the best overview possible on a complicated issue; Thanks to Martin Lidegaard, Claus Hjort Frederiksen, Michael Aastrup Jensen, Christel Schaldemose, Pernille Weiss, Karen Melchior, Niels Fuglsang, António Esteves Martins, Thomas Wulff and Christian Friis. We would like to thank all for their input and participation in our project and for validating the data.

Furthermore, we would like to acknowledge each other for providing each other with unyielding support, good mood and encouragement throughout the process. Finally, we would like to thank our families and friends for their support throughout our many years of studying and especially during the challenging times of writing this thesis.

Our accomplishments would never have been realized without all the support we have had.

Thank you!
Fadi Assi, Jacob Brink Hansen, Jacob Munch Jensen and Jens Lie Stokbro

3 Table of Content

1 Abstract 1
2 Acknowledgments 2
3 Table of Content 3
4 Abbreviations 4
5 Introduction 6
6 Methodology 9
6.1 Structure of the thesis 9
6.2 Research method 10
6.3 Choice of theory 15
6.4 Applying small state theory 18
6.5 Data 20
6.6 Validity and reliability 25
6.7 Research design 27
7 Theory 28
7.1 Small states 28
7.2 Defining small states 29
7.3 Developing a theory of small states 32
7.4 Criticism of the theory 37
8 Background of the analysis 39
8.1 Historical overview 39
8.2 Conceptual framework of issues in cyberspace 43
9 Analysis 54
9.1 NATO cooperation - The Danish cybersecurity guarantor? 54
9.2 EU cybersecurity cooperation 67
9.3 Danish reluctance to engage in closer EU cooperation 87
10 Conclusion 103
11 Perspective and evaluation 108
12 Bibliography 110

4 Abbreviations

- AFSJ – Area of Freedom, Security and Justice
- ASEAN – Association of Southeast Asian Nations
- CCDCOE – Cooperative Cyber Defence Centre of Excellence
- CERT-EU – Computer Emergency Response Team for EU Institutions, bodies and agencies (EU's CSIRT)
- CFCS – Center for Cyber Security (the Danish national CSIRT)
- CFSP – The Common Foreign Security Policy of the EU
- CIDCC – Cyber and Information Domain Coordination Center (PESCO project led by Germany)
- CISA – Cybersecurity and Infrastructure Security Agency
- CRRTs – Computer Rapid Response Teams (PESCO project led by Lithuania)
- CSDP – the Common Security and Defence Policy of the EU
- CSIRT – Computer Security Incident Response Team
- CTIRISP – Cyber Threats and Incident Response Information Sharing Platform (PESCO project led by Greece)
- CyOC – Cyberspace Operational Centre
- DDA – Danish Defense Agreement
- DDIS – Danish Defence Intelligence Service
- DIIS – Danish Institute for International Studies
- EC – European Commission
- EDA – European Defence Agency
- EEAS – European Union External Action Service
- EIS – Europol Information System
- ENISA – European Union Agency for Cybersecurity
- EU – European Union
- EU CAIH – EU Cyber Academia and Innovation Hub (PESCO project led by Portugal)
- EUCO – Council of the European Union
- EUMS – European Union Military Staff
- Europol – European Union Agency for Law Enforcement Cooperation
- IOCTA – Europol's Internet Organised Crime Threat Assessment
- IR – International relations
- IT – Information technology
- J-CAT – Europol's Joint Cybercrime Action Task force

- JHA – Justice & Home Affairs
- MN CD2 – Multinational Cyber Defense Development
- NATO – North Atlantic Treaty Organization
- NAC – North Atlantic Council
- NCIRC – NATO Computer Incident Response Capability
- NCISS – National Cyber Information Security Strategy
- NIS – Network and Information Security
- PESCO – Permanent Structured Cooperation
- TEU – Treaty of the European Union
- TFEU – Treaty on the Functioning of the European Union
- UN – United Nations
- US – Unites States

5 Introduction

> *"In the cyber world, we are still on Thucydides' island of Melos; where the strong do what they want and the weak acquiesce." (Ilves, 2013)*
> *- Toomas Hendrik Ilves, Estonian President 2006-2016*

This was how Estonian President Toomas Hendrik Ilves described the issues faced by small states in cyberspace during a lecture at the Fletcher School at Tufts University on September 26, 2013. In 2007, during Ilves's presidency, Russian-sponsored hackers conducted a series of cyberattacks on an array of websites belonging to Estonian institutions, such as the parliament, banks, ministries and media (Tamkin, 2017). As one of the most severe cyberattacks ever conducted, the attack rendered governmental communication, online banking and media broadcasting nonfunctional for weeks (McGuinness, 2017). Having vital consequences for Estonia, the attack marked a new era of cybersecurity (Crandall & Allan, 2015; Hansen & Nissenbaum, 2009, p. 1169).

As a fellow small state, Denmark, like Estonia, faces externals threats to its cybersecurity from great powers such as Russia and China (Danish Defence Intelligence Service, 2019b; Interview Claus Hjort Frederiksen, 06.04.2020, 4:00-4:40). Being one of the most digitized countries in the world, Denmark falls victim of tens of thousands of cyberattacks on a daily basis (R. E. Rasmussen, 2018), and cyberattacks have arguably become a new normality (Finkielman, 2019, p. 25). According to Demchack of the US Naval War College, consolidated democracies lose between 1-2% of their GDP yearly from cyberattacks and digital corporate espionage (Danish Defense Committee, 2019, 49:00-50:15). In Denmark, especially the so-called NotPetya attack against the shipping company Mærsk with an estimated loss of between 1.5-1.8 billion DKK (approximately 201-241 million €) caught much media attention (Jyllands-Posten, 2018), while the Danish Ministries of Foreign Affairs and Defence are periodically targeted (Centre for Cyber Security, 2017, p. 3).

In addition to the attacks conducted against Denmark itself, the consequences of cyberattacks often spill over across national borders: Due to small states' reliance on globalized and digitized supply chains, industrial control systems and critical infrastructure, modern, small state societies contain many potential digital weak points (Woodcock & Stapleton-Gray, 2011, pp. 2–3), and an attack conducted against e.g. Swedish power plants or South European shipping control systems would likely have grave consequences for Denmark as well (Centre for

Cyber Security, 2019, pp. 2, 8; Interview Thomas Wulff 24.04.2020, 27:30-28:00). As President Ilves dramatized during his lecture at the Fletcher School, in the realm of cyberspace, the small and weak are at a considerably disadvantage to the great and strong (Burton, 2013, p. 224; Guang, 2020, p. 162; Ilves, 2013).

Contrary to the great power focus of much international relations theory, the field of small state theory has proven valuable in addressing small states' struggles for security (Neumann & Gstöhl, 2006, p. 10). According to small state theorists, small states looking to make up for their relative weakness vis-à-vis great powers can do so by entering into alliances, by gaining international institutional influence and by building and altering international norms (Dosenrode, 1994; Handel, 1990; Ingebritsen, 2002; Krasner, 1981; Rothstein, 1968; Thorhallsson, 2012; Thorhallsson & Wivel, 2006; Vital, 2006). Serving as the Danish guarantor for security in a narrow sense (Danish Defence Intelligence Service, 2019a; Ministry of Foreign Affairs of Denmark, 2018a, p. 11; Nissen et al., 2020, p. ix), NATO has recently begun developing its cybersecurity policy (Brent, 2019), whilst the EU, through its Network and Information Security directive, has laid the groundwork for EU member state legislation on cybersecurity (NIS Directive, 2016, p. 2; The Danish Government, 2018, p. 14), and developed strong member state cooperation on cybersecurity through the Common Security and Defence Policy and Europol (Europol, n.d.-c; Trimintzios et al., 2017, p. 9). As such, NATO and the EU may provide Denmark with the possibility of utilizing its existing alliances and institutional memberships in order to make up for its relative weakness in cyberspace.

While some research on small states in cyberspace has been conducted (e.g. Areng, 2014; Burton, 2013a; Crandall & Allan, 2015; Guang, 2020; Hughes & Colarik, 2016; Janczewski & Caelli, 2016; Rivera, 2015; Woodcock & Stapleton-Gray, 2011), only little case study research on how issues of cybersecurity affect specific small states has been done (Burton, 2013; Crandall & Allan, 2015; Guang, 2020). In 2013, Burton showed the potential of applying small state theory to cybersecurity policies when he explored how New Zealand improved its cybersecurity through the scope of alliances, institutions and norm-building (Burton, 2013). The field of small state cybersecurity studies was further developed in 2015 when Crandall and Allan investigated Estonia's role in establishing cybersecurity norms through its NATO membership (Crandall & Allan, 2015), and in 2020 when Guang similarly focused on Singapore's ability to create cyber norms through ASEAN (Guang, 2020, p. 169).

Prior to this thesis, however, no small state theoretical research has been con-

ducted on Danish cybersecurity policy and cooperation. Similar to Estonia, Denmark is a member of both NATO and the EU, but whereas Estonia fully partakes in most aspects of the EU cybersecurity cooperation, Denmark, with its opt-outs on Defence and Area of Freedom, Security and Justice (AFSJ), does not (Nissen et al., 2020, p. ix). This leaves Denmark in a unique position among those states, which have both EU and NATO memberships. With this uniqueness and the lack of prior research in mind, this thesis will apply Burton's promising small state theoretical focus on alliances, international institutions and norms to the case of Danish cybersecurity policies and cooperation in NATO and the EU in order to address a knowledge gap in the developing field of small state studies in cyberspace. To do so, the thesis has put forth the following research question:

From a small state perspective, how can the Danish state compensate for its relative weakness in cyberspace through EU and NATO cooperation, and why does Denmark not engage in deep cooperation with the EU on cybersecurity?

6 Methodology

The following chapter will delve more deeply into the methodology of the thesis. It will discuss the structure of the thesis, and why the thesis has chosen to base its research on a case study whilst discussing the possibilities and limitations of this choice. Subsequently, the chapter discuss the choice and application of theory followed by the qualitative deductive reasoning of the thesis. Further, the methodological considerations of the choice of data and data collection will be discussed. Finally, all these sections will be summarized into the comprehensive research design of the thesis.

6.1 Structure of the thesis

The following section will shortly give an overview the different chapters throughout the thesis and briefly discuss their contents, structure and relevance to answering the research question.

In 5. "**Introduction**" the paper will give a brief presentation of research field from both political and scholarly points of view and outline the case that will be examined. Further, the small state theoretical perspective applied in cyberspace will be presented to delineate the knowledge gap, which the thesis will attempt to address, as well as establishing the research question the thesis.

In 6. "**Methodology**", it will be discussed how the thesis intends to find answers to the research question by presenting the research methodology. In this chapter, the structure of the analysis will be presented, followed by a methodological discussion of the possibilities and limitations of a case study as the chosen research method. Further, the chapter will illuminate the choice and application of theory and discuss the qualitative deductive reasoning of the thesis. Subsequently, a section will present the methodological considerations of choice and validity of data processed in the thesis as well as considerations of limitations. Lastly, a final research design will be presented, which builds on all the methodological considerations presented previously in order to present a short outlining of how the thesis intends to answer its research question.

In 7. "**Theory**", the paper will introduce the small state theory, which will serve as an analytical framework and toolbox for the exploration of Danish cybersecurity policy and cooperation. Initially, a section will give a historical outline of the scholarly field of small state theory, which have been developed through the last six decades. Then, the theory chapter will attempt to provide a workable definition of what a small state is and how small states may be distinguished from great powers in the international system. Further on, the chapter will build

a theory of small state behavior in international relations drawing special attention to *alliances*, *international institutions* and *norms* before finally presenting a set of issues to the application of the small state theoretical perspective in general and to issues of cybersecurity.

In 8. "**Background of the Analysis**", the objective is to create fundamental knowledge that the analysis will be built upon. Firstly, a historical section will present how Denmark has found itself in conditions common for small states as well as Danish engagement in NATO and the EU. Secondly, a conceptual framework for security issues in cyberspace will be presented in order to address essential terms and consideration deemed vital for the understanding of security issues in cyberspace and the ensuing analysis.

In 9. "**Analysis**", the thesis will have the overall aim of answering the research question. The first two parts of the analysis will illuminate how Denmark can compensate for its relative weakness in cyberspace through NATO and the EU respectively by examining their cybersecurity initiatives beginning with NATO followed by the EU. The third part of the analysis is built upon the findings in the previous sections and will examine why Denmark does not engage in closer EU cooperation. It will investigate Denmark's own cybersecurity initiatives as well as domestic and external reasons for Danish reluctance to engage in deep EU cooperation on cybersecurity matters.

In 10. "**Conclusion**" the thesis main findings will be discussed to answer the research question.

In 11. "**Perspective and evaluation**" a brief reflection on the thesis will be presented. It will briefly evaluate on academic contributions, theoretical and methodological considerations as well as limitations posed upon the process of writing the thesis because of the outbreak of a global pandemic.

In 12. "**Bibliography**" a list of the all the references utilized in the thesis will be shown.

6.2 Research method

6.2.1 Choosing the research method

This section aims to discuss the different methodological approaches this thesis could use to address the research question; *From a small state perspective, how can the Danish state compensate for its relative weakness in cyberspace through EU and NATO cooperation, and why does Denmark not engage in deep cooperation with the EU on cybersecurity?*, with the ambition of outlining the reason behind using a case study as the methodological framework of the thesis.

This section will address the strengths and weaknesses of different social science research methods with a special focus on the possibilities and limitations that a case study approach provides.

Swanborn argues that the research question as well as specific conditions of influence over data determine if conducting a case study is a useful research method (Swanborn, 2010, pp. 24-25). Swanborn further argues that the research question is the methodological point of departure and suggests that the question determines either extensive research designs or intensive research designs (Swanborn, 2010, p. 2). Yin stresses similar considerations when a researcher is deciding which research method to use. He suggests it is important to consider the following three conditions:

> "*(a) the type of research question posed, (b) the extent of control an investigator has over actual behavioral events, and (c) the degree of focus on contemporary as opposed to historical events.*" (Yin, 2009, p. 8).

When addressing the first condition (a), it is possible to categorize different types of research questions: "[…] *'who', 'what', 'how much' 'where', 'how,' and 'why', questions."* (Yin, 2009, p. 9). Furthermore, Yin argues that it is helpful to separate these questions into two different categories with the first (1) encompassing 'what', 'where', 'how much', and 'who' questions and the second (2) with 'how' and 'why' (Yin, 2009, pp. 9–10). Though generally agreeing with Yin, Swanborn, however, suggests adding a third (3), *predictive* category of research questions that have a "[…] *format of 'what will happen' questions*." (Swanborn, 2010, pp. 28-29).

The first (1) category of questions shares the similarities of connoting *exploratory* or *descriptive* studies, often intending to develop a hypothesis for further examination. Usually, it is helpful to use either a survey or an archival analytical method to approach the first category of research questions (Yin, 2009, p. 9). Contrary to the first category, the second (2) category of questions connotes *explanatory* studies. These research questions aim at explaining changes by investigating the linkage of the altering of behavior and data over a longer period. These research questions are commonly approached in social science with a historical, experimental or case study method (Yin, 2009, pp. 9-10). In the third (3) category, Swanborn argues that data and historical events can be used to generate predictions as to what will happen in the future (Swanborn, 2010, pp. 28-29). As this thesis has an explanatory research question, Yin would thus suggest applying a historical, experimental or case study method.

Further, it is suggested to examine "[…] *(b) the extent of control an investigator has over actual behavioral events and (c) the degree of focus on contemporary as opposed to*

historical events." (Yin, 2009, p. 9). These two conditions are considered concurrently as they are mutually interfering when settling on the correct research method to use. Generally, a historical approach would have none to very little control over the behavioral events being studied, seeing as, by the nature of the study, it is essentially a research conducted of events that have taken place. In contrast, an experimental method is only focused on contemporary events, and as a method, it requires the investigator to have control over the actual behavioral events. In an experiment, the investigator must be able to control and directly manipulate its empirical data (Swanborn, 2010, p. 2).

The case study resembles mostly the historical approach rather than the experimental one as it uses similar techniques and data as the historical method, e.g. documents, speeches and policy-papers. Though a case study may focus on historical events, the case study method is most useful when applied with a greater focus on contemporary events (Yin, 2009, p. 11). This is how the case study method can be distinguished from the historical method, seeing as the former may supplement its historical sources of evidence with contemporary observation, while also enabling the investigator to interview persons of interest in the events being studied (Swanborn, 2010, pp. 35-36).

The intent of the discussion above is to outline the differences between these three methodological approaches. However, such a discussion may have the consequence of oversimplifying how and when the different methods should be applied in a study. It should be addressed that there are various similarities and overlapping elements between the different methodological approaches, yet the reason behind diverse categories of social science methods is grounded in the acknowledgment that they hold distinguished features (Yin, 2009, pp. 11). Moreover, this leads the thesis to discuss why it has chosen a case study approach rather than one of the other methods presented above.

Though this study has already presented its two-fold research question, which belongs to the (2) second category with explanatory '*how'* followed by a '*why*' questions, it should be considered if the thesis could have utilized a different approach in using a first (1) category question. The thesis could have chosen a research question such as, 'What are the Danish cybersecurity capabilities, and how many times has cybersecurity legislation changed?' or 'How many operational cybersecurity initiatives have been started in NATO and the EU, what are their responsibilities, and how many EU cybersecurity initiatives has Denmark not participated in because of its opt-outs on Defence and AFSJ?' These are arguably legitimate research questions to pose and fit closely with the content this thesis proposes to investigate.

The strengths of choosing such research questions would be that the findings would be precise and somewhat indisputable. The researcher could for instance use an archival analytical approach to address such research questions, and such research would be effective in describing and exploring what Danish cybersecurity policies have been developed and which initiatives and operational institutions Denmark has engaged in through the EU and NATO. Yet, a study built around such exploratory research questions cannot answer *how* or *why* its findings are happening (Rennison & Hart, 2018, p. 437). The exploratory research could work as a foundation for further investigation, which would include an explanatory angle on the exploratory conclusions of the thesis. Still, this leaves the question of why this thesis chooses an explanatory research question.

Because this thesis seeks to analyze the reasoning behind Danish cybersecurity policies in NATO and the EU, the thesis considers it crucial to conduct explanatory research. This is, however, not to be mistaken with the understanding that this thesis does not find exploratory research useful. In fact, an essential part of this thesis is arguably exploratory as a part of the thesis seeks to *describe* NATO and EU cybersecurity initiatives, entities and responsibilities as a foundation for the utilization of the small state theoretical perspective to *explain* how the Danish state can compensate for its relative weakness in cyberspace through NATO and EU cooperation, and why Denmark has been reluctant to engage in deeper EU cooperation on cybersecurity.

Having chosen to conduct an explanatory study, this leads the thesis to consider Yin's following two conditions "[…] *(b) the extent of control an investigator has over actual behavioral events, and (c) the degree of focus on contemporary as opposed to historical events."*(Yin, 2009, p. 9). This thesis will utilize policy-papers, legislation and other documents as main sources, and it will also investigate past events similar to the historical method, leaving out an experimental approach. However, the study differs from a historical approach in two ways: Firstly, its main focus is on contemporary events as it attempts to explain the current Danish cybersecurity cooperation with NATO and the EU. The fact that Danish cybersecurity cooperation is the main unit of analysis also favors a contemporary research approach since cybersecurity is a field that has changed rapidly during the last decade and keeps accelerating (Ismail, 2019). Secondly, though the thesis will mainly utilize policy-papers and legislation documents, it will also attempt to gather its own empirical data, mainly through interviews with experts, authorities and politicians. Thus, the thesis will have somewhat control over the presen-

tation of the actual, behavioral events it is studying, by its choice of persons of interest to interview and how these interviews are conducted. Swanborn argues that this way of utilizing open-source documents as well as interviews is a common and useful way of conducting a case study (Swanborn, 2010, p. 12).

Having outlined why the thesis chooses to conduct a case study, the following section aims to illuminate the weaknesses and strengths of a case study method.

6.2.2 Case study

Swanborn suggests a case study is a research of a social phenomenon,

> "[…] *in which the researcher focuses on process-tracing: the description and explanation of social processes that unfold between persons participating in the process, people with their values, expectations, opinions, perceptions, resources, controversies, decisions, mutual relations and behaviour, or the description and explanation of processes within and between social institutions*." (Swanborn, 2010, p. 12).

Moreover, Yin defines a case study as: "*An empirical inquiry that investigates a contemporary phenomenon within its real-life context."* (Yin, 2009, p. 13). The strength of a case study is its unique ability to investigate a phenomenon in-depth and in great detail (Flick, 2009, p. 134). In much the same way, Lijphart argues that in conducting a case study, researchers have the possibility of intensively exploring the selected case even if only limited resources pertaining to the case exist (Lijphart, 1971, p. 691). This makes the case study method ideal to use when investigating a phenomenon in its real-life context but leads to a weakness of generalization. According to Flick, if one chooses to concentrate solely on one case, case studies are an unfit method for making broad scientific generalizations (Flick, 2009, p. 134). As such, creating new theories on the basis of a case study can prove difficult. The case study is, however, considered an ideal method to use for applied science, using a theoretical generalization or framework, which, in this thesis, is the small state theoretical perspective, allowing the research to focus on the case, rather than improving a generalization (Lijphart, 1971, p. 692).Therefore, a prior developed theoretical proposition will be applied as a tool to guide data collection and analysis, which is useful in a qualitative deductive case study research (Kennedy, 2018, p. 49-52).

When conducting a case study, one has to choose between a single- or multiple-case study (Swanborn, 2010, p. 19) and whether the case study should be *holistic* or *embedded* (Yin, 2009, p. 50). Single-case studies are those case studies which explore only one main unit

of analysis (only one case), while multiple-case studies have several main units of analysis (several cases) (Swanborn, 2010, pp. 20-21). Single-case studies are justifiable under certain conditions: *"(a) a critical test of existing theory, (b) a rare or unique circumstance, or (c) a representative or typical case, or where the case serves a (d) revelatory or (e) longitudinal purpose*." (Yin, 2009, p. 52), while multiple-case studies should follow a design fit for replication and comparison (Yin, 2009, pp. 53-59).

This thesis intends to utilize the single-case study design as the rationale of the thesis is arguably that of condition (b). Though the thesis wishes to reflect upon the applicability of the small state theoretical perspective in cyberspace, the main focus will be on the unique case of Denmark's circumstances and its ability to compensate for its relative weakness in cyberspace. In addition, Denmark's opt-outs on Defence and AFSJ arguably leave Denmark in a unique circumstance in its ability to secure itself in cyberspace (Folketinget, 2019a, 2020), also favoring a single-case study approach. As the thesis wishes to address in-depth Danish cybersecurity capacities rather than comparing an array of different states' capacities, the single-case study approach is arguably the most rational approach for this study.

In addition to choosing between single- and a multiple-case study methods, it is also important to address whether the case study is of a *holistic* or *embedded* nature (Yin, 2009 p. 50, 59). A holistic case study is characterized as a study with one unit of analysis, whereas an embedded case study entails providing several subunits of analysis in order to address the main unit (case) (Yin, 2009, p. 50). This study is an example of an embedded single case study as multiple subunits of analysis will be provided in order to address the singular main unit of analysis. In order to address the main unit, i.e. Danish cybersecurity policies and cooperation, the thesis has three subunits. The two first subunits are Denmark's ability to compensate for its relative weakness in cyberspace through a) NATO; and b) the EU. In order to explain why Denmark does not engage in deep cybersecurity cooperation in the EU, a third subunit will investigate c) how the relationship between foreign and domestic affairs influences Danish cybersecurity policies and political maneuverability.

6.3 Choice of theory

This section aims at illuminating why the thesis has chosen small state theory as a theoretical framework for the thesis. In order to do so, it will discuss whether traditional IR theories developed before the age of digitization are applicable in explaining cybersecurity issues. It will present a variety of scholars that have utilized different traditional IR theories in cyberspace as

well as discussing their strengths and weaknesses before addressing why this thesis utilizes the small state theoretical perspective.

Kremer & Müller address the overall applicability of traditional IR theories in cyberspace in their book 'Cyberspace and International Relations: Theory, Prospects and Challenges (2014)'. They argue:

> "*As state leaders respond to the overwhelming insecurities posed by this globally open and unregulated 'substrate,' the international system's topology will be changing as well. A rising "Cyber Westphalian" process likely to take 20 years to solidify will define the accepted characteristics of national jurisdictions in cybered terms*." (Kremer & Müller, 2014, p. v).

With this in mind, it can be argued that as cyberspace is changing, so will the theories that try to explain it. However, this prophecy of a 'Cyber Westphalian' has not materialized yet and thus it is still feasible to utilize IR theories to test and modify their ability to explain security issues in cyberspace (Kremer & Müller, 2014, pp. v-ix).

In their book 'Conflict in Cyber Space: Theoretical, strategic and legal perspectives' (2016), Friis & Ringmose argue that the nature of cyberspace and its continued potential development is the main factor for determining if traditional IR theories are successful in explaining conflicts and security issues in cyberspace (Friis & Ringmose, 2014, pp. 1-4). Since cyberspace was built to be open and easily accessible while being globally interconnected, it is simultaneously under little control, anarchic in nature and insecure, which proves difficult to handle for state policy-makers and security experts (Friis & Ringmose, 2016; Kassab, 2014). It could be argued that this description of cyberspace as insecure and anarchic in nature does not differ notably from a realist understanding of the international system (e.g. Waltz, 1979), and would suggest realism having explanatory powers in cybersecurity issues as well. The first scholarly discussion around cybersecurity originating in the 1990s also centered around a realist argument regarding the possibility of cyberwar and how this could materialize (Langø, 2016). Moreover, several modern scholars have attempted to apply (neo)realism to explain cyberspace conflicts as well (Craig & Valeriano, 2018; Kassab, 2014; Libicki, 2009; Rivera, 2015; Saltzman, 2013). The strengths of the (neo)realists' approach are arguably that they address how power between states is transferred into and how this affects cyberspace (Craig & Valeriano, 2018; Rivera, 2015).

However, the realist school has been criticized for extensively focusing on the possibility of cyberwar and military conflict in cyberspace, which evidence proves little risk of, and therefore implicitly neglecting many cybersecurity issues, as realists reject to see non-military attacks and conflicts in cyberspace as security issues (Christensen & Liebetrau, 2016; Deibert & Rohozinski, 2010; Hansen & Nissenbaum, 2009). This leads to the notion that the extensive focus of the realist approach on cyberwarfare is "[…] *basically, old wine in new bottles.*" (Eriksson & Giacomello, 2006, p. 229). Another IR theoretical approach that has been applied to understand cybersecurity issues is the Copenhagen School's, mainly constructivist, securitization framework (Buzan et al., 1998), which Hansen & Nissenbaum (2009) set out to utilize. Though, contrary to the realists, they were able to include non-military issues in cyberspace, they provided little policy advise besides arguing that cyberspace has been securitized.

Further, scholars have shown how neoliberalism can be applied to the field of cybersecurity by analyzing how institutions can be useful in facilitating intergovernmental cooperation on cybersecurity (McDowell et al., 2014), and how realism fails to address the great role of non-state actors in cyberspace (Cavalty et al., 2007, p. 32). However, neoliberalism has been criticized for being contradictory in its view of cybersecurity as it advocates free accessibility of data and ideas, which, in turn, renders cyberspace less controllable and more anarchic (Parks & Schwoch, 2012, p. 35). This focus on free accessibility, inarguably leaves neoliberalism less able to address fundamental disagreements on the freedom of information between great powers such as China, Russia and the US (Crandall & Allan, 2015, p. 361; Gong & Yang, 2017, p. 9).

Because of the unique nature of cybersecurity, both realism, liberalism and constructivism have proven to have their respective pros and cons when applied to different cases and problem fields. As a theoretical perspective that incorporated thoughts from all three, small state theory has shown to be rather straightforward in its application to the field of cybersecurity. However, it is important note that much literature on small states predates the digitized age (e.g. Baker Fox, 1959; Handel, 1981/1990; Krasner, 1981; Rothstein, 1968; Vital, 1967/2006). Yet according to Burton, issues in cyberspace seem to be an extension of typical small state issues where security is always of high priority (Burton, 2013). Because of this, though acknowledging that cyberspace is a new frontier of security studies, whose issues traditional IR theories have yet to fully explain (Kremer & Müller, 2014, pp. v-ix), the thesis adopts small state theory as it includes aspects of both (neo)realism, (neo)liberalism and constructivism.

As a small state, Danish cybersecurity policy-making is today facing similar issues as those dealt with in much small state literature, i.e. how the small state can guarantee its security through alliances, how it can gain influence through international institutions and how it can affect norms as means to secure its sovereignty and political maneuverability. Combining different theoretical perspectives, the small state framework allows for greater variety of approaches and explanations of patterns of small state behavior in order to provide policy advise for small state actors. This is the main reason why the thesis applies a small state theoretical perspective.

6.4 Applying small state theory

Little research has been done on small states in terms of cybersecurity. Burton (2013) lists three options for how a small state can compensate for its relative weakness in cyberspace: *Alliances with greater powers* (neorealist)*, to seek institutional influence* (neoliberal) and *to be norm entrepreneurs/ norm builders* (constructivist) and argues there are general problems if they are applied separately in the field of cybersecurity. The problem for examining alliances in cyberspace according to Burton is establishing a collective cyberdefence, exemplified with NATO and the tensions with Russia over the Estonian cyberattack in 2007 (Burton, 2013, p. 221). Institutional cooperation similarly has proven difficult to apply in cyberspace as well with Burton highlighting the UN Security Council as an example of strategic rivalries between member states posing problems (Burton, 2013, p. 221). As for international norm building, it mirrors the strategic rivalries between leading global powers, showing that globally accepted cyber norms are not realistic to accomplish because of the disagreement on freedom of information between Russia and China and the West (Burton, 2013, pp. 222–223).

Despite of the difficulties each theoretical perspective poses, Burton finds their respective explanatory ability valuable for the specific problems of small states in cyberspace. Burton points to alliances being important for a small state in cyberspace as the 13 most internet-dependent countries are small states, including Denmark, with cyber vulnerabilities increasing concurrently with digitization and finding that small states do not have the political, diplomatic or economic tools to respond to global issues in the same way as a larger one has with the borderless threat of cyberattacks (Burton, 2013, pp. 223–224). In terms of institutionalism and norm-building, Burton points to the security interests and outlook having been enlarged for small states in the realm of cyberspace. For solving cybersecurity issues, small states are therefore in need of institutional influence for the development of capabilities and knowledge with

greater powers and to cooperate with other small states to be successful cyber norm-entrepreneurs (Burton, 2013, pp. 236-238).

For these reasons, this thesis finds Burton's theoretical small state perspective, with a focus on alliances, international institutions and norms, useful for examining the case of Denmark in cyberspace. These three theoretical focal points will be applied when found relevant, will help the thesis to answer its research question and to embrace an array of possibilities for Denmark to make up for its relative weakness in cyberspace, and provide explanations of the way Denmark conducts itself in the realm of cyberspace.

6.4.1 The deductive method of reasoning in qualitative research

This case study will be conducted using a deductive methodological reasoning. In short, this entails how a study approaches the relationship between theory and data (Kennedy, 2018, p. 49). Generally in social science, the deductive method is described to: "[…] *start with a theory, which is narrowed to a testable hypothesis. Data is then collected and analysed to see if the hypothesis can be confirmed and the theory, substantiated."* (O'Leary, 2007, p. 2). The inductive method in social science research, on the other hand, is defined in the following way:

> *"Inductive reasoning works the other way around and starts with a question, followed by data collection. Data is then explored for regularities, patterns and themes that lead to generalizations and eventually theory.* […] *In the end, the goal is to put forth findings and even theories that help explain what's really going on."* (O'Leary, 2007, p. 2).

The debate of which method is the best to use can be boiled down to if data should lead the research in an unbiased way or if the context surrounding the data is of as great importance as the data itself. In most cases, it is acknowledged that cycles of both deductive and inductive types of reasoning are used as there can be a need to modify theory after data analysis or confirm the theory with further data (O'Leary, 2007, pp. 2–3). Kennedy (2018) stresses that the deductive and inductive reasonings are ideal types and commonly overlap. She argues that conducting qualitative research usually creates two conflicting challenges: Firstly, she argues that a generally accepted premise of scientific research is that it has to refer to previous insights, whilst secondly, she argues that theoretical preconceptions may hamper exploration of new knowledge because theories do not consider the constant altering and reshaping of the meanings and actions of social life (Kennedy, 2018, p. 49).

With this suggestion in mind, this thesis has no intention of forming a new theory or generalization as the inductive method suggests. According to Kennedy, the deductive way of 'testing' a theory is usually connected to quantitative research in which a hypothesis can be formed and tested for validity. However, in deductive, qualitative research, the researcher is more specifically concerned with utilizing the theory as an analytic framework or tool when processing the data of the study (Kennedy, 2018, pp. 49-52). The latter is what this thesis intends to do. It will apply the small state theoretical perspective as guidance and an analytic approach to investigate Denmark's relative weakness in cyberspace by looking at the case of Danish cybersecurity policy and cooperation.

This thesis will primarily employ a qualitative method with a focus on interpretivist, rather than positivist, approach. However, it will also utilize quantitative data when found appropriate, but the primarily qualitative approach will be key in understanding the decision-making and policy-creation (Yin, 2011) of cybersecurity initiatives. This is the reason why the deductive, qualitative method has been chosen, rather than the more quantitative, data-driven method of reasoning. However, the thesis does accept the premise suggested by Kennedy (2018) of cycles of both methods of reasoning influencing the process as it is difficult not to let data somewhat influence the theoretical grounds of the research or let theory influence the analysis of data.

As mentioned previously, the case study method does not immediately invite scientific generalizations as the case study is usually the investigation of a single entity (Lijphart, 1971, pp. 691-692). Thus, it is also difficult to use for scientific generalization as the variables cannot be controlled and that it has more variables of interest than data points. This means that interpretation and the context of the case is a vital part and turning point of the case study. Using a mainly qualitative research means employing weigh on the interpretations of a research data. This is a method used commonly by scholars that utilizes a case-study method (Flick, 2018, p. 7).

6.5 Data

The following section will outline the choice, validity and limitations of data and data collection processes of the thesis. It will include methodological considerations of using policy-papers and documents as the main source of evidence as well as the considerations behind gathering its own data through interviews with politicians and experts.

6.5.1 Choice of data and data collection

In choosing the data utilized throughout its research, the thesis has been guided by its theoretical framework. In analyzing Danish cybersecurity policies and cooperation with NATO and the EU, the thesis relies heavily on policy-papers, legislation, strategies and scholarly literature on both cybersecurity issues and EU and NATO initiatives. According to Schreier (2018), when choosing data for a case study, it is favorable to use different methods of data collection (Schreier, 2018, p. 95). As much of the thesis deals with political matters, the thesis has furthermore been conscious of collecting data representative of an array of different political opinions. Most clearly, this can be exemplified in the thesis's own attempt at gathering empirical data through interviews with an array of politicians of different parties in the Danish parliament and the European Parliament.

When collecting data, there are two approaches, the natural and the elicited. The natural approach is based on the idea that researchers should take an interest in the world as events unfold, without the involvement of researchers, their independent practices, constructions or methods (Flick, 2018, p. 4). The role of the research should simply be the recording of events, activities and interactions, and based on those findings, the researcher makes her or his analysis. This opposite to this is the elicited approach, in which the researcher participates through e.g. interviews, and interactive observations to produce the material necessary for the analysis (Flick, 2018, p. 4). In order for the thesis to conduct its analysis, it is argued that it needs some degree of control over its data and data collection.

Therefore, the thesis has chosen to take an elicited approach to data collection. The reason for this is that the thesis seeks to understand and analyze a problem that is, at this time, a newly developing field of research and a highly complicated political matter that is, at least somewhat, clouded in secrecy. Thus, the thesis will conduct interviews with experts and politicians, and through these interviews, the authors will be able to question the interviewees in-depth. The elicited approach further allows the authors to make a determination of what information is relevant to this case and what is not. This is particularly needed as research studies of small states in cyberspace is still a developing research field. Moreover, no small state theoretical research of Denmark as a small state in cyberspace has been conducted, thus offering new knowledge to the developing field.

6.5.2 Interview design

In exploring how the Danish state can compensate for its relative weakness in cyberspace through greater cooperation with NATO and the EU and discussing why Denmark has chosen

not to engage in deep cooperation on cybersecurity with the EU, the thesis is dealing with political choices. To get a glimpse into the decision-making processes that go behind these political choices, the thesis has followed an elicit approach to data collection by conducting a series of interviews with members of the political elite, such as the spokespersons on defense of different Danish political parties as well as some of the Danish members of the European Parliament. Interviews are thus integral to the research of the thesis and its methodology.

An interview can be described as a conversation, which has been planned and designed in advance by researchers (Brinkmann, 2013; Yin, 2011). Whereas normal conversations tend to happen naturally, generally following their own flows, interviews are conducted according to a design. These designs can vary greatly in their degree of structuring, but no matter how loosely an interview is structured, an interview will always be conducted according to a predetermined design (Brinkmann, 2013, p. 45). In the following, the thesis will discuss interviewing techniques and describe the methodological framework applied in the interviews conducted.

In qualitative research, a common distinction can be drawn between *structured*, *semi-structured* and *unstructured* interviews (Choi & Roulston, 2018, p. 233). Generally speaking, the more unstructured an interview is, the more it will resemble an everyday conversation, whereas interviews that follow a very tight structure typically follow the same logic as a survey (Choi & Roulston, 2018, p. 233). Typically, *structured* interviews follow a very formalistic logic, and the interviewer is encouraged to read the question in the exact same, standardized way to every respondent, whilst following a clear-cut interview chronology (Brinkmann, 2013, pp. 19–21). Resembling verbal questionnaires, structured interviews allow for clear comparisons across respondents and may even provide quantifiable data, but they do not give the interviewer the chance to gain additional insight by asking follow-up questions (Brinkmann, 2013, p. 20). By following a very tight structure, the interviewer thus misses out on the ability to build additional knowledge through more conversational elements of the interview (Mikecz, 2012). A less tightly structured interview design thus seems more valuable.

At the other end of the spectrum is the unstructured interview. While the interviewer does have clear aims for the research he or she is conducting through the use of unstructured interviews, the aim of this kind of interview is to provide little structure to allow the respondent as much room as possible to put forth their perspectives and ideas (Edwards & Holland, 2013, p. 29-30). In this type of interview, flexibility of the interviewer is essential, and the interviewer should be able to adjust the aims of interview accordingly if the respondent

brings forth unexpected themes. Often used in anthropological studies and oral history, the unstructured interviews are useful in highlighting particularities and individual worldviews (Edwards & Holland, 2013), but the interviewer also runs the risk of not getting an answer to the issues she or he is looking to address (Brinkmann, 2013).

The middle ground between the two is the *semi-structured* interview, which this thesis intends to make use of. Though having a structured set of issues the interviewer wishes to discuss with the respondent, the semi-structured interview also allows the interviewer to enter into a dialogue with the respondent and ask follow-up to build additional knowledge (Brinkmann, 2013). As many of the respondents relevant to this study belong to the political elite, especially the ability to ask follow-up questions may prove fruitful. When interviewing (political) elites, who are used to being interviewed, the interviewer runs the risk of receiving only generic, "public relations" answers if follow-up questions and "re-calibrations" of the interviews through rephrasing of questions are not allowed (Mikecz, 2012, p. 484). Conducting very tightly structured interviews would thus not allow follow-up questions in order to 'break through' the "public relations" answers. On the other hand, as the study at hand does have a set of particular issues it wishes to address through its interviews, some degree of structure is needed to make sure that the issues get addressed properly. As such, a very loose structure would not be advantageous either.

The thesis has taken contact to Danish politicians in parliament as well as elected officials in the European Parliament from all political parties represented.[1] The reasoning behind this has been to attempt to achieve as broad a representation of political opinions as possible and to counter bias in the research by choosing persons of interest grounded in their political position. The thesis has attempted to gain as many different opinions as possible, as it assumes this strengthens the research findings in the end. However, it has proven difficult to gain contact with representatives from across all political parties. It would have favored the thesis if all political parties were represented, yet it is out of the control of the researchers when people of interest do not intend to engage in an interview. To make sure these political opinions will be represented in the thesis, the researchers will attempt to find statements in the media or other sources to gain knowledge of the political parties that did not engage in an interview with the researchers, though the thesis acknowledges that this is not optimal as it denies the researchers the ability to ask its specific questions.

[1] See appendices A and B.

As this thesis has interviewed politicians, the conversation has been structured around five main questions being the following: 1) Which political initiatives do you think have been important for Danish cybersecurity? 2) Do you have any propositions as to how Denmark could strengthen its cybersecurity? 3) Do you regard closer cooperation within the EU on cybersecurity as favorable, and do you see Denmark's opt-outs on Defence and AFSJ as obstacles for further cooperation? 4) Do you see possibilities for closer cooperation on cybersecurity in NATO? 5) More broadly, do you regard European cooperation on security matters as an alternative or a compliment to NATO? The aim of asking these overall questions is to gain an insight into the political aspects of the main research question of how Denmark can compensate for its relative weakness in cyberspace through NATO and EU cooperation and why Denmark does not engage in deep cooperation with the EU on cybersecurity.

As semi-structured interviews, there have been some differences to the order in which the questions have been asked according to the interviewees' answers and certain follow-up questions outside of the five questions stated above have been asked to get the interviewees to elaborate on certain points made during the interviews. Furthermore, some politicians have asked for written questions before engaging in an interview, giving them different circumstances for the interview as they have had time to prepare. Moreover, one politician wished only to answer in written form[2]. The researchers have also utilized some of the opinions articulated by the first interviewees as a foundation for follow-up questions to the following interviewees to create deeper understanding of the political differences and similarities. The order of the interviews has been a result of the availability of interviewees. While these points may not be ideal for comparing the responses of the politicians interviewed, the researchers have attempted to gain as much knowledge as possible from each interview, which has, in turn, influenced the researchers' follow-up questions as they became aware of the different political opinions. To somehow counter this issue, the researchers have attempted to contact interviewees after the initial interview with follow-up questions if this was found relevant. Further in preparation for each interview, the thesis has utilized policy documents and statements in the media by the interviewees or their respective political parties as supportive sources.

[2] See appendix E.

6.5.3 Limitations of data

Initially, the thesis had the intention of collecting its own empirical data through interviews with experts and politicians. As the topic is, in itself, a new field of research that deals with military intelligence norms, information is often cloaked in secrecy, which limits public availability. In an attempt to counter this issue, the thesis has been successful in gathering insights into these norms by interviewing the CFCS. Due to the worldwide outbreak of Covid-19 early into the process of conducting the research, the ability of the thesis to follow its initial plan of gathering data was severely hampered, as it could not attend conferences or utilize its established networks to gain contact to as many persons of interest as planned. Nonetheless, the thesis did manage to interview politicians and experts in the field. Similarly, due to Covid-19, Aalborg University was shut down during the outbreak and libraries across the country were inaccessible. This has made the thesis rely almost entirely on digital libraries and data, limiting access to especially older scholarly literature.

6.6 Validity and reliability

Four tests are commonly utilized in social science methods to reflect upon validity of data and research design: *1) Validity-construction, 2) Internal Validity, 3) External validity* and *4) Reliability* (Yin, 2009). The four tests are described in the following way:

> *"**Construct validity**: establishing correct operational measures for the concepts being studied. **Internal validity**: establishing a causal relationship, whereby certain conditions are shown to lead to other conditions. as distinguished from spurious relationships. **External validity**: establishing the domain to which a study's findings can be generalized. **Reliability**: demonstrating that the operations of a study-such as the data collection procedures can be repeated. with the same results* […]*"* (Yin, 2009, p. 33).

Each test has different purposes and different means. The first test and research tactic of constructing validity occurs in the data collection and composition phase of the research. The second test of internal validity takes place in the data analysis phase of the research and the third test of external validity takes place in the research design phase of the research. The final and fourth test of reliability takes place in the data collection phase (Yin, 2009, p. 33)

In order to construct validity, the thesis has considered the relationship between the main unit of analysis and the collection of data (Drost, 2011, p. 116). The thesis has followed

Yin's proposition of utilizing multiple sources of evidence (policy-papers, strategies and scholarly literature) and key informants (politicians and experts) to construct a chain of evidence (Yin, 2009, pp. 34-35) to examine the main unit of analysis of the thesis, i.e. Danish cybersecurity policy and cooperation.

The second test of internal validity is a concern for causal or explanatory case studies, where the investigator's aim is to explain a causal relationship between events. A case study involves an inference whenever an event cannot be directly observed, where the basic questions of source criticism and consideration of rival explanations have to be considered. In doing so, Yin argues that the researcher can establish internal validity when the tactics of pattern-matching can be used (Yin, 2009, p. 35). This thesis is especially conscious of internal validity in the processing of data in the analysis as the thesis considers a variety of conditions, before suggesting a causality and further reflects upon the validity of such a causality.

The third test of external validity deals with knowing whether the findings of a study can be generalized beyond the immediate research (Drost, 2011, pp. 120–121). The problem of external validity in case study research has been criticized for having a poor basis for generalizing. However, Yin argues that case study research can be used to generalize within the theoretical framework of which the case was chosen. Yin argues that the utilized theory will help to identify other cases to which the results are generalizable. When the possible generalizable case(s) have been identified, a replication of the original findings has to be applied, and then a wider generalization can be used (Yin, 2009, pp. 35-36). This thesis has, however, argued that it is researching a unique case; thus, the findings of the thesis prove little ground for broad generalizations. However, the thesis will reflect upon the ability of the small state theoretical perspective to explain Danish cybersecurity policy and cooperation and may prove as a piece in the puzzle of generating a broader understanding of the ability of the small state theoretical perspective to explain cybersecurity issues.

The fourth and final test of reliability is to be sure that an investigator, conducting the same case study, following the same procedures at a later stage, would come to the same results. This test requires documentation of the procedures followed, making every step as operational as possible and making sure that the methods of the research could be audited (Drost, 2011, pp. 106-107). In order to construct reliability, the thesis has attempted to be precise and comprehensive in its methodological approach and has chosen a theoretical framework to guide the collection and processing of data, which would increase the possibility of other researchers'

abilities to mirror the thesis steps and come to somewhat similar results. However, some elements, such as the authors' preconceptions as well as including themselves in its semi-structured interviews may arguably have affected the data collection of the thesis as well as its interpretation of it.

6.7 Research design

Drawing on the previous sections of the methodology chapter, this section will condense the main points of the methodology chapter into the finalized research design of the thesis. According to Flick, "[…] *a good research design is the result of reflection, planning and clear decisions about the steps of constructing a design* […]" (Flick, 2007, p. 14). In order to answer the research question, i.e. *from a small state perspective, how can the Danish state compensate for its relative weakness in cyberspace through EU and NATO cooperation, and why does Denmark not engage in deep cooperation with the EU on cybersecurity?,* the thesis has decided to utilize a single embedded case study method in its exploration of the main unit of analysis, being Danish cybersecurity policies and cooperation. Additionally, three subunits a), b) and c) have been put forth, i.e. Denmark's ability to compensate for its relative weakness in cyberspace through a) NATO; and b) the EU, and further explore c) how the relationship between foreign and domestic affairs influences Danish cybersecurity policies and political maneuverability. To address the main unit and the subunits, the qualitative, deductive method of reasoning will be utilized as the small state theoretical perspective with a focus on alliances, institutions and norms serves as the framework for conducting the analysis and guides the choice and processing of data. With an elicited approach, the thesis has attempted to gather its own data through interviews and meticulous use of primarily digital scholarly literature and empirical data as the thesis has been limited from certain aspects of conventional resource gathering due to Covid-19. Being a unique case, the thesis is limited from and will not propose broad generalizations of small states in cyberspace (Lijphart, 1971, p. 686), though it will reflect upon the applicability of the small state theoretical perspective on the case. With the validity test and all the methodological considerations in mind, the thesis contends that this research design will be valid for answering the research question.

7 Theory

This chapter will present the small state theoretical framework the thesis seeks to utilize in its analysis. First, it will provide an overview of the different streams of scholarly small state literature before defining the understanding of a small state applied in this thesis. Further on, the chapter will build a theory of small state behavior in international relations drawing special attention to *alliances*, *international institutions* and *norms* before finally presenting a set of issues to the application of the small state theoretical perspective in general and to the field of cybersecurity.

7.1 Small states

Within the field of international relations, over the centuries, much attention has been drawn to great power politics. Interestingly, though, despite the high focus on great powers, only very few of the almost 200 sovereign states in the world can arguably be defined as great powers (Handel, 1981/1990, p. 30). As such, the majority of the world's states do not fall into the great power category, and, according to certain scholars, all but a dozen or two can be characterized as so-called 'small states' (Neumann & Gstöhl, 2006, p. 3).

In her seminal work 'The Power of Small States: Diplomacy in World War II' (1959), Baker Fox explores the power, influence and challenges of small states in the international system. With a focus on the World War II diplomacy of six European small states, Baker Fox explored how small states managed to cope with ongoing pressure from the great powers at a time when small states faced huge security risks (Baker Fox, 1959). Although she acknowledged the unique military superiority of great powers vis-à-vis small states (Baker Fox, 1959, p. 2), Baker Fox went against the general great power bias found in much literature on international relations at the time (Handel, 1981/1990, p. 3) by emphasizing how small powers could gain influence and resist threats. Baker Fox thus lay the groundwork for much scholarly research on small states in the ensuing decades (Neumann & Gstöhl, 2006, pp. 9–10).

Though the small state perspective has a state-centric focus in which uneven (military) power relations is a fundamental premise, the study of small states in international relations cannot solely be anchored within realist thinking. Instead, as is evident from the many different takes on the theory since its inception some sixty years ago, small state theory(ies) builds on an array of different theoretical schools of thought (Knudsen, 2002, p. 182). Broadly speaking, small state studies can be grouped into three streams. The first stream deals with the

general question of a small state's foreign political choices to assure its survival, whilst the second and third streams have tended to focus on policy formation and questions of recognition and self-determination respectively (Knudsen, 2002, p. 182). Falling within the first stream are authors like Baker Fox (1959), Vital (1967/2006) and Rothstein (1968), who wrote their works in the decades following World War II when international relations theory was generally centered around the realist and neorealist schools of thought (Neumann & Gstöhl, 2006, p. 16).

As the attention of international relations scholars began to shift in the 1980s, and neoliberal institutionalism started to challenge the prevalent thoughts of neoliberalism, studies of small states received new attention by neoliberal scholars. Krasner (1981) studied how Third World states attempt to increase their power through manipulation and creation of international institutions, norms and arrangement, whilst Katzenstein (1985) explored how European small states developed and secured their economies through the 1970s and 1980s at a time of crisis, international pressure and accelerating economic change. Further, starting in the 1990s, the deeper integration of European small states in the European Union has attracted new scholarly attention to small state studies (Dosenrode, 1994; Thorhallsson, 2000; Thorhallsson & Wivel, 2006), touching on the relationship between international cooperation and self-determination.

Through the turn of the millennium, small state studies increasingly turned to the constructivist research agenda, and since then, European small states have remained focal points for small state research (e.g. Crandall & Allan, 2015; Ingebritsen, 2002). With a focus on the Scandinavian and Nordic states, Ingebritsen discusses how small states can build and reshape international norms, in this case about the environment, conflict resolution and economic reallocation from rich to poor, to gain influence in international relations (Ingebritsen, 2002, pp. 12-13, 22). A more recent addition is Crandall & Allan (2015), whose analysis on Estonia's effort to build security norms in cyberspace stands out as one of few case studies discussing cybersecurity from a small state perspective (see also Burton, 2013; Guang, 2020).

7.2 Defining small states

Before attempting to build any theory of small states, one must first define what is meant by a small state. Making one singular, clear-cut definition of what a small state is, has, however, proven immensely difficult (if not downright impossible), as different scholars have vastly different takes on the matter, whilst others have simply refrained from attempting to define the term (Handel, 1981/1990, p. 31). Still, what most scholars tend to agree on is that small states share a fundamental relative weakness vis-à-vis great powers, which stands as a focal point of

small state theory(ies) (Knudsen, 2002, p. 184). Consequently, the simplest definition of a small state is to simply view them as those states that are not great powers (Thorhallsson & Wivel, 2006, p. 652).

This negative definition, however, gives no actual description of great or small states, so it does not help in defining either of the two. Instead, one must put up certain parameters to define small states. Among these parameters, military might, population size, geography, GDP, the scope of the state's interests and whether the state is developed or underdeveloped are often used as denominators for categorizing a state on the spectrum between small and great powers (Handel, 1981/1990, pp. 52–53). Most scholars agree that, contrary to the great powers, a small state is generally preoccupied with ensuring its survival, and it is often said that a small state's foreign policy is largely governed by the policy of other, greater powers (Handel, 1981/1990, p. 4). The issue of survival is ever-present for small states because great powers, coalitions of small states and even a singular opposing small state can cause any small state considerable harm and threaten its existence (Handel, 1981/1990, p. 36).

On top of the question of military capabilities, population size is often a valuable tool in defining small states (Knudsen, 2002, p. 184). The cut-off point for the population of a small state is sometimes set at 10 or 15 million people for developed states and 20-30 million people for underdeveloped ones (Vital, 2006, p. 81), whilst other scholars set the maximum at the population of the Netherlands (Thorhallsson & Wivel, 2006, p. 6). Geographically, small states generally occupy a smaller territory than great powers. Due to their generally small size, small states tend to lack the necessary variety of resources to sustain themselves at any great length without external aid (Knudsen, 2002, p. 187). In certain cases, however, small states occupy a large area, which may also cause an issue. Even if a state occupies a large area with vast natural resources, the state's small population size creates a lack of human resources needed to protect its large borders. As such, even if small powers control a large geographic territory, the small population size makes the geographically large small states susceptible to attacks from the outside (Handel, 1981/1990, p. 71).

Notably, while geography plays an integral role in the conventional security of states, in cyberspace, this is not so. This is because, in cyberspace, a person from around the globe may be just as 'close' as your next-door neighbor. This raises the question if geography is even relevant to discuss in the case of cybersecurity. If one redefines what is meant by 'geography', the answer is arguably yes: As one of the most digitized states in the world, cyberspace spans across much of the Danish society (Finkielman, 2019, p. 25). Guang (2020) has

suggested that small states with large cyber landscapes and little manpower are much more vulnerable than great powers in cyberspace (Guang, 2020, p. 162). As such, cyberspace covers a vast 'area' that Denmark needs to protect with its limited amount of resources. In this way, Denmark's large 'area' within the realm of cyberspace may pose similar issues as those faced in the real world by Mauritania or Iceland, whose small populations in comparison to their large landmasses may prove insufficient to defend their boundaries.

Furthermore, while certain scholars focus on quantifiable criteria to distinguish small states from great powers, Rothstein argues that self-perception is important in setting great powers apart from the small:

> "*Any new definition should also take account of the fact that there is a psychological, as well as material, distinction between Great and Small Powers. The latter earn their title not only by being weak but by recognizing the implications of that condition. Thus, a Small Power is a state which recognizes that it can not obtain security primarily by use of its own capabilities, and that it must rely fundamentally on the aid of other states, institutions, processes, or developments to do so* (…)*"* (Rothstein, 1968, p. 29).

In much the same way, as small states and great powers are relational terms, proximity to a greater power may also affect the self-perception of certain states. This is particularly the case for countries like Canada and Mexico, themselves arguably not archetypes of small states, which just so happen to neighbor the US. To these states, their economically, militarily and population-wise vastly superior neighbor seems to dwarf their self-perception, leaving the two states feeling smaller than their economy, military and population would suggest on a global level (Handel, 1981/1990, p. 51).

Setting the perimeters of small states and great powers is a question of much discussion, and categorizing states is best done on a state-by-state basis. In its definition of a small state, this thesis combines Handel's criteria of a small state, i.e. a state with a small population size, small territory, high dependence on outside aid against external threats, a limited scope of interests and a strong support of international law (Handel, 1981/1990, pp. 52–53), with Rothstein's criteria of state self-perception (Rothstein, 1968, p. 29). With this definition, Denmark proper fits quite well into many of the criteria of a small state previously mentioned. With a population of some 5.8 million, a relatively small territory with limited natural resources, and a high degree of dependence on the global economy as well as external military support to ensure

the country's conventional security, Denmark is something of an archetype of a small state, as is also often evident in much literature on small states (Ingebritsen, 2002; Knudsen, 2002; Neumann & Gstöhl, 2006). Further, both Danish media (Bertelsen, 2018; Lykkeberg, 2017; Mouritzen, 2015), historians (Brammer, 1987; Midtgaard, 2005) and former Danish Minsters of Foreign Affairs (Lidegaard, 2020; Lykketoft, 2019) tend to perceive Denmark as a small state.

7.3 Developing a theory of small states

As shown, the small state perspective of international relations has spanned across an array of theoretical schools. Drawing on both realist, neoliberal and constructivist 'takes' on the small state perspective, the following section will attempt to 'piece together' a theoretical framework of small state behavior in international relations for further application in the analysis. The theory will primarily deal with how a small state can compensate for its relative weakness and gain political influence through *alliances*, *international institutions* and *norms* and which consequences their actions may have for their self-determination.

7.3.1 Alliances

As seen, small states are at an inherent disadvantage to great powers in terms of power. Both states pursuing neutral or 'non-aligned' policies and states looking to enter into alliances with a great power have been explored by scholars. Looking at states which pursued neutral foreign policies during World War II, Baker Fox (1959) found a set of patterns related to small states and their ability to withstand pressure from the great powers. Her research showed that the greater the number of great powers interested in the small state, the greater maneuverability of the small state, and that small states had the possibility of exploiting two or more competing great powers' interests in the small state to their own advantage by achieving economic and military gains (Baker Fox, 1959, pp. 184-185). According to Baker Fox, would-be neutral states thus have the ability to play on their neutrality to gain from either side if more great powers see an interest in it.

While Baker Fox focused on how would-be neutral small states maintained and could gain through their positions, others have explored why and how certain small states, fearing for their safety and aiming to enhance their political influence, find themselves drawn to entering into alliances with greater powers to make up for their relative weakness (Handel, 1981/1990; Rothstein, 1968). In his work, Rothstein (1968) explores the concerns of small states when entering into alliances with great powers. According to him, two types of alliances

can be distinguishes from one another: "*A military alliance emerges from the perception of a threat which cannot be met with one's own resources. A political alliance emerges from the perception that a situation exists which can be exploited by an alliance*." (Rothstein, 1968, p. 52). In Rothstein's view, such alliances are inherently dangerous for the small state as the small state runs the risk of losing sovereignty and becoming a satellite of the great power if it chooses to ally with a vastly superior power (Rothstein, 1968, p. 61). He argues that a small state should only ally itself with vastly superior powers if it senses immediate, military danger. If, instead, the small state enters into the alliance with the aim of achieving political goals, the small state should seek to ally itself with a less powerful great power, so as not run the risk of heavy great-power intervention (Rothstein, 1968, p. 61). To Rothstein, alliances may prove valuable for small states attempting to achieve political goals.

As Rothstein points out, upon entering into alliances with greater powers, small states run the risk of losing at least some degree of national self-determination. Vital (1967/2006) makes a similar point:

> "*Of course, some small powers can—and in very many cases do—seek to offset their weaknesses by association or alliance with other powers, great and small. But where the quest for protection and insurance is successful a price must normally be paid in terms of sacrifice of autonomy in the control of national resources and loss of freedom of political maneuver and choice.*" (Vital, 1967/2006, p. 79)

However, where Rothstein points to the political advantages of certain alliances (Rothstein, 1968, p. 61), Vital stresses that alliances should only be sought during war-time or during great international crises as alliances are likely to be dominated by the greatest and most influential power during more peaceful times (Vital, 1967/2006, p. 84). This great power dominance would, in Vital's words, be 'disastrous' for the less powerful states, so in his view, the only true way for a small to assure its sovereignty and political maneuverability is by following a policy of non-alignment (Vital, 1967/2006, pp. 84–85).

According to Handel (1981/1990), these perceived dangers for small states posed by alliances with great powers were exaggerated through the course of the Cold War due to the USSR's dictation of treaties with the Baltic and eastern European states in the 1940s (Handel, 1981/1990, p. 122). In alliances made by *free choice* rather than by the great power's dictation,

Handel argues that issues posed to the small state's integrity and self-determination are secondary. The primary concern of the small state should rather be how the small state can reinforce the commitment of a great power to its interests, seeing as the withdrawal of aid by the great power might prove fatal for the small state (Handel, 1981/1990, p. 122). To him, the advantages of forming an alliance by *free choice* thus outweigh the risk for the small state of losing self-determination.

For small states, alliances can thus be a helpful tool in their pursuit of survival, but whereas certain scholars see alliances as giving small states a chance of achieving political goals outside of wartime (Handel, 1981/1990; Rothstein, 1968), others argue that small states should pursue non-alignment or neutrality if they wish to preserve integrity, political maneuverability and self-determination (Baker Fox, 1959; Vital, 1967/2006). As such, alliances, though commonly sought by small states seeking to compensate for their relative weakness by entering into coalition with others, are by no means without potential consequences to their self-determination and political maneuverability.

7.3.2 International institutions

Due to their relative weakness, small states have often sought international influence through international institutions. According to Krasner (1981) small states generally pursue an array of different goals, such as economic growth, security, international political equality and autonomy and independence (Krasner, 1981, p. 121). In this pursuit, international institutions provide a means to the small state's goals: "*By building and altering international institutions, rules, principles and norms, weaker countries can* […] *ameliorate the vulnerability imposed by their lack of national material-power capabilities* […]" (Krasner, 1981, p. 122). Krasner refers to this as 'meta-power'. This 'meta-power' behavior, he argues, can be valuable for small states trying to compensate for their relative weakness between themselves and the great powers: "*Relational power behavior accepts the existing rules of the game; meta-power behavior attempts to alter those rules*." (Krasner, 1981, p. 122). Thus, by changing the very rules and norms that govern international relations, small states can, in Krasner's view, persuade great powers to act to the small state's benefits.

Though Krasner concerns himself with Third World countries, more developed small states can also gain advantages by joining international institutions. Dosenrode (1994) suggests that western European small states, too, may find joining institutions advantageous to

their pursuit of security (Dosenrode, 1994, p. 245). To him, small states looking to secure themselves may find institutions useful: "*Small states will, as a matter of principle and as a result of their weakness, support the creation of regimes that bring some kind of order to the international system* […]."[3] (Dosenrode, 1994, p. 247). Like Krasner, Dosenrode further suggests that small states can join international institutions to (re)shape the international rules and norms that influence the small states, and by doing so, they also get the chance to articulate and promote their ideas and values (Dosenrode, 1994, pp. 246–247). Building on Rothstein and Vital's points that small states may wish to stay out of alliances unless absolutely necessary (Rothstein, 1968, p. 61; Vital, 2006, p. 79), Dosenrode argues that the same can be said for any other responsibility that may limit the small state's sovereignty (Dosenrode, 1994, p. 246). Therefore, as he points out, small states tend to prefer international institutions, which they can enter and leave as they please, to supranational solutions, which restrict their freedom (Dosenrode, 1994, p. 248).

For European small states, the EU has provided a forum through which they can gain influence. In the EU, Thorhallsson (2000) points out that small states tend to focus on the policy areas most important to them. They thus put great emphasis on their core sectors whilst paying minimal interest in political issues outside their sphere of interests (Thorhallsson, 2000, p. 13). In policy of high priority to the small states, Thorhallsson even argues that small states may have an advantage to the greater powers as they have an easier time stating their position in a clear manner (Thorhallsson, 2000, p. 48). Thorhallsson & Wivel (2006) see great possibilities for small states within the EU. In their view: "[…] *small states benefit the most from an international environment characterised by strong international institutions, they have an interest in continued and increasing effectiveness of EU policy-making*." (Thorhallsson & Wivel, 2006, p. 663) In their view, coalition building with other member states and namely the EU Commission is especially important, because greater states tend to work actively against a policy that only has a positive effect for others than themselves (Thorhallsson & Wivel, 2006, pp. 663-664). As such, as a forum with many small states, the two argue that the EU provides an arena for small states to work together on shared issues (Thorhallsson & Wivel, 2006, p. 664).

[3] Throughout the thesis, the terms "regimes" and "international institutions" are used interchangably. In contemporary IR literature, the term "institutions" has largely replaced "regimes" (Simmons & Martin, 2002, p. 328) .

7.3.3 Norms

As mentioned earlier by Krasner (1981) and Dosenrode (1994), international institutions offer small states a platform to affect and create norms. Thorhallsson (2012) has further investigated how small states gain organizational influence through the UN. In this analysis of organizational influence for small states, he sets up the two categories of qualitative factors that determine the ability for small states to influence the UN Security Council: the first category is the administrative competences in areas such as knowledge, initiative, diplomatic/coalition and leadership skills (Thorhallsson, 2012, pp. 159–160). The second category is the image of the state in the international system, hereby its perceived neutrality or reputation as a norm entrepreneur in particular policy fields. Thorhallsson highlights the importance of picking certain policy areas of focus and a small state's ability to present itself as more neutral than others (Thorhallsson, 2012, pp. 159–160). This suggests that small states have been effective in placing themselves as norm entrepreneurs in international institutions.

Finnemore and Sikkink's (1998) norm life cycle, which has become a fundamental theory of norm emergence in IR literature, has also been utilized by small state scholars, such as Crandall & Allan (2015). The norm life cycle consists of *1) norm emergence, 2) broad norm acceptance,* and *3) internationalization* (Finnemore & Sikkink, 1998, p. 6). The first phase requires a 'norm entrepreneur(s)' as the actor, who has strong notions about desirable behavior, and who usually calls attention and dramatize issues to convince a critical mass of states to embrace new norms, using organizational platforms (Finnemore & Sikkink, 1998, p. 9). In the second phase norm entrepreneurs socialize other states to accept norms, through forming a certain critical mass of states and then seeking a domino effect of convincing others. The second stage usually leads to the third stage where norms assume the status of an international recognized truism (Finnemore & Sikkink, 1998, pp. 7).

Scandinavian small states have been highlighted by Ingebritsen (2002) as particularly successful norm entrepreneurs. She points to certain distinct characteristics and factors as the reasons, including Scandinavia's peripheral position to larger European states, its dependence on natural resources leading to pragmatic policies and the prominence of social democratic institutions (Ingebritsen, 2002, p. 20). Ingebritsen uses Scandinavian states as an example of successful norm promotion, but also points to their limitations, describing their goals to be unsuccessful if they contest the interests of global powers such as the US, exemplified with environmental norms versus industrialization (Ingebritsen, 2002, p. 14-16).

As Ingebritsen does not cover much about how and why small states follows a norm-building foreign policy strategy, Goetschel (2011) seeks to fill this gap. He does so by investigating neutral European states as norm-builders and covers the realistic (how to stay out of conflict and survive) and idealistic (how to use ideas as justification of neutral policy) reasons to pursue a neutral norm building foreign policy (Goetschel, 2011, pp. 325–326). Goetschel recognizes that the realistic survival reasons to have a neutral position have passed after the end of the cold war and are not as relevant as the idealistic and normative reasons. He argues that the position of being neutral gives states the justification to promote norms, and small states will often do so in international organizations (Goetschel, 2011, pp. 323-325).

As much academic focus regarding norm-entrepreneur small states is centered around neutral states and the importance of seeming neutral as a norm entrepreneur, Crandall and Allan (2015) seek to fill the research gap of norm-building for non-neutral (or aligned) small states. They do so by examining Estonia as a small state in NATO in terms of cybersecurity policy. Using Finnemore and Sikkink's norm life cycle theory, Crandall and Allan argue that the reasons why non-aligned (neutral) states are successful in the third norm-building phase, are the same reasons that aligned states are not. However, Crandall and Allan argue that aligned states can be successful in the first phase of norm-building (norm-emergence) within international organizations as evident in the case of Estonia (Crandall & Allan, 2015, p. 363). Crandall and Allan argue that the use of NATO as an organizational platform has made it difficult for creating a common international understanding for cyber norms because it excludes Russia, whom Crandall and Allan find to be a critical partner of achieving the second phase of broad acceptance (Crandall & Allan, 2015, pp. 359–362). Crandall and Allan, though, find the case of Estonia to prove that small states can use the promotion of norms to create changes to increase their security environment. Furthermore, Crandall and Allan note that small states might be satisfied with their norm-promotion efforts to only reach the first stage as it leads to knowing that their preferred norms are accepted by their allies (Crandall & Allan, 2015, p. 363).

7.4 Criticism of the theory

One of the major critiques of small state theory, which the thesis has already touched upon, revolves around the issues of defining a small state. Nasra believes that small state theory has a problem with how to define small states in their behavior and their opportunities for influence (Nasra, 2010, p. 1). The problem that small state theory often finds itself in, is that there is no universal definition of a small state and therefore studies use different definitions. The small

state theory(ies) simply do not make a clear distinction between a state's relative perception of its smallness and quantifiable indicators of being small (Neumeyer, 2012, p. 33). This thesis cannot fully overcome this problem as the thesis cannot change the definition of past scholars. However, the thesis will make a definition that makes use of the most common variables (see "Defining small states").

Because of this issue with defining the different commonalities in small states, the list of foreign policy approaches taken by small states is often viewed as being too large to be useful and therefore often offers contradictory solutions (Long, 2017, p. 2). This problem gives small state theory(ies) a "[…] *lack of a common framework in which the numerous insights into single issues can be ordered, and an accumulation of knowledge can happen*." (Dosenrode, 1994, p. 251). This lack of a single consistent framework is a weakness in the small state theoretical perspective as it may result in contradictory explanations and a general incoherence. The thesis seeks to overcome this issue by actively specifying which scholars' points are being used at any given time throughout the thesis. Paradoxically, the ability of the small state theoretical perspective to draw on different strings of IR theories (e.g. Realism, Liberalism, Constructivism) is also its strength as it provides multiple angles, which can result in nuanced explanation and greater knowledge. Connecting this to cyberspace, it seems rather doubtful that all small states share common security challenges, which is arguably why different scholars draw on different aspects of the small state theoretical perspective in their works. The thesis intends to use especially Burton (2013) and Crandall & Allan (2015), as these have proven successful in explaining cybersecurity issues for small states.

8 Background of the analysis

This chapter is structured in two parts with a common objective of creating fundamental knowledge that the analysis will be built upon. Firstly, a historical section will present how Denmark has found itself in conditions common for small states as well as Danish engagement in NATO and the EU. Secondly, a conceptual framework for security issues in cyberspace will be presented in order to address essential terms and consideration deemed vital for the understanding of cybersecurity and the ensuing analysis.

8.1 Historical overview

This section intends to illuminate how Denmark, historically, has been considered and behaved as a small state. Furthermore, it will briefly describe Danish engagement in NATO and the EU.

8.1.1 Denmark before NATO and the EU: A neutral small state between great powers

Danish geography of controlling the entrance to the Baltic Sea has historically put Denmark in the interest of great powers. When examining Danish history from 1864 until the end of the World War II, it becomes evident that Denmark has behaved as a neutral small state. After losing the war against Germany in 1864, Denmark accepted its relatively small size to its large neighbor (E. S. Petersen, 2009). Thus, from then on, Denmark pursued to stay out of conflicts, which it was successful in during the World War I. Though this did not prevent Denmark from being invaded in the World War II, the neutral policy was somewhat reflected in Danish cooperation policy with its occupying neighbor state (Poulsen, 2009). After the war in 1948, the Danish Prime Minister Hedtoft stated:

> *"We [Danes] should not place our country in any block at all. We are a member of the United Nations and must here do our duty as a Nordic country. […] May I add that in my opinion it is not a Danish or Nordic interest to elaborate on the obvious contradictions between East and West. A final rupture between the great nations who came together to win the war will be a disaster for all of us - perhaps mostly for the Nordic."* (Kühle, 2008, pp. 248–249).

This shows that Denmark initially attempted to continue its strategy of non-alignment in the aftermath of the war.

8.1.2 Denmark in NATO

After World War II, Denmark's large neighbor Germany was no longer the main reason for Denmark's perception of being a small state. This, instead, now stemmed from a new bipolar world order shaped by the US rivalry with the Soviet Union. Denmark sought a closer security relationship with the US, even though this was not a position that Denmark deemed ideal (S. H. Rasmussen & Brunbech, 2009b). The closer relationship with the US involved Denmark as a founding member of NATO in 1949, a collective defense alliance between Denmark, the US and several Western European states (NATO, 2020c). Denmark joined NATO hoping to achieve some form of guarantee of its security from aggression (Wivel, 2014, p. 109).

Though Danish membership in NATO guaranteed its security, it also created new issues for Denmark. Denmark had to come to terms with altering its deep-seated strategy of neutrality and reluctance from entering greater power politics (Wilkinson, 1956, p. 394). This is perhaps one of the reasons why Denmark was renowned for being an ally with reservation and not fully committing to NATO's wishes. Denmark did not meet the US demand for military spending, refused to have nuclear weapons or NATO personnel deployed in Denmark, and neither did Denmark agree to having Danish troops permanently stationed outside of Danish territories (S. H. Rasmussen & Brunbech, 2009a). However, the Danish government permitted the US to build the Thule base in Greenland, while Prime Minister H.C. Hansen secretly gave permission to US deployment of nuclear weapons (S. H. Rasmussen & Brunbech, 2009a).

For Denmark, the primary goal of entering into NATO was to deter any possible aggression from the outside, with membership supported by both Danish politicians and citizens (P. V. Jakobsen, 2005, pp. 38–41). After the Cold War, Denmark has increasingly committed actively to NATO. Since 1991, Denmark has contributed to all major military interventions led by the US, e.g. Iraq, Afghanistan, Libya and Syria (Malmvig, 2019). However, recently, internal issues in NATO that may affect the global security landscape have arisen. In particular, these issues concern US President Trump's 'America First' policy, which questions US commitments to Europe (Kaufman, 2017, p. 251); the French President Macron's claims that NATO is becoming "brain-dead" (The Economist, 2019); and bilateral issues with Turkey (Yegin, 2019, p. 1).

8.1.3 Denmark in the European Union

In 1973, Denmark, together with Ireland and the United Kingdom (UK), joined the European Community (later the EU). Since then, the UK, which, as of 2020, however, is no longer a member, has been considered Denmark's most important ally in the Union (M. H. Petersen,

2018). The dynamic between the UK, Denmark and the EU has been described in the following way: *"If the European Union is a school class, Denmark and the UK have always been best mates sitting on the back row – Denmark as the younger, who didn't always abide by the rules, and the UK as the older, who tried to rewrite them."* (M. H. Petersen, 2018). Denmark can to some extent be understood as a reluctant member, though still a member, who values the possibilities of the European cooperation (Olesen, 2013).

However, when the European Community was reformed and the EU established with the Maastricht treaty in 1993, Denmark, in its referendum to ratify the treaty in 1992, voted no to include Denmark in this process of European integration (Krunke, 2005, pp. 339–340). As a result, Denmark renegotiated a separate agreement with the European Community, better known as the Edinburgh Agreement, which meant that Denmark got four opt-outs from the EU. Denmark held a second referendum in May 1993, which ended in a yes to the reamended treaty (Krunke, 2005, pp. 351–352). Through the Edinburgh Agreement, Denmark gained four opt-outs on the European Monetary Union, Union citizenship, the Justice & Home Affairs (JHA) and the Common Security and Defence Policy respectively (Krunke, 2005, pp. 343–345).

Denmark's opt-outs were created under different circumstances at a time where the structure of the EU was different from the structure known today. The opt-outs were structured according to the pillar structure created in the Maastricht treaty: Pillar 1: European Communities, Pillar 2: Common Foreign and Security Policy (CFSP), Pillar 3: Justice and Home Affairs (JHA) (EU-oplysningen, 2019). The Danish opt-outs are to this day still structured according to this pillar structure even though the three pillars were abolished with the Lisbon Treaty in 2009 (Fondation Robert Schuman, 2009, p. 1). The abolishment created a more complicated picture of Denmark's opt-outs to the EU, though the EU tried to compensate for this lack of clarity by incorporating them in the Treaty, Protocol 22 (TFEU, 2012, protocol 22). The legal foundation of the Danish opt-outs has a great impact on which initiatives Denmark can be a part of. The abolishment of the pillar structure meant that what was formerly known as the opt-out on JHA now became an opt-out on the AFSJ (see section five of the TFEU (TFEU, 2012, sec. 5).

The Danish opt-outs are defined in the Treaty on the Functioning of the EU (TFEU) protocol 22. Article 1 defines the opt-out on *Area of Freedom, Security and Justice* (AFSJ): "*Denmark shall not take part in the adoption by the Council of proposed measures pursuant to Title V [Area of Freedom, Security and Justice] Part Three of the Treaty on the*

Functioning of the European Union." (TFEU, 2012, protocol 22, article 1). Meanwhile, the defense opt-out is found in article 5: "*Measures adopted by the Council pursuant to Article 26(1), Article 42 and Articles 43 to 46 of the Treaty on European Union* […]" (TFEU, 2012, protocol 22, article 1). Something that should be noted is that not all defense matters are articulated in articles 26(1), 42 and 43-46 of the Treaty of the European Union (TEU): For instance the European Defence Fund (EDF)[4] is legally based in the EU's Industrial, Research, Techonology and Space policy, as such allowing Denmark to cooperate fully (Rynning, 2020, p. 4; TFEU, 2012, secs. XVII, article 173 & XIX, articles 182-183, 188).

A decision to remove the defense opt-out is a unilateral Danish decision. The seven parties behind the opt-outs made a political agreement, which entails that the opt-outs may only be changed or lifted through referendums. This requirement is a legal and not a political decision (Nissen et al., 2020, p. 20). Legally, a removal of the defense opt-out is not covered by Section 20 in the Danish constitution as a removal of this opt-out does not transfer any national sovereignty to the EU as the EU cooperation on defense is intergovernmental (Danish Constitution, sec. 20; Nissen et al., 2020, p. 20). However, a vote to remove the defense opt-out can find a legal basis in Section 42 of the Danish Constitution (Danish Constitution). The Danish opt-out on the AFSJ, however, would classify under section 20 of the Constitution as the AFSJ has been a supranational cooperation since the implementation of the Lisbon Treaty, and therefore removal of the opt-out would transfer sovereignty to the EU (European Values, 2014). The Lisbon treaty allows Denmark – after a referendum – to transform the AFSJ opt-out into an opt-in scheme meaning that Denmark could, on a case-by-case basis, decide which parts of the cooperation on AFSJ it would partake in. This was, however, declined in the Danish referendum in 2015 (BBC, 2015; European Office - Foreign Ministry n.d.).

Since the introduction of the defense opt-out in 1993 and until 2019, the opt-out was invoked in relation to 27 actions and initiatives (Nissen et al., 2020, pp. 19-20). Denmark first used the opt-out in 1996 in connection with the evacuation of European citizens and the last one recorded in 2019 was in September when Denmark opted out from Operation Atalanta in Somalia (Madsen & Sørensen, 2019, p. 3). From 1993 to September 2019, 1,400 legislative

[4] *"The European defence fund supports the cross-border cooperation between EU countries and between enterprises, research centres, national administrations, international organisations and universities. This applies to the research phase and in the development phase of defence products and technologies. It has 2 strands. Under the research strand, the EU budget will provide funding for collaborative defence research projects. Under the capability strand, the EU will create incentives for companies and EU countries to collaborate on the joint development of defence products and technologies through co-financing from the EU budget."* (European Commission, n.d.)

acts were implemented under the CFSP, of which Denmark had joined 1,211 (Madsen & Sørensen, 2019, p. 4). This means that since the introduction of the Maastricht treaty in 1993, Denmark has been unable to participate in approximately 13.5 % of all acts made within the CFSP. In addition to this, Denmark is not able to partake in any planning or decision-making in regard to the EU CSDP.

8.2 Conceptual framework of issues in cyberspace

This section will define and present an array of terms integral to the understanding of cyberspace. The section precedes the analysis as the thesis finds it vital to have a conceptualization of security in cyberspace when conducting a study centered around cybersecurity. The section commences with a definitional discussion of the term *security* in both a 'narrow' and a 'wide' sense before providing definitions of the term's *cyberspace, cyberattack, cybercrime* and *cyberwarfare.* Finally, the chapter will discuss 'narrow' and 'wide' understandings of security when applied in cyberspace in order to present the 'wide' conceptualization of cybersecurity utilized in this paper.

8.2.1 Security

Within international relations research, security studies have constituted their own subfield (Baldwin, 1995; Walt, 1991). This subfield received much attention in the decade following the dissolution of the Soviet Union and the end of the Cold War when a debate on security spurred among IR scholars. This section focuses primarily on this surge of academic writings in the aftermath of the Cold War as this period saw the rise of a discussion among scholars on whether Cold War understandings of security still applied (e.g. Allison & Treverton, 1992; Baldwin, 1995; Buzan, 1997; Buzan et al., 1998; Romm, 1993; Walt, 1991).

In their work *Security: A New Framework for Analysis* (1998), Buzan, Wæver and de Wilde distinguish between 'narrow' and 'wide' conceptualizations of security (Buzan et al., 1998, p. 2). 'Narrowly' speaking, security concerns issues within the military sector, regarding threats and the use of force, while a 'wide' understanding of security also concerns non-military phenomena, which may threaten states, companies and individuals (Buzan, 1997; Walt, 1991). Though acknowledging that other categorizations have been presented (Baldwin, 1995; Buzan, 1997; Williams, 2004), this chapter adopts the distinction between 'narrow' and 'wide' conceptualizations of security, which the following conceptualization will be based upon.

With a 'narrow' conceptualization of security, Lebow defines the study of security as anything related to "(…) *the prevention of superpower nuclear war*." (Lebow, 1988, p. 508). This originates from a Cold War, (neo)realist understanding of security with its emphasis on military and nuclear armament (Baldwin, 1995, pp. 123–126). This primacy of security in a military sense over non-military policy goals was stressed by Waltz. To him, military security was a precondition for the pursuit of other essential policy areas within the state: "*In anarchy, security is the highest end. Only if survival is assured can states safely seek such other goals as tranquility, profit, and power*." (Waltz, 1979, p. 126). This understanding of security as centered around survival through the ability of the military to secure the state was further exemplified by Mearsheimer: "*A state can have no higher goal than survival, since profits matter little when the enemy is occupying your country and slaughtering your citizens*." (Mearsheimer as cited in Allison & Treverton, 1992, p. 222).

Walt proposes that security studies are "(…) *the study of threat, use and control of military force.*" (Walt, 1991, p. 212). Walt acknowledges that security can concern areas outside the realm of military capabilities as he stresses that security studies may also include other entities as long as they deal with the likelihood and character of war, such as diplomacy, arms control and crisis management (Walt, 1991, p. 213). However, in his view, security cannot be disconnected from the instruments that either conduct or secure the state from war, so even if Walt has moved on somewhat from the almost one-sided focus on military capabilities, especially portrayed by Mearsheimer, he does not widen his scope much beyond the realm of military conflicts between states and war. When comparing Lebow's definition of security (Lebow, 1988, p. 508) with Walt's (Walt, 1991, p. 212), the field of 'narrow' security studies entails small disagreements on specific conceptualizations of security, though they share the understanding that security is inherently interlinked with military capabilities and the threat of war.

Contrary to scholars with 'narrow' understandings of security, 'wide' security studies constitute a more diverse scholarly field, which was stimulated by a general dissatisfaction with the Cold War 'narrow' focus limited to military and nuclear weapons (Buzan et al., 1998, p. 2), and its inability to properly explain the security issues in the unipolar world order following the Cold War (Allison & Treverton, 1992). This critique of the 'narrow' understanding of security is exemplified by Baldwin: "*Unless one is willing to argue that military threats to national well-being are the only ones that matter, it is difficult to justify labeling the study of the threat, use, and control of military force as "security studies."*" (Baldwin, 1995, p. 139).

Instead, he argues that scholars of security studies should broaden their perception of what may threaten national security.

With a 'wide' perception of security, Romm (1993) defines a threat to national security as "[…] *whatever threatens to significantly (1) degrade the quality of life of the people, or (2) narrow the range of policy choices available to their government.*" (Romm, 1993, p. 85) As examples, Romm argues that declining economic competitiveness and climate change ought to be viewed as threats to national security. By broadening his scope of threats to national security, Romm follows Ullman's Hobbesian logic: "*A victim is just as dead if the bullet that kills him is fired by a neighbor attempting to seize his property as if it comes from an invading army.*" (Ullman, 1983, p. 130). Defined like this, it matters not if national security is threatened by foreign military, climate change, criminals or drug abuse (see Allison & Treverton, 1992) as these threats may all have the consequence of weakening the quality of life of the citizens of a state and limit the maneuverability of its government.

With their theory of *securitization*, Buzan, Wæver and de Wilde of the Copenhagen School of international relations place themselves among the 'wideners' (Buzan et al., 1998, pp. 2–5). Within the Copenhagen School, security is perceived as a constructed practice beyond the normal political sphere, but it also acknowledges that the military remains a crucial sector when addressing security issues (Buzan, 1997, p. 13). Buzan et al. argue that securitization is a tool to influence the logic of security itself, which can be applied to certain political issues in order to move them into the realm of emergency security concerns. This is done to legitimize extraordinary political means to counter the constructed threat (Buzan et al., 1998, pp. 23–26). Moreover, securitization may also happen when a traditionally politicized area is institutionalized within the military sector as this implies that the issue must be regarded with utmost priority (Buzan, 1997, p. 15). In practice, Buzan et al. (1998) argue that military, environmental, economic, societal and political sectors can be become matters of national security, although they stress "(…) *the shifting of issues out of emergency mode and into the normal bargaining processes of the political sphere* (…)" (Buzan et al., 1998, p. 11) is the ideal. What sets the Copenhagen School apart from other scholars with a 'wide' perception of security (e.g. Allison & Treverton, 1992; Romm, 1993; Williams, 2004), is the school's argument that security must be seen in an international context (Buzan, 1997, p. 13).

Baldwin points out that scholars with both 'wide' and 'narrow' perceptions of security share an understanding of security as *high politics* of great importance, implicitly referring to other political issues of less importance (Baldwin, 1995, p. 139). What sets the two

scholarly groups apart is their understanding of what should be regarded as security or *high politics.* A strong critique of the 'wide' conceptualization of security has been articulated by Walt:

> "*By this* ['wide'] *logic, issues such as pollution, disease, child abuse or economic recession could all be viewed as threats to "security". Defining the field in this way would destroy its intellectual coherence and make it more difficult to devise solutions to any of these important problems.*" (Walt, 1991, p. 213)

Though acknowledging the need for military capabilities, Baldwin counters this 'narrow' argument:

> "[…] *states need minimum amounts not only of security from external attack but also of breathable air, drinkable water, economic welfare, and so forth. A state without armed forces to protect it from external attack may not survive, but a state without breathable air or drinkable water will surely not survive."* (Baldwin, 1995, p. 128).

With their different perceptions of security, Walt and Baldwin put different emphasis on what they regard as security concerns calling for strong, political attention.

On the basis of these consideratons, it will later be discussed how these two conceptualizations of security can be applied to the realm of cyberspace and why this thesis chooses a 'wide' concept of security. However, before doing so, the thesis will define an array of terms essential to the understanding of cybersecurity.

8.2.2 Cyberspace

The most recognized guideline on the interpretation of international law in cyberspace by western states is the Tallinn Manual (CyberPeace Alliance, 2019; Jensen, 2017). It is an academic report created upon invitation from NATO, giving guidelines on how to act regarding cyberwarfare in line with international law. Originally from 2013 with the 2.0 updated version from 2017, the Tallinn Manual 2.0 defines cyberspace as: "*The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks*." (Schmitt, 2017, p. 564). Similarly, the Royal Danish Defence College defines the term as "[…]

the total global amount of entities that process, store and transmit digital information and code, whether connected or not." (Royal Danish Defence Academy, 2019, p. 8).[5]

Furthermore, within the scholarly field of security studies in cyberspace, there are similar ways of defining cyberspace (Friis & Ringmose, 2016). Some scholars, such as Deibart & Rohozinski, operate with somewhat broad definitions closely aligned with the formulation in the Tallinn Manual and by the Royal Danish Defense College: "[…] c*yberspace is both a material and virtual realm – a space of things and ideas, structure and content.*" (Deibert & Rohozinski, 2010, p. 16). Moreover, Friis & Ringmose (2016) argue that Libicki's (2007) model of three independent, yet interlinked, layers in cyberspace is another recognized and useful way of understanding cyberspace. These layers are characterized as the physical layer ('real' entities such as servers and wires), the syntactic/logical layer (e.g. codes, software, programs etc.) and the semantic/cognitive layer (e.g. data and strategic goals) (Friis & Ringmose, 2016, pp. 2-3).

8.2.3 Cyberattack

Leading cybersecurity company UPGuard defines cyberattacks as being "[…] *any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to a computer system, infrastructure, network, or any other smart device*." (Tunggal, 2020). Tunggal of UPGuard argues that cyberattacks can be conducted by both states and non-state actors. Similarly, the CFCS defines cyberattacks as threats where an actor attempts to gain unauthorized access to data (Centre for Cyber Security, 2019b). The EU definition, which was released in a briefing paper from the European Court of Auditors in 2019, includes states, criminals and hacktivists as the attackers in question (B. Jakobsen et al., 2019, p. 6). The DDIS further argues that cyberattacks "[…] *could potentially result in death, personal injury, property damage, or destruction or manipulation of information, extensive restoration is undertaken*." (Danish Defence Intelligence Service, 2019a, p. 34). According to the DDIS, despite the non-physical nature of cyberattacks, the consequences of a cyberattack can materialize both physically and virtually within IT systems.

[5] Translated from Danish by the authors.

8.2.4 Cybercrime

The International Criminal Police Organization, Interpol, defines cybercrime as "[…] *crimes against computers and information systems, where the aim is to gain unauthorized access to a device or deny access to a legitimate user (typically thorough* [sic] *the use of malicious software)*." (Interpol, 2019). According to Interpol, cybercrimes occur when criminals use new technologies to commit cyberattacks against governments, businesses and individuals.

According to Europol's most recent Internet Organized Crime Threat Assessment, criminals' use of ransomware poses the biggest threat within the realm of organized cybercrime (Europol, 2019, p. 8). Europol defines ransomware as software that enables criminals to block users from gaining access to their computer system while demanding that the users pay a ransom through online payment to regain access (Europol, n.d.-a). On top of ransomware attacks, criminals may also commit what is referred to as 'cyber-enabled' crimes. According to Interpol, these crimes are not necessarily new, hitherto unknown types of crime. Instead, in committing a cyber-enabled crime, criminals commit more traditional forms of crime through the use of the internet to

> "[…] *facilitate their activities and maximize their profit in the shortest time. These 'cyber-enabled' crimes are not necessarily new – such as theft, fraud, illegal gambling, the sale of fake medicines – but they have taken on a new online dimension*." (Interpol, 2019).

In this way, criminals can make use of cyberspace to gain faster and broader access to potential victims.

8.2.5 Cyberwarfare

The academic discussion about defining cyberwarfare has two main poles, the traditionalists and the revolutionists. The discussion between the two fronts is whether cyberwarfare can be considered warfare in its own realm (revolutionists), or if it has to be supplemented by conventional warfare, becoming a form of hybrid warfare (traditionalists) (Langø, 2016, p. 9). The term cyberwarfare logically connotes to war and therefore the military aspects of offensive and defensive operations in cyberspace. The early revolutionists argued that cyberwar is fought by the military, whereas they termed 'netwar' as a sphere of lesser conflict in cyberspace, which could encompass cyberoperations such as disinformation, deception and propaganda (Langø, 2016, p. 11). Both the EU and NATO acknowledge cyberspace as the fifth operational domain of warfare, enabling the development of cyberdefense capabilities (Brent, 2019). In this regard,

NATO has acknowledged that article 5, meaning an attack on one NATO state is treated as an attack on all member states, is also applicable in case of serious cyberattacks that may be characterized as cyberwarfare (Stoltenberg, 2019).

8.2.6 Cybersecurity

This section aims to briefly present EU, US and Danish institutionalized definitions of cybersecurity before dealing with the more theoretical considerations behind security studies in cyberspace in the following section.

The EU has a broad definition of cybersecurity and describes it in the following way:

> "*Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein*." (European Commission, 2013, p. 3).

Moreover, the American Cyber Infrastructure Agency (CISA), under the Department of Homeland Security, defines cybersecurity as "[…] *the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.*" (CISA, 2019). In addition, cybersecurity is defined somewhat similarly in the Danish National Cyber and Information Security Strategy (NCISS) 2018-2021:

> *"Cyber security encompasses protection against breaches of security resulting from attacks on data or systems via a connection to an external network or system. Cyber security thus focuses on vulnerabilities inherent to the interconnection of systems, including connections to the Internet*." (The Danish Government, 2018 p. 7).

These three examples show a somewhat similar broad definition of cybersecurity, stressing it as the protection against unauthorized access to data or systems through network connectivity in information and communication technology.

8.2.7 Security in cyberspace

This section aims at illuminating the scholarly field of security studies in cyberspace and how it connects to the field of security studies discussed earlier. The main reason for doing so is to

argue, why this thesis has chosen a 'wide' conceptualization of security and clarify how cybersecurity is defined in this study.

Langø (2016) suggests that the security discussion in cyberspace originates from the 1990s during which two scholarly fields were formed: the traditionalists and the revolutionists (Langø, 2016). Though the terms would suggest that the traditionalist is a synonym to the 'narrow' security field, and revolutionist the 'wideners', a short examination proves otherwise. Boiled down, the revolutionists constitute the oldest school, which envisions great security concerns regarding the development of cyberspace and have predicted that these concerns would eventually change the understanding of warfare itself in the same way as the development of nuclear weapons did (Langø, 2016, pp. 9-11). The traditionalist school originates from criticizing the revolutionist school as they argue there is little evidence to suggest that cyberspace is fundamentally changing warfare. They argue that cyberspace is simply a new dimension of war, and that existing concepts and theoretical approaches are sufficiently capable of explaining the complications of security in the realm of cyberspace (Langø, 2016, pp. 12-13).

What the two schools have in common is an intense focus on cyberwarfare resulting in a mutual understanding that security implications connote to military operations in cyberspace. Both schools address concerns for the 'use of force' on physical objects through cyberspace, and the traditional school stresses that physical destruction must be evident for something to be categorized as warfare (Langø, 2016, pp. 10-13). This focus on military capabilities in cyberspace and the use of force suggests that both schools share the understanding of security closer to the 'narrow' field as it lies closely within Walt's suggestion that security is "(…) *the study of threat, use and control of military force.*" (Walt, 1991).

However, a large part of the scholarly field of cybersecurity seems to have moved its focus from cyberwarfare to a broader and more complex understanding of security in cyberspace that surpasses the military element (e.g. Christensen & Liebetrau, 2016; Deibert & Rohozinski, 2010; Friis & Ringmose, 2016; Hansen & Nissenbaum, 2009; Kassab, 2014; Kremer & Müller, 2014; Langø, 2016). The main critique of the 'narrow' conceptualization of security in cyberspace is that the 'narrow' understanding concerns itself more with explaining the concept of war rather than that of security (Christensen & Liebetrau, 2016, pp. 15-16). Since cyberattacks rarely show signs of physical violence, i.e. the use of physical force or destruction (Langø, 2016, p. 13), the 'narrow' conceptualization of cybersecurity disregards cyberwarfare in its 'pure', non-physical form, implicitly ignoring the non-military security issues that exist in cyberspace (Lewis, 2018, p. 1). This leads Christensen & Liebetrau to argue:

> "*It (traditionalist)* ['Narrower'] *neglects the ways in which the meeting between security and cyberspace transforms security politics. We run the risk of blinding ourselves to the transformative role of ICT* [information and communication technology] *and to the new actors and practices of security that cyber security potentially entails*." (Christensen & Liebetrau, 2016, pp. 2-3)

In addition, Langø (2016) and Deibart & Rohozinski (2010) argue that this 'narrow' focus on cyberwarfare, use of force and military fails to address how conflicts are happening in cyberspace. The latter argue that the 'narrow' field neglects to see the complexity of cyberspace and the implications this has on cybersecurity. They suggest:

> "[…] *cyberspace is comprised of both a material and a virtual realm—a space of things and ideas, structure and content. Theorists and observers of cyberspace often focus on one of these elements to the exclusion or diminution of the other, but both are important and interdependent."* (Deibert & Rohozinski, 2010, p. 16).

By suggesting that security in cyberspace implies material consequences, the 'narrow' conceptualization fails to address the interlinked sphere of both the virtual and physical realm. Deibart & Rohozinski (2010) and Langø (2016) suggest that one must examine the layers of cyberspace and its capabilities in order to understand security issues in cyberspace (Deibert & Rohozinski, 2010, pp. 16-17; Langø, 2016, pp. 17-18). Deibert & Rohozinski address security in cyberspace as such:

> "[…] *we do so by first disaggregating cyberspace security into two related but distinct dimensions, articulated as "risks": risks to the physical realm of computer and communication technologies and their associated networks (risks to cyberspace, commonly known as critical infrastructure protection); and risks that arise from cyberspace and are facilitated or generated by its associated technologies, but do not directly target the infrastructures per se (risks through cyberspace)*." (Deibert & Rohozinski, 2010, pp. 16-17).

This focus on cyberspace leads to an understanding of an existence of multiple different "securities" in cyberspace that transcend only looking at military capabilities. Christensen & Liebetrau suggest a somewhat similar understanding by focusing on the structure of cyberspace as they build their understanding of multiple "cybersecurities" (Christensen & Liebetrau, 2016 pp. 2-3). It can be suggested that Langø, Christensen & Liebetrau and Deibert & Rohozinski broaden the understanding of cybersecurity from the 'narrow' traditionalist and revolutionist schools by focusing on cyberspace itself, rather than a focus on military capabilities, use of force and the possibility of war in the realm of cyberspace. This would suggest that these scholars would be closer to a 'wide' understanding of security rather than a 'narrow' one.

Furthermore, there are also specific examples of scholars applying the Copenhagen School's understanding of security to the realm of cyberspace. This application opens for an understanding of cybersecurity that transcends merely investigating military aspects (Hansen & Nissenbaum, 2009; Kassab, 2014). In Kassab's argument for conceptualizing the 'New Copenhagen School' in which she suggests cyberspace is a new sector as well as level of analysis, she ties her understanding of security to that of the 'wideners':

> *"Integrally, security according to Ullman can no longer be considered state centric, but humancentric. Thus, insecurity can be defined as anything that degrades human life and reduces state autonomy. Cyber-security fits in well with this analysis. As discussed prior, cyber-attacks have the potential to degrade human life and reduce state autonomy. National security can no longer be considered as military threats to the state, but rather, must focus on these aspects, even if we have to sacrifice an analytical concept.*" (Kassab, 2014, p. 65).

This understanding of cybersecurity 'widens' the perception of security in cyberspace to encompass issues that are not solely affecting the military. This also suggests that a 'wide' understanding of security is highly applicable when addressing security issues in cyberspace.

In cybersecurity, the so-called *attribution problem* is the main reason why this thesis has chosen a 'wide' conceptualization of security rather than a 'narrow' one. In short, the *attribution problem* describes the fact that if a cyberattack on an entity has been conducted, it is extremely difficult to determine who is responsible: "*Cyberspace affords actors unprecedented opportunities to carry out operations under a cloak of anonymity*." (Poznansky and Perkoski, 2018, p. 402). As such, cyberspace is a realm in which damaging attacks could be

conducted with anonymity, without capabilities to specifically pinpoint in all cases, who the aggressor is or whence the attack originates (Jakobsen et al., 2019, p. 6). Further, the CFCS accepts this premise in their practical, everyday work as they do not distinguish between criminal or state-sponsored attacks in their immediate response (Interview Thomas Wulff of the CFCS, 2020, 14:50-20:00). In Ullman's view, "*A victim is just as dead if the bullet that kills him is fired by a neighbor attempting to seize his property as if it comes from an invading army.*" (Ullman, 1983, p. 130). However, if one is to follow Ullman's Hobbesian analogy to the realm of cyberspace, the *attribution problem* would suggest that the victim cannot even see whether the bullet came from criminals or soldiers. In cyberspace, due to the *attribution problem*, applying a 'narrow' understanding of security, focusing exclusively on military issues, is missing the point by ignoring the complexity of cyberspace.

As Langø (2016), Christensen & Liebetrau (2016) and Deibert & Rohozinski (2010) argue, one's understanding of cybersecurity should be built according to the complexities of cyberspace and how it operates. The 'wide' conceptualization of security in cyberspace applied in this thesis is thus a direct consequence of the unique nature of cyberspace, here exemplified by the attribution problem. As such, the thesis does not focus on distinguishing between attacks committed by states, state-sponsored groups, organized criminals or 'lone wolves'. Rather, much in line with the EU, the Danish government and CISA, this thesis understands cybersecurity as the protection against state-sponsored military attacks and criminal activity in cyberspace. The thesis thus adopts the EU's definition of cybersecurity:

> "*Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein*." (European Commission, 2013, p. 3)

This understanding of security in cyberspace enables the thesis to look into the Danish state's policies of protecting itself, both independently as well as through EU and NATO cooperation, against state-sponsored military attacks and criminal activity in cyberspace.

9 Analysis

The overall aim of this chapter is to answer the research question. The first two parts of the analysis will illuminate how Denmark can compensate for its relative weakness in cyberspace through NATO and the EU respectively, by examining their cybersecurity initiatives beginning with NATO followed by the EU. The third part of the analysis is built upon the findings in the previous sections and will examine why Denmark does not engage in closer EU cooperation on cybersecurity. It will investigate Denmark's own cybersecurity initiatives as well as domestic and external reasons for Danish reluctance to engage in deep EU cooperation on cybersecurity matters.

9.1 NATO cooperation - The Danish cybersecurity guarantor?

This chapter intends to illuminate how the Danish state utilizes NATO as an alliance in cyberspace. The small state theory suggests that a small state can engage in military alliances when it perceives its fundamental security to be threatened or when it wishes to gain political influence (Handel, 1981/1990; Rothstein, 1968; Vital, 1967/2006). As mentioned earlier, the DDIS stresses that cyberthreats to Denmark and Danish interests are very high, and the DDIS assesses that the problem will accelerate fast in the future (Danish Defence Intelligence Service, 2019b, pp. 8-9; Centre For Cyber Security, 2019, pp. 2-3). The severity of the cyberthreat against Denmark is also demonstrated by the Danish government's choice of allocating 1.4 billion DKK over 5 years in the 2018 Danish Defense Agreement (Danish Ministry of Defence, 2018, p. 10).

NATO is widely recognized as the cornerstone for Danish defense and thereby the Danish security guarantor. This is demonstrated in Danish history (S. H. Rasmussen & Brunbech, 2009a); by Danish authorities such as Ministries of Foreign Affairs and Defence and Danish Intelligence Agencies (Ministry of Foreign Affairs of Denmark, 2018, p. 11; Danish Ministry of Defence, 2018, p. 2; Danish Defence Intelligence Service, 2019, p. 4); by former Danish ministers and current national and EU parliamentarians (Interview Claus Hjort Frederiksen, 2020; Interview Martin Lidegaard, 2020; Interview Karen Melchior, 2020; Interview Christel Schaldemose, 2020; Interview Pernille Weiss, 2020; Interview Michael Aastrup Jensen, 2020); and by Denmark's current Defense Minister (Bramsen, 2019) and Prime Minister (Frederiksen, 2019). However, whether NATO can also be viewed as Denmark's security guarantor in the realm of cyberspace, and whether the alliance serves as a relevant cooperation for a small state to engage in to compensate for its relative weakness in cyberspace will be analyzed in the following sections. In order to do so, these will initially explore NATO's

main cybersecurity policy and initiatives to gain knowledge of NATO's overall cybersecurity commitments and the operational relationship between NATO and its member states in cyberspace. In light of the fact that NATO affirms that the cornerstone of the alliance is obtaining solidary defense and deterrence (NATO, 2020b), it will further be discussed if NATO is successful in obtaining deterrence in the realm of cyberspace.

9.1.1 NATO's role in cyberspace: Structure and entities

This section intends to illuminate NATO's policy in cyberspace and investigate NATO's responsibilities and operational entities. The reasons for doing so are two-fold. Firstly, it aims at giving an overview of NATO's intentions in cybersecurity, which creates a foundation for the rest of the chapter to discuss upon. Secondly, the section aims at investigating the relationship between NATO's responsibilities in cybersecurity and that of the individual member state with a focus on Denmark.

9.1.1.1 NATO's cybersecurity structure

Cybersecurity has been on NATO's agenda for little over two decades (Brent, 2019). As the first main organizational entity of NATO, the so-called Computer Incident Response Capability (NCIRC) was launched in 1999 following an incident, during which NATO saw e-mails compromised and its website locked down in response to NATO air strikes against Serbia (Hasanov, Iskandarov, & Sadiyev, 2019, p. 95). The NCIRC was set up to be an operational entity within NATO with technical personnel to "[…] *prevent, detect, and respond to cyber incidents.* (Hasanov et al., 2019, p. 95). However, despite being the only operational cyber emergency response entity in NATO, the NCIRC's sole responsibility is to protect NATO's own networks and communication systems (NATO, 2019b, pp. 1-2), but not the individual member states' (Alatalu, 2016 pp. 2-3). Because of this, Alatalu suggests that NATO should initiate an: "[…] *operational, interoperable-with-Allies and deployable-if-needed operational capability to respond to an incoming cyber-attack* […]" (Alatalu, 2016, p. 3), in order for NATO to be able to actually protect and assist its member states if they fall victim to cyberattacks.

Due to the lack of external operational capabilities of the NCIRC, NATO was unable to mitigate the major cyberattack carried out against Estonia in 2007. The cyberattack, which is assumed to have originated from state-sponsored groups in Russia, disrupted governmental and business websites and communication networks for three weeks, and it is regarded as one of the most severe cyberattacks on any state to date (Herzog, 2011; Schulze, 2018; Tamkin, 2017). As a fellow small state which, like Denmark, is a member of both NATO and

the EU, the example of Estonia seems to underline the risk for small states posed by cyberattacks. With NATO's inability to secure its weaker member states at the time, Rothstein and Vital would suggest that a state like Denmark or Estonia ought to reconsider whether the alliance was truly necessary for their cybersecurity (Rothstein, 1968, p. 61; Vital, 1967/2006, p. 84).

However, instead of exiting the at-the-time ineffective alliance, which scholars like Vital or Rothstein may have suggested to be the most prudent course of action for a small state, Estonia chose a different tactic often found in other small state scholars' literature. Following the attack, by taking on the role of a norm-entrepreneur, Estonia sought to set up a common set of internationally agreed upon norms and rules regarding cyberspace. Crandall & Allan (2015) demonstrate this as they point to Estonia's success in establishing bilateral agreements with the US, in pushing for the creation of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn and in developing the Tallinn Manuals 1.0 and 2.0, which suggest how to apply international law in cyberspace (Crandall & Allan, 2015, p. 353). Though Estonia only built norms, which have been accepted by NATO allies, Crandall & Allan conclude that Estonia's norm-entrepreneurship through NATO has increased Estonia's ability to assert its own state interest through cyber norm-building (Crandall & Allan, 2015, pp. 357-361).

As with the establishment of NCIRC, the establishment of the CCDCOE and the adaptation of NATO's first policy on Cyber Defense in 2008 came in response to the attack on Estonia rather than as a preventive measure. With its main objective of conducting research, education and development in the field of cybersecurity (NATO, 2019b, p. 2), the CCDCOE acts as a focal point of expertise-sharing between NATO states and contributing partners, among which 25 (Western) countries are represented, including Denmark (Plantera, 2018). CCDCOE experts argue that the most notable research accomplishment produced by the center is its publication of the Tallinn Manual 1.0 in 2013 and 2.0 in 2017, which, according to the CCDCOE is: "[…] *the most comprehensive analysis on how existing international law applies to cyberspace."* (CCDCOE, 2020). However, as only Western academics were invited to co-write the analysis, the manual has been subject to criticism mainly because it does not reflect how great powers such as Russia and China expect international law to be applied in cyberspace (Crandall & Allan, 2015, p. 358). Therefore, the Tallinn Manuals 1.0 and 2.0 reflect how NATO countries believe the international law should be applied in cyberspace, though it has not been successful in creating international norm-acceptance (Finnemore & Sikkink, 1998, p. 6).

As an institutional framework, the CCDCOE may be regarded as a useful project within NATO for a small state like Denmark (Krasner, 1981, p. 121). Much in line with general small state arguments (e.g. Handel, 1981/1990, pp. 52–53), it is suggested by Giegerich from the International Institute for Strategic Studies that a country's intellectual man-power capacity in IT is crucial when considering cybersecurity capabilities of any given state (Danish Defense Committee, 2019, 2:22-2:30). Considering this, CCDCOE is an example of an institution through which a small state such as Denmark can compensate for its relative weakness in man-power and human-talent capabilities due to its relatively small population size, by gaining additional knowledge and expertise through international cooperation established in NATO (Krasner, 1981, p. 121). Having acknowledged this, the Danish government stresses the importance of Danish contribution to the CCDCOE and sees it as an important way to enhance Danish cybersecurity capabilities (Danish Ministry of Defence, 2018, p. 3; Eriksson & Pettersson, 2017, pp. 72-73; The Danish Government, 2018, p. 44).

In its pursuit of increasing its cybersecurity expertise and development through NATO, Denmark further took part in NATO's 'Smart Defense Initiative' from 2013[6], which encouraged allies to: "[…] *pooling and sharing capabilities, setting priorities and coordinating efforts better*." (NATO, n.d.). As part of this initiative, Denmark, together with Canada, Romania, Norway and the Netherlands, engaged in NATO's Multinational Cyber Defense Capability Development project (MN CD2) (NCI, 2013). Similarly as with the CCDCOE, this initiative would suggest that Denmark was utilizing its cooperation with NATO to compensate for its relative weakness (Handel, 1981/1990, p. 120; Rothstein, 1968, p. 61) by sharing expenses with other allies and by more efficiently gaining cybersecurity expertise and capabilities (Krasner, 1981, p. 143). However, by 2015, Denmark had left the MN CD2 as the only state, whilst Finland had joined the project with an observatory status (NCI, 2015). According to Major Christian Friis of the Danish Ministry of Defence, Denmark decided to leave the MN CD2 cooperation in order to focus all its limited resources on building up its own domestic capabilities in the CFCS (see appendix C). However, this move is rather paradoxical in light of the current Danish National cyber strategy, in which international cybersecurity development and expertise sharing have been set as priorities (The Danish Government, 2018 p. 44).

[6] *"Smart defence is a concept that encourages Allies to cooperate in developing, acquiring and maintaining military capabilities to meet current security problems in accordance with the new NATO strategic concept. Therefore, NATO smart defence means pooling and sharing capabilities, setting priorities and coordinating efforts better."* (NATO, n.d.).

In 2018, NATO announced its new trial project called Cyberspace Operational Centre (CyOC). With this initiative, NATO seems to be moving in more proactive and defensive direction by pooling NATO members' intelligence and offensive capabilities:

> "*The CyOC serves as NATO's theatre component for cyberspace and is responsible for providing cyberspace situational awareness, centralised planning for the cyberspace aspects of Alliance operations and missions, and coordination for cyberspace operational concerns."* (Brent, 2019)

Among the members participating in the CyOC is Denmark, which can offer NATO its offensive capabilities in an agreement to NATO reaching a desired outcome (Vavra, 2019). In this way, by offering its capabilities to the CyOC, Denmark has the chance to influence the overall decision-making and priorities of the initiative. If one follows Dosenrode's notion that a small state may be able to join and influence cooperational frameworks to persuade great powers to act to the small state's benefit (Dosenrode, 1994, pp. 246–247), by joining an initiative like the CyOC, Denmark might be able to persuade its fellow NATO allies to act according to Danish priorities in cyberspace. However, as the Deputy Director of the CyOC, Neale Dewar, said in an interview in 2019, the center is not scheduled to be fully operational until 2023 (Vavra, 2019), so until then, there is no telling whether the initiative will be successful.

To summarize, cybersecurity has been on NATO's agenda for over two decades, and through the years, it has created initiatives for Denmark to utilize the alliance to compensate for its relative weakness in cyberspace. However, this compensation has mainly happened through the sharing of research, expertise and developing programs in the CCDCOE and briefly in the MN CD2 project that Denmark had paradoxically left by 2015. When singling out the realm of cyberspace, NATO has articulated strong commitments to defending its member states but has yet to show equally strong responses seeing as the individual member states are in essence defending themselves. As an example, NATO's operational emergency response entity, the NCIRC, is only responsible for defending NATO's own internal networks. NATO's own network security does, however, rely on outside support. Herd and Kriendler argue:

> *"Because NATO depends critically on inter-connected networks, most of which are not under its direct control, NATO cyber defense is really a matter of (1) determining the key components of NATO's mission that must be protected; (2) identifying the networks and cyber assets that critically support*

> *those components; and (3) working with the various network operators to ensure an adequate level of security."* (Herd and Kriendler, 2013, p. 163).

The fact is that even if NATO only had to secure its networks, it would still be a daunting organizational and technical challenge, which requires a clear definition as to how, when and under what circumstances NATO's proprietary networks interconnect with the networks of the alliance member networks (Herd and Kriendler, 2013, p. 163).

As such, due to the interconnectedness of NATO's and its members' systems, which NATO cannot control on its own, NATO's ability to address incidents in cyberspace seems to be hampered. In this regard, Alatalu (2016) suggests that the creation of an operational, deployable cyber entity with responsibility to assist member states that have fallen victim to cyberattacks would help close the gap between NATO's commitment and its response.

NATO does, however, not rely solely on its ability to address cyberattacks once they have happened. Instead, as in other operational domains, NATO has developed a cyber deterrence strategy, which the following section will look into.

9.1.2 NATO's ability to create cyber deterrence

One of the cornerstones of NATO is the ability of the alliance to secure its members by deterring hostile states or groups from attacking the alliance (NATO, 2020b). In general, deterrence can be defined as a strong defensive system that can reject any attack and have effective offensive capabilities that can impose massive retaliatory damage as a responsive action. In addition, deterrence entails a third aspect, the diplomatic, i.e. the notion that a state has to get the adversaries to fear the state (Snyder, 1961, pp. 9–10). Falling closely in line with Snyder's general definition of deterrence, NATO, acknowledging the dangers arriving from cyberspace, has developed its own cyber deterrence strategy, consisting of three approaches: 1) Responsive and retroactive: punishing the adversary trough different countermeasures; 2) Defensive: setting up systems and infrastructures that deny any adversaries the possibility of successfully attacking the alliance. 3) Declaratory and diplomatic: reassuring the adversaries that any action taken against the alliance will have devastating consequences for the adversaries (Herd and Kriendler, 2013, p. 162). By making this strategy, NATO thus makes a pledge to its member states that the alliance can secure them in cyberspace.

Being an alliance, small state theorists such as Vital and Rothstein would suggest that a small state like Denmark should not enter into tight NATO cooperation unless its security is at risk (Rothstein, 1968, p. 61; Vital, 1967/2006, p. 84). Though acknowledging Vital's and

Rothstein's points that small states may fall victim to great power dictation in alliances, Handel argues that small states which join alliances out of a *free choice* can benefit greatly from the alliance, as long as the great power or the alliance as a whole makes good on its contractual promises towards the small state (Handel, 1981/1990, pp. 121-122). Following this logic, the thesis thus suggests that Denmark should be able to enhance its security in cyberspace through greater NATO cooperation if NATO is able to make good on its pledge to deter hostile groups from committing cyberattacks against the alliance. With this logic, the following sections will discuss NATO's ability to create cyber deterrence both isolated through capabilities in cyberspace and through cross-realm capabilities.

9.1.2.1 Cyber deterrence as an isolated realm

As stated, one of the main factors of deterrence lies in the possibility of retaliation (Snyder, 1961, pp. 9–10). Because of this, it is essential to investigate the capability of cyberweapons to create deterrence. In most cases, the ability of a state to gain effective cyberweapons entails intelligence agencies being able to hack into an adversary's critical network systems to search for weaknesses and place malicious malware. In turn, these weaknesses can be exploited or the malware triggered to e.g. shut down a powerplant to retaliate (Jacobsen, 2016, pp. 2-3; Interview Thomas Wulff of the CFCS, 2020, 27:30-28:00). However, for a cyberweapon to be effectful, the adversary cannot know that the attacker has found a weakness in its system or placed a malicious malware in it as the weakness or the malware would likely just be corrected. This fundamentally changes the nature of deterrence as it was known during the Cold War era. Libicki argues: "*In the Cold War nuclear realm, attribution of attack was not a problem; the prospect of battle damage was clear; the 1,000th bomb could be as powerful as the first; counterforce was possible* […]" (Libicki, 2009, p. XVI). Contrary to the great powers' nuclear weapons during the Cold War, today's cyberweapons must be kept secret to be effective, seeing as any demonstration of one's cyberweapons would drastically reduce and probably nullify their effectiveness. Because of this need for secrecy, the creation of isolated cyber deterrence is immensely difficult, if not downright impossible, as the adversary will never know that a weakness has been discovered (Bebber, 2018; Jacobsen, 2016, pp. 2–3). Furthermore, if the adversary state learns that the attacking state has hacked its systems and placed malicious malware, it may create political and diplomatic conflict as it has been conducted in time of peace (Jacobsen, 2016, p. 3).

Moreover, the armament of cyberweapons creates a security dilemma unique to

the realm of cyberspace. The operational systems that the attacking state is usually targeting are often commercial software products, like, for example Microsoft Windows (Jacobsen, 2017b, p. 5). This means that if the attacking state utilizes a weakness in the commercial software system, this weakness can potentially be used by other actors after the initial attack, against all users of the commercial software system, putting the attacking state's own public and private entities at risk, seeing as some of them are likely to be users of the same commercial software system (Jacobsen, 2016, pp. 4-5). In short, a cyberattack can have a backlash effect on the state that attacks. Therefore, another choice of action could be to alarm the commercial provider of a found exploit, so an update would remove actors' abilities to utilize that weakness and thereby ensuring stronger cybersecurity for all users of the product. However, logically, this disables the entity from utilizing this exploit as a means of cyberattack and therefore their cyberweapon capacity (Jacobsen, 2016, p. 4; 2017b).

Thus, these issues demonstrate the inherent problems in obtaining deterrence in cyberspace if cyberspace is seen as an isolated realm of military operation. Within this framework, it seems extremely difficult for NATO to establish deterrence like that provided by its nuclear weapons, and since NATO regards deterrence as one of the cornerstones of creating solidary defense and security for the member states in the alliance (NATO, 2020b), NATO does not seem to be successful in obtaining this in cyberspace as a single realm. As such, if NATO maintains that cyber deterrence capabilities must originate from cyberspace itself, Handel would suggest that a small state such as Denmark should not engage in NATO cooperation, since NATO cannot make good on its promise to protect the small states from the cyberthreats it encounters (Handel, 1981/1990, pp. 121-122).

However, as argued by Davis, if NATO is to live up to its promises of creating deterrence in cyberspace, the alliance must manage to integrate its defensive and offensive cyber capabilities with other instruments used in the alliance (Davis, 2019, p. 3). Nye Jr. furthers this point:

> *"The term "cyber deterrence" can be confusing because theorists tend to focus on in-kind or in-domain deterrence rather than on a broad range of tools that can be used both actively and passively and with graduated effects."* (Nye Jr., 2016, p. 46).

In much the same way, Maldre argues that NATO's cyber deterrence strategy should not be separate from that of the combined deterrence strategy of NATO (Maldre, 2016, p. 9). As such,

instead of looking at deterrence from isolated realms, the following section will discuss NATO's possibility of achieving cross-realm deterrence.

9.1.2.2 Kinetic deterrence against cyberattacks

According to Steiner, cyberwarfare cannot be seen as warfare in a single isolated realm as many cyberattacks are the possible actions or instrument of an overall political strategy with multiple instruments used to obtain these goals, and are therefore not just inflicting damage without a direct purpose (Steiner, 2016, pp. 144-145). Having to confront cyberattacks from such a perspective, it is necessary for, in this case, NATO and Denmark to create not only offensive and defensive capabilities to deter adversaries, but it is also important to be able to deter the adversaries from taking actions (Herd & Kriendler, 2013, p. 162).

Following this point, during the 2014 Wales summit, NATO decided that cyberdefense should be a core task for NATO's collective defense (NATO, 2019b, p. 1). Two years later, at the Warsaw summit in 2016, the North Atlantic Council (NAC) declared cyberspace as the fifth operational domain of NATO on equal terms of air, land, sea and space (NATO, 2020). Echoing the notion that the alliance through its history has adapted to the different threats and security needs of the alliance, the NAC agreed that any attack in cyberspace is subject to a responsive action as an attack in the other four realms. This factually means that a cyberattack on an alliance member state allows that member state to invoke NATO's article 5, which is the cornerstone of NATO's deterrence strategy (Limnéll & Salonius-Pasternak, 2016). Article 5 reads:

> "[…] *an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them* […] *will assist the Party or Parties so attacked by taking* […] *such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."* (NATO, 2019a)

At the Warsaw summit, it was thus decided that a severe cyberattack could lead to an allied military response, though no clearly-defined threshold for the severity of such a cyberattack was decided upon (Hasanov et al., 2019, p. 98).

Though not defining a clear threshold of severity, the decision did open for the

possibility of using conventional, kinetic weaponry to provide cyber deterrence. To date, however, kinetic countermeasures have never been taken in response to a cyberattack on a NATO ally. Globally, to date, only one state has done so when Israel launched a kinetic counterattack as a follow-up after a cyberattack conducted by Hamas. For Israel, this counterattack did not have any consequences for further actions because of the dynamic between the two parties (Doffman, 2019). However, one should be very careful in comparing Israel and Hamas's relationship to that of NATO and its potential adversaries as Hamas is not a state. The relationship between NATO and its potential adversaries is much more complex and would have far more dire consequences should an attack occur both non-kinetically, but especially if kinetic warfare should arise as a result of a cyberattack (Herd & Kriendler, 2013 p. 164).

Still, despite the possible consequences, if a NATO member state falls victim to a severe attack, all military, retaliatory measures, including kinetic warfare, are available. By making cross-realm responses possible, NATO has expanded its toolbox for creating cyber deterrence by allowing its cyber deterrence strategy to draw on the main conventional deterrence strategy that relies heavily on kinetic weaponry (Taddeo, 2018, p. 348). Though never invoked, this is likely to strengthen NATO's cyber deterrence, as a kinetic attack on an adversary would likely prove incredibly devastating, thus possibly deterring the hostile state, group or entity from attacking. In this way, following Handel's suggestion Denmark might feel encouraged to look to NATO for its cybersecurity (Handel, 1981/1990, p. 121-122).

9.1.2.3 Cyber deterrence restrictions in international law

The use of kinetic weaponry may, however, not be particularly applicable as a countermeasure to cyberattacks. During the Cold War, Libicki argues, use of nuclear weaponry crossed an acknowledged line (Libicki, 2009, p. XVI). However, seeing as NATO has yet to agree on a threshold for how severe a cyberattack must be to allow NATO allies to respond in unison with kinetic countermeasures, the question still remains whether a devastating kinetic response to a cyberattack is crossing a line. As with any other countermeasure, these responsive actions have to be in accordance with the UN Charter and general international rules of law, e.g. Jus ad Bellum & Jus in Bello, and must follow the principle of proportionality as a core concept for self-defense (Taddeo, 2018, pp. 348-349):

> *"Proportionality is to be understood in the sense that the counterattack or the amount of force used is proportionate in relation to what is desired to accomplish, or proportionate in relation to the wrong-doing against a victim*

> *state (self-defense), when the use of counter-force has been deemed necessary. Proportionality refers to the size, duration and target of the response."* (Pank, 2019, p. 29)

Even though the UN Charter sets some clear conventional guidelines as to what constitutes an armed attack and when responding to such attack, Schmitt believes that *"*[…] *cyber operations do not fit neatly into this paradigm because although they are "non-forceful" (that is, non-kinetic), their consequences can range from mere annoyance to death."* (Schmitt, 2011, p. 573). Schmitt is backed by Lieutenant General and USA Nominee for Commander, at the US Cyber Command, Keith Alexander, who states:

> *"There is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force. Thus, whether in the cyber or any other domain, there is always potential disagreement among nations concerning what may amount to a threat or use of force."* (Alexander, 2010, p. 11).

In this way, NATO should arguably push for the creation of clear guidelines as to when a cyberattack is sufficiently damaging in order to cross the threshold that allows for an armed countermeasure (Melzer, 2011, p. 36). Internally, NATO might have some idea as to when this threshold is met, but as is argued by Melzer, until the International Court of Justice sets a precedence for this threshold, no international common set of rules can guide the alliance (Melzer, 2011, p. 36).

Arguably, this lack of an internationally agreed upon threshold could create issues for a small state like Denmark. In general, small states are strong supporters of international law, because international law is able to create some degree of order in an otherwise anarchic international system (primarily) controlled by the great powers (Handel, 1990, p. 53; Neumann & Gstöhl, 2006, p. 20). By this logic, a small state like Denmark, which arguably gains from strong international law and institutions, would thus have a moral and ethical obligation to create a comprehensive set of international laws and thereby eliminate the lack of clarity related to the threshold, and until such laws and a clear threshold have been agreed upon, it may not be in Denmark's interest to depend on NATO as its cybersecurity guarantor (Handel, 1981/1990 p. 122).

According to Ingebritsen (2002), small states like Denmark may, in fact, be able to gain great influence in the creation and shaping of international norms and rules (Ingebritsen, 2002, pp. 11–13). Crandall and Allan furthers this point as they argue that Estonia has been successful in establishing themselves as a norm-builder in cyberspace through its NATO membership (Crandall & Allan, 2015 p. 353). As such, if Estonia has been able to use NATO as a forum through which to spread international norms, Denmark might be able to do the same. To further stress this point, it is argued by Guang (2020) that all small states should engage in creating rules-based norms in cyberspace to prevent conflicts and being steamrolled by great powers (Guang, 2020, p. 169). In this way, it should be in Denmark's best interest to attempt to act as a norm entrepreneur and use NATO as a potential platform to promote these norms. The thesis has, however, not found anything that suggests Denmark is following such a strategy through NATO, yet Denmark's independent strategy of building cyber norms will be further examined later in the analysis.

Casting idealist notions aside, there may, however, be advantages in keeping a vague definition of 'severe cyberattack' as this arguably allows NATO to pursue a deliberately ambiguous strategy of cyber deterrence, which the following section will look into.

9.1.2.4 Ambiguity as a strategic approach

Ambiguous by nature, NATO's cyber deterrence strategy, unlike the other realms of military operation, has not organized, nor created, a working definition as to what the collective response will be if the aforementioned threshold is met (Davis, 2019, p. 7). While certain members may wish for NATO to be less ambiguous in its cyber deterrence strategy, according to Patrick, it could also be beneficial for the alliance to keep some form of ambiguity because it will make the adversaries wary of going too far, simply because they do not know when far is too far (Patrick, 2018). This could make any adversaries fearful of overstepping this invisible line and thus make the adversaries tread lightly when trying to conduct attacks against the alliance.

However, taking such an ambiguous approach to the threshold can lead to strong adversaries, which are comfortable taking risks, e.g. Iran, Russia, North Korea and China, still taking advantages of this 'grey zone' and test NATO's determination, and they may perhaps over time increase their efforts and actions against the alliance (Wallace & Visger, 2018, p. 53). However, to overcome this problem, it is argued, NATO does not necessarily need a complete deterrence strategy but rather needs a comprehensive policy that includes multiple response options to such cyberattacks. In Fischerkeller's and Harknett's (2018) views, NATO needs to

develop such options collectively, individually and with the international community, and to overcome this issue, the US 'persistent engagement strategy' might serve as an option for NATO. Fischerkeller and Harknett argue:

> *"A strategic approach of persistent engagement—described operationally as the combination of seamless resiliency, forward defending, contesting, and countering—will compel many U.S adversaries to shift resources to defense and reduce attacks. Moreover, persistent engagement is expected to allow for greater freedom of maneuver to impose tactical friction and strategic costs on U.S. adversaries pursuing more dangerous activities before they impair U.S. national power. This effort seeks to render the majority of adversary cyber and cyber-enabled activity inconsequential."* (Fischerkeller and Harknett, 2018, p. 4)

With such a strategy, allowing an array of different, albeit not pre-determined, measures and countermeasures, Fischerkeller and Harknett argue that NATO would be able to prevent and counter most attacks.

Though the lack of a threshold makes NATO's cyber deterrence strategy highly ambiguous, it does not constitute the only ambiguity inherent in NATO's strategy. If a NATO member falls victim to a severe cyberattack that crosses the ambiguous threshold, NATO's response is, in itself, ambiguous, seeing as NATO maintains the ability to retaliate both through cyberattacks and kinetic attacks (Patrick, 2018). What remains clear at this time is that NATO does not limit its responsive action to similar attacks, but nor does it exclude this option. This, like the issue of the vaguely defined threshold, can lead to doubt and confusion of the adversaries, who might then feel compelled not to attack (Herd & Kriendler, 2013; Patrick, 2018).

Whether NATO's ambiguous cyber deterrence strategy can be viewed as effective or ineffective, is difficult to conclude. Arguably, making its cyberdefence strategy rely on the collective defense and deterrence pledge was a big step in the right direction for NATO. However, as is evident from much scholarly literature (e.g. Bebber, 2018; Brantly, 2018; Iasiello, 2014; Tolga, 2018), it can be hard to live up to this pledge as it is argued that cyber deterrence can never truly exist due to the complex nature of security in cyberspace. Finding its basis in the attribution problem, one can never truly control one's adversaries' actions in cyberspace, seeing as a cyberattack does not necessarily originate from an easily identifiable group or state but could rather be the actions of a single person or group with an agenda not in line with that

of their government (Tolga, 2018, p. 16). Therefore in the case of cyberspace, Tolga argues that, at times, deterrence will simply fail (Tolga, 2018, p. 16).

The main debates and empirical studies on cyber deterrence have primarily be centered around the US (Bebber, 2018; McKenzie, 2017; Brantly, 2018). However, in the case of Denmark, deterrence and defense is not solely a great-power problem. The current climate of geopolitics arguably makes small state deterrence even more difficult as Denmark, contrary to the US, relies more heavily on international cooperation to secure itself in cyberspace (Burton, 2013, p. 218). During the Cold War, small states like Denmark were able to tailor their deterrence strategies to that of NATO and the US against the Soviet Union (McKenzie, 2017, p. 13). However, with the cyberthreats of today, NATO is faced with challenges on a much more complex landscape with less ability to take countermeasures against every cyberattack. According to McKenzie no matter the amount of efforts that NATO puts into cyberdefense, it will never be completely impenetrable (McKenzie, 2017, p. 13).

Still, what can be argued, is that since NATO started putting more emphasis on cyberspace as a realm of potential conflict and made cyberattacks subject to potential counter-measures, no cyberattacks on a scale comparable to that of Estonia in 2007 have been conducted against a NATO ally. NATO does, however, have issues with helping small states like Denmark against cyberattacks that fall under the non-existing threshold, thus suggestion it unfavorable for Denmark to engage in an alliance (Handel, 1981/1990, p. 121-122; Vital, 1967/2006, p. 79). Arguably, this comes down to the fact that NATO is a military alliance with no judicial power, making it unable to act on every manner of attack which threatens security in cyberspace. Overall, in deterring hostile states or groups from conducting vast, severe cyberattacks, it seems that NATO's ambiguous strategy works quite well. However, it still leaves small states weak and vulnerable to less consequential cyberattacks (Balakrishnan, 2018).

As NATO's main cyber initiatives have been investigated, the following section will illuminate how Denmark can utilize the EU to compensate for its relative weakness in cyberspace.

9.2 EU cybersecurity cooperation

In 2013, the European Commission (EC) issued a joint communication covering the EU's cybersecurity strategy. Focusing on increasing European cybersecurity capabilities, the EC pointed to five main focal areas for development: 1) Achieving cyber resilience; 2) Reducing cybercrime; 3) Developing a CSDP cyberdefense policy; 4) Developing industrial resources for

cybersecurity; and 5) Establishing a coherent cybersecurity policy for the EU (European Commission, 2013, pp. 4–5). In 2017, the EC incorporated these five focal areas into a three-point plan of increasing cyber resilience, cyberdefence and cyber deterrence (European Commission, 2017, p. 1). In achieving these goals, the Commission put emphasis on the roles of the European Network and Information Security Agency (ENISA), the *EU Cyber Diplomacy toolbox*, the CSDP, Europol and the *Computer Emergency Response Team for EU Institutions, bodies and agencies* (CERT-EU) (European Commission, 2017, pp. 4, 17). As the main task of CERT-EU is to contribute to the internal cybersecurity of the EU itself (CERT-EU, 2019, p. 2), the analysis will not look closer at this EU body, seeing as the member states themselves are not directly affected by it. Instead, the following sections will look into how a small state like Denmark may be able to compensate for its relative lack of capabilities to secure itself in cyberspace through cooperation with ENISA, CSDP and Europol bodies.

9.2.1 Creating EU cyber resilience: ENISA and the NIS Directive

The European Union Network and Information Security Agency (ENISA) is an EU agency founded in 2004, whose function is to help the EU institutions, the EU member states and the business community to improve European network and information security (Liebetrau, 2019, p. 208). Located in Heraklion in Greece, ENISA provides expertise, research and innovation, policy support, capacity building and cooperation, market standardization and certifications (ENISA, 2019, pp. 1–13), which in Krasner's view, would be favorable for a small state (Krasner, 1981, p. 121).

Every other year, ENISA brings together upwards of 1000 participants from all over Europe to partake in a shared exercise named "Cyber Europe". Joined by all (at the time) 28 EU members along with Norway and Switzerland, the fifth Cyber Europe exercise was held in December 2018 (ENISA, 2018, p. 6). During this exercise, special attention was put on organizational and national crisis management plans as well as cross-country cooperation and information-sharing (ENISA, 2018, p. 6). Though arguing that ENISA and the EU member states had come far in the development of cybersecurity on the technical level, the report called for stronger cooperation on the operational level, whilst also stressing the need for greater information exchange between the public and private levels in the member states: "*Special care needs to be taken during the development of such procedures and tools in order to provide incentives to cooperate and exchange information avoiding unidirectional information flow*." (ENISA, 2018, p. 7). Much in line with the points made by former Danish Minister of Defence Hjort Frederiksen during an interview with the authors, ENISA thus called for the creation of a

norm both internally in member states and externally among member states for greater transparency in case of a cyberattack (Interview Claus Hjort Frederiksen, 2020, 12:20-20:50). As ENISA already emphasizes the importance of better information-sharing, Denmark could establish clear internal procedures for public-private information-sharing in an attempt to set a normative precedence among EU member states and use ENISA to spread this norm (Finnemore & Sikkink, 1998, pp. 8-9). This would streamline intelligence-sharing, strengthen cooperation between EU members in the field of cybersecurity and ultimately strengthen Danish cybersecurity.

On top of the bi-annual Cyber Europe exercises, ENISA had a central role in the development of the so-called Network and Information Security directive (NIS), which was adopted in 2016. Calling for the strengthening of national capabilities, cross-border collaboration and national supervision for critical sectors (NIS Directive, 2016, pp. 2, 5), the NIS directive was the first ever EU legislation on cybersecurity and as such a cornerstone in EU cybersecurity initiatives (Liebetrau, 2019, p. 13). As an EU directive, the NIS directive serves as a binding legal act requiring EU member states to achieve a particular result without dictating the means of achieving it (EU, n.d.), and upon adaptation, the NIS directive was to be implemented in national legislation by May 9 2018 (NIS Directive, 2016, p. 24). The Danish Government published its NCISS in May 2018 implementing the NIS directive, which is explicitly mentioned and highlighted within the strategy, before the deadline (The Danish Government, 2018).

In the directive, cyber incidents in the energy, transport, banking and financial, health and water production sectors are emphasized as the most critical, seeing as an attack on any of these sectors is perceived to have disruptive effects on the smooth function of member states, the EU as a whole and the internal market (NIS Directive, 2016, pp. 1, 5). In order to strengthen cooperation among member states in case of an incident, the NIS directive calls for member states to establish a "[…] *national single point of contact responsible for coordinating issues related to the security of network and information systems and cross-border cooperation at Union level.*" (NIS Directive, 2016, p. 5). To do so, a computer security incident response team (CSIRT) with strong technical, financial and human resources should be appointed in every member state in order to achieve the objectives of the directive. In the case of Denmark, the CFCS serves as a CSIRT.

Representatives from the member states, the EC and ENISA should further have the ability to partake in a 'Cooperation Group' tasked with collecting, exchanging and managing information pertaining to risks and incidents (NIS Directive, 2016, p. 18). On top of this, the Coordination Group would provide guidance to a 'CSIRT network' comprised by the national CSIRTs, whose function is to, where possible and on a voluntary basis, discuss and identify responses to cyber incidents, share risk intelligence and providing mutual assistance to cyberattacks (NIS Directive, 2016, p. 19). As a voluntary cooperation, with this CSIRT network, the NIS directive provides an operational framework, through which a small state like Denmark can cooperate with other states on cybersecurity without the risk of having its hands forced by greater powers. Following Krasner's and Dosenrode's points, a small state like Denmark can help secure itself through such a cooperation without fearing for its national sovereignty (Krasner, 1981, p. 121; Dosenrode, 1994, pp. 245-246).

Despite this, when discussing ENISA and the NIS directive with Thomas Wulff of the CFCS during an interview with the authors, Wulff did not put much emphasis on the power of neither ENISA nor the NIS directive to provide emergency assistance in case of a cyberattack. Rather, he viewed ENISA as a coordinating agency, whilst he argued that the NIS directive constitutes some of the initial "baby steps" taken by the EU to integrate every EU member state in the same framework for cybersecurity following the notion that attacks, whose consequences potentially span across national borders, must also be addressed in a cross-national manner (Interview Thomas Wulff of the CFCS, 2020, 27:30-28:40). In Thorhallsson and Wivel's views small states stand to gain much from efficient EU cooperation (Thorhallsson & Wivel, 2006, p. 663). With this in mind, as ENISA and NIS provide an institutional framework that tries to streamline European cybersecurity and helps strengthen communication and expertise-sharing between the EU members, Denmark is arguably able to mitigate some of the risks posed by borderless nature of cyberspace by cooperating closely with the EU.

ENISA and NIS are, however, not the only EU bodies concerned with cybersecurity. Within the framework of the Common Defence and Security Policy on the one hand and Europol on the other, additional EU cybersecurity initiatives can be found. Paying special attention to the so-called Permanent Structured Cooperation, the newly established EU Cyber Diplomacy Toolbox, and the Europol Cybercrime Center, the following sections will analyze some of EU's other cybersecurity initiatives.

9.2.1.1 The CSDP and PESCO: Developing European cyberdefense

As a cornerstone of EU's Common Foreign and Security Policy (CFSP), the Common Security and Defence Policy (CSDP) is a central component in the crisis management, peace-keeping, conflict prevention and security policies of the EU (EEAS, 2018b). In 2017, a group of ENISA experts issued a report covering the risks and challenges in cyberspace faced by the CSDP. In particular, the report called for the necessity to join efforts and increase mutual assistance between member states, whilst focusing on avoiding unnecessary duplication of capabilities (Trimintzios et al., 2017, p. 9). In the report, ENISA points to one of the main issues of EU cybersecurity cooperation:

> "*Since the mandates within EU institutions and bodies sometimes still largely reflect the old 'pillar system' (comprising the European Communities, the common foreign and security policy and police and judicial cooperation in criminal matters) cooperation between different actors is less easy.*" (Trimintzios et al., 2017, p. 9).

In order to alleviate such issues and strengthen European cybersecurity, the report calls for the tightening of cooperation between the relevant EU organizations such as Europol, ENISA and the CSDP, especially stressing the importance of collaboration between the EU Military Staff and the European Defence Agency (EDA) (Trimintzios et al., 2017, p. 9). One such collaboration is the Permanent Structured Cooperation (PESCO), which the EC highlighted in its plan to strengthen cyberdefense (European Commission, 2017, p. 17).

9.2.1.2 PESCO

On November 22, 2017, 23 EU members notified their intention of signing an agreement to establish a Permanent Structure Cooperation (PESCO). First of its kind, PESCO was hailed by EU High Representative Mogherini, who called the signing of the declaration "[…] *quite a historic day for European Defense* […]" (Barigazzi, 2017). A few weeks later, on December 11, 2017, the European Council (EUCO) formally ratified the establishment of PESCO as a new European framework for security with 25 members[7]. Finding its mandate in the TEU article 42(6), PESCO provides a framework for EU member states seeking to deepen defense cooperation. Though open to any member state, article 42(6) in the TEU specified that exclusively

[7] Portugal and Ireland had notified Mogherini of their intentions of joining on 7 December, 2017 (Notification on Permanent Structured Cooperation (PESCO) to the Council and to the High Representative of the Union for Foreign Affairs and Security Policy, 2017).

those states whose military capabilities had met higher criteria should have the possibility of working more closely together on defense cooperation (Consolidated Version of the Treaty on European Union, 2015). However, when PESCO was formally initiated in late 2017 with 25 of the then-28 EU Member States, the original aim of creating an exclusive framework for tightened cooperation between leading EU members had arguably failed. Instead, PESCO has become a broad cooperation for every EU Member State apart from Malta and Denmark (Nissen et al., 2020, p. 27).

As of 2020, PESCO consists of 47 projects concerning areas such as land, air, maritime and cyberspace (PESCO, 2020). Providing a binding legal framework for cooperation on and investments in security for the EU members, PESCO encompasses both shared investments and concrete projects based on 20 binding commitments from those member states which wish to improve their capabilities in a given area (Notification on Permanent Structured Cooperation (PESCO), 2017, pp. 1, 3-5). Together with the High Representative of the Union for Foreign Affairs and Security Policy, the PESCO secretariat consisting of the EEAS, including the EU Military Staff and the EDA, have the role of overseeing and ensuring that the obligations of member states be met: In particular, the EDA oversees those PESCO initiatives concerning capacity development, whilst the EEAS acts as the authority on operational PESCO initiatives (Notification on Permanent Structured Cooperation (PESCO), 2017, p. 6).

A framework for developing European security in a broad array of different fields, PESCO allows member states to submit ideas for new projects, which will help the member states deliver on those 20 commitments they agree to when joining PESCO. These commitments can be roughly grouped into five categories focusing on a) cooperation on achieving an increase of defense expenditure to near 2%; b) streamlining defense apparatus, e.g. by conducting cooperation on training; c) enhancing interoperability and deployability of member states' armed forces; d) making up for shortfalls on European defensive capabilities with; and e) partaking in developing programs within the framework of the EDA (Consolidated Version of the Treaty on European Union, 2015). To deliver on these commitments, member states can submit ideas for projects they deem particularly useful and relevant to the overall goals of PESCO, and the relevance of these project proposals will then be assessed by the PESCO secretariat (Notification on Permanent Structured Cooperation (PESCO), 2017, p. 7). PESCO thus provides great powers and small states alike the chance to seek institutional influence and shape security policies to fit their needs. From a small state institutional view (e.g. Dosenrode, 1994, p. 247; Thorhallsson, 2000, p. 13), PESCO's legal framework for voluntary cooperation on defense

and security arguably seems to provide a sound institutional basis for small states like Denmark to focus on specific matters of security and bring some degree of order to their issues of security. As membership is voluntary and members are free to leave the cooperation whenever they choose, PESCO thus seems to provide small states with a valuable institutional framework.

In an attempt to strengthen the European pillar within NATO, PESCO officially aspires to work in technical and operational interoperability with NATO (Notification on Permanent Structured Cooperation (PESCO), 2017, pp. 4-5). Falling under the umbrella of the CSDP, PESCO's complementarity with NATO is accounted for in the TEU article 42(2):

> "*The policy of the Union* […] *shall respect the obligations of certain Member States, which see their common defence realised in the North Atlantic Treaty Organisation (NATO), under the North Atlantic Treaty and be compatible with the common security and defence policy established within that framework*." (Consolidated Version of the Treaty on European Union, article 42(2), 2015)

Recently, however, PESCO's potential for aiding in the build-up of European autonomy on defense and security has become a topic of some discussion (Dunn, 2020; Fiott et al., 2017; Zamarripa, 2020). In a publication by the European Union Institute for Security Studies, Fiott, Missiroli and Tardy (2017) argue: "*In the current climate* […] *defence capability development takes on even more salience in the context of a changing transatlantic relationship and a lack of clarity over the future relationship between the EU and the UK.*" (Fiott et al., 2017, p. 41) As such, though complementary to NATO, PESCO can be viewed as a framework for European states to gain autonomy over their own security matters.

Still a rather new framework for cooperation, whether PESCO will strengthen European defensive autonomy has yet to show. Zamarripa (2020) sees PESCO as the most promising framework for reinforcing and updating EU military capabilities (Zamarripa, 2020, p. 88). With the impact of the EDF on PESCO and its big focus on cooperation on the production of tangible military hardware, PESCO has been argued to show great potential for achieving more concrete results than earlier EU defense initiatives (Dunn, 2020, p. 7). However, the results of these initiatives will depend heavily on the member states. As with other EU security initiatives in the past, PESCO's projects may fall victim to waning commitments of the member states (Béraud-Sudreau et al., 2019, p. 4). The completion of projects will be tantamount to the

success of PESCO as a whole: With many projects relying on French or German support, concerns that these two European great powers may not be able to provide a date for final deliveries on their projects have been brought to the fore (Béraud-Sudreau et al., 2019, p. 5). Further, due to its great potential funds in the EDF, PESCO will need to ensure that member states do not initiate projects to sponsor their own industries but rather focus on the development of necessary capabilities and hardware (Dunn, 2020, p. 7). Still, what sets PESCO apart from earlier EU security initiatives are the legally binding commitments that members states agree to when participating in projects (Dunn, 2020, p. 8).

Clearly, whether the establishment of PESCO truly constitutes a historic turn in European security as Mogherini proclaimed in late 2017, cannot be concluded yet. From a small state perspective, the framework does show potential. As Rothstein and Vital argue, small states may be reluctant to establish and join alliances with greater powers due to the risk of losing national sovereignty and being controlled by the greater power (Rothstein, 1968, p. 61; Vital, 2006, pp. 84-85). However, due to the legally binding commitments that the states agree to when initiating cooperation on a given area within the PESCO framework (Dunn, 2020, p. 8), the risk for small states that the greater, more influential powers in the cooperation will 'run the show' seems to be somewhat alleviated. This contractual guarantee between the great powers and small states in PESCO cooperation thus seems to follow Handel's line of argument that small states stand to gain from alliances and cooperation made by free choice on the basis of a formalized, signed agreement or treaty (Handel, 1990, p. 122). Despite PESCO's potential value for small states, due to its opt-outs on security matters, Denmark is one of only two EU member states (Malta being the other) that are not PESCO partners. Because of this, Denmark cannot partake in capacity development, information sharing and operational activities in PESCO, though theory would suggest great potential for Denmark in the cooperation. The following section will analyze the potential of four PESCO initiatives explicitly focused on cybersecurity and discuss the consequences of the Danish defense opt-outs for Danish cybersecurity.

9.2.1.3 PESCO cybersecurity initiatives

Four of the 47 PESCO projects have the explicit aim of developing European cybersecurity either through innovation, information-sharing or emergency response teams. Coordinated by Greece and Lithuania respectively, two projects called '*Cyber Threats and Incident Response Information Sharing Platform'* (CTIRISP) and '*Cyber Rapid Response Teams and Mutual Assistance in Cyber Security'* were initiated as two of the first 17 PESCO projects in March 2018.

Of these two projects, CTIRISP aims at streamlining information-sharing and cyberdefensive capabilities, whilst CRRTs have the aim of strengthening member states' operational responses to incidents in cyberspace (Permanent Structured Cooperation (PESCO)'s projects - Overview, 2018, pp. 14-15). Further, in November 2019, two additional projects were initiated, with Germany coordinating the so-called '*Cyber and Information Domain Coordination Center'* (CIDCC) and Portugal coordinating the '*EU Cyber Academia and Innovation Hub*' (EU CAIH) (Permanent Structured Cooperation (PESCO)'s projects - Overview, 2018, pp. 3, 17). CTIRISP and the EU CAIH are expected to deliver on their goals by 2020, though the launch of the EU CAIH was postponed due to Covid-19 (see appendix D), whilst CRRTs is expected to deliver between 2022-2024 (Béraud-Sudreau et al., 2019, p. 6). The CIDCC has not put forth official dates for when the projects are expected to achieve their goals.

Information on PESCO's cyber initiatives is scarce, and information on the CIDCC, the CTIRISP and the EU CAIH especially amounts to next-to-nothing apart from the official mission statements provided by PESCO[8]. What can be gathered from the official intention, however, is that the CIDCC will become a future center for information and capability-sharing, creating a platform for member states to cooperate on cyberthreat management and cyber operations. This center will allow member states to voluntarily pick between those threats they deem especially crucial and will thus provide an institutional basis for cooperation between states on a voluntary case-by-case basis (Permanent Structured Cooperation (PESCO)'s projects - Overview, 2018, p. 17). Similarly, the CTIRISP will provide a platform for states to share cyberthreat intelligence and develop new measures to increase their cybersecurity capabilities (Permanent Structured Cooperation (PESCO)'s projects - Overview, 2018, p. 14). What could be asked, however, is whether two strikingly similar-yet-independent initiatives are actually necessary, or if a single initiative with a slightly broader mandate to cover both might not help streamline PESCO's cyber initiatives?

Putting this critique aside, the two initiatives may have potential: Following a small state logic, in an interview, former Danish Minister of Defence Hjort Frederiksen told the authors that one of the main cyber-related priorities for Denmark and the DDIS in particular should be to help establish common sets of rules and norms regarding the management of and

[8] To make up for the lack of accessible information regarding the CI DCC, CTIRISP and EU CAIH, the group discovered a list of PESCO initiative spokespersons, whom the group chose to contact via email. At the time of handing in the thesis, only the spokesperson of the EU CAIH initiative, António Esteves Martins, has replied to the group's questions.

intelligence-sharing concerning cyberthreats and cyberattacks (Interview Claus Hjort Frederiksen, 2020, 12:20-20:50). From this point of view, though little more than the initial intentions of the CIDCC and the CTIRISP have been made public, these initiatives might eventually provide platforms for Denmark to help establish a shared set of norms and rules. Thus, following the logic of small state theorists (Crandall & Allan, 2015, p. 363; Krasner, 1981, pp. 121-122), if Denmark was to make use of its potential of becoming a norm entrepreneur in cyberspace, membership of the CIDCC and the CTIRISP might prove valuable to Danish interests.

With a different focus, but equally shallowly described, the EU CAIH aims to establish an institution for shared innovation and education in fields related to cybersecurity. In PESCO's words:

> "*The project of EU CAIH can add value by enhancing the creation of an innovative web of knowledge for cyber defence and cyber security education and training, providing a vital contribution to strengthening national, NATO and EU's capability to defend against the threats of the digital world.*" (Permanent Structured Cooperation (PESCO)'s projects - Overview, 2018, p. 3).

Clearly, though, the initiative sees great complementarity in EU and NATO cybersecurity policies, something which the spokesperson of the initiative, António Esteves Martins, also stressed in an email to the authors. In fact, the initiative itself is built upon past Portuguese experience from EU and NATO cyber education projects and will, according to Martins, focus highly on not duplicating capabilities already found in NATO (see appendix D). Though not joining the initiative through the EU, Martins pointed out that NATO members may access the imitative upon signing a Memorandum of Understanding, which would allow Denmark as a NATO partner with an opt-out on defense to still be allowed to partake in the initiative.

Contrary to the other three projects, the Lithuanian-led '*Cyber Rapid Response Teams and Mutual Assistance in Cyber Security'* (CRRTs) has delivered more tangible results. Shortly after its establishment, the CRRTs cooperating states, Lithuania, Estonia, Croatia, Romania, Spain and the Netherlands, signed an agreement to aid each other in the development of stronger European cyber defense capabilities by bringing together experts from the participating states to be on stand-by for swift investigation and neutralization of cyber incidents (EEAS, 2018a). Out of all PESCO's initiatives, deputy secretary general of the EEAS, Serrano, has emphasizes CRRTs as the most advanced project within the framework of PESCO (EEAS,

2018a). In a declaration of intent, the Lithuanian Minister for Defense highlighted the possibility of having the national CSIRTs cooperate within the framework of the project for swift handling of cyber incidents. This, combined with the creation of a shared set of cyber incident toolkits, should provide the necessary means for CRRTs to reach its initial operational level by 2019 (Lithuanian Minister for Defence, 2018, p. 2).

The CRRTs initiative conducted its first training exercise called "Cyber Shield/Amber Mist" in Lithuania in 2018 with the initial six members as well as France, Finland and Poland as participants and Belgium, Germany, Greece and Slovenia as observers (Vasiliauskaitė & Šakūnas, 2018, p. 7). During the exercise, each of the nine participating member states appointed one person of contact, who would join a Council in which strategies and priorities for the initiative were decided upon. Taking turns to lead the CRRTs initiative, the leading member state at any given time would furthermore appoint a Chairman whose job was to set the agenda during meetings and act as the main point of contact for member states affected by a cyberattack (Vasiliauskaitė & Šakūnas, 2018, p. 9). Additionally, a mission coordinator was appointed to compose and lead a team of experts to aid the member state under attack. By setting up a fictitious cyberattack, the participating member states used the exercise to test the CRRTs' effectiveness at responding to threats in cyberspace (Vasiliauskaitė & Šakūnas, 2018, p. 15).

With the framework applied during the "Cyber Shield/Amber Mist" exercise, if a member state comes under attack, (one of) the national CSIRT(s) would have the responsibility of submitting a request to the CRRTs Council Chairman, which would then decide whether or not a mission coordinator should assemble a team and travel to the affected country to aid the national CSIRT in handling the incident (Vasiliauskaitė & Šakūnas, 2018, p. 12). By having the national CSIRT contact the Chairman, the member state affected by the cyberattack allows the CRRT to act within its territory. Without permission, the CRRTs cannot act on other national territories (Vasiliauskaitė & Šakūnas, 2018, p. 12). To decide whether an attack is serious enough for action, paragraphs 27 and 28 of the NIS directive will serve as a guideline, deeming attacks on the energy, financial, transport, health as well as food and water supply sectors especially critical (NIS Directive, 2016, p. 5).

With experts appointed by the member states on stand-by, whom the mission coordinator can pick from in putting together a CRRT, the CRRTs initiative is the closest PESCO comes to creating an actual, operational cyber alliance. However, in deciding the severity of the attack and whether or not a CRRT is to be deployed, every member state must consent to the

deployment (Vasiliauskaitė & Šakūnas, 2018, p. 17). This means that any member state participating in the CRRTs initiative essentially holds the power to veto the deployment if it does not wish to partake. In this way, the initiative holds a guarantee for small states against great power dictation, which, according to Rothstein and Dosenrode (Dosenrode, 1994, p. 246; Rothstein, 1968, p. 61), would arguably allow a small state like Denmark to join the initiative without much concern for its self-determination.

As nascent initiatives, no fair assessment of the true potential of these four PESCO cybersecurity projects can be made. Still, if PESCO has success with delivering on these four projects, the cooperation may just provide new shared European initiatives for capacity development, intelligence-sharing and operation capabilities in cyberspace. As Krasner and Thorhallsson & Wivel argue, small states can make great use of international institutions to shape rules to their own advantage (Krasner, 1981, p. 126; Thorhallsson & Wivel, 2006, p. 663). Arguably, with fora to discuss cyber-related issues, a small state like Denmark could gain benefits from certain PESCO initiatives like CTIRISP and CI DCC, whilst the more alliance-like CRRTs initiative seems to show great potential for small states to address and act on cyberattacks without Vital's and Rothstein's fear that great powers may take advantage of the small states due to their relative weakness (Rothstein, 1968, p. 61; Vital, 1967/2006, pp. 84-85).

9.2.2 EU strategies: Sanctions and criminal prosecution

Like NATO, the EU has attempted to develop a credible cyber strategy. Contrary to the military focus of NATO, EU cyber deterrence relies more heavily on sanctions and criminal prosecution. In achieving these goals, the Commission has highlighted the importance of creating a strong defensive base centered around PESCO cooperation and developing a comprehensive set of possible responsive measures against aggressors such as sanctions as well as swift and effective prosecution of cybercrime conducting against the Union and its members (European Commission, 2017, pp. 13–17).

9.2.2.1 The EU cyber diplomacy toolbox: Sanctions as restrictive measures

In recent years, the EU has developed a sophisticated sanctions regime against states, as well as non-state actors in an attempt to strengthen conflict management, countering terrorism and promoting democracy and human rights (Moret & Pawlak, 2017, p. 2). With its Cyber Diplomacy Toolbox, which was agreed upon in 2016 and finalized in May 2019, the EU would allow itself to impose sanctions against criminal groups and states responsible for cyberattacks or attempted cyberattacks (van Dijk, 2019). As one of the most forceful measures the EU can

apply, these would logically be a strong addition to the EU's cyber response. However, in order for the EU to sanction a group or a state, unanimity among member states is required. With the attribution problem in cyberspace, getting all member states to collectively agree upon attributing an attack to a certain group of state may likely prove difficult and may cause hesitation from certain members (van Dijk, 2019). As such, the EU has failed to sanction states or groups following severe ransomware attacks against many of the EU member states, and it was only when four Russians operatives were caught red handed in the middle of an attack against the Organisation for the Prohibition of Chemical Weapons in the Hague that the EU was able to unanimously agree on attribution (van Dijk, 2019).

As of yet, the ability of the EU to sanctions groups and states as a response to cyberattacks is still a newly acquired tool, so whether it will be an effective weapon has still to show. Though unanimous attribution is likely to become a hindrance in cyberspace, if successful, sanctions have been argued to provide an appealing middle-ground between diplomacy on the one hand and war as a last resort on the other (Moret & Pawlak, 2017, p. 2). Further, it has been argued that sanctions may provide effective indirect deterrence against cybercriminal groups because states from which cybercriminals operate may face sanctions on a state-wide level and will, as such, feel pressured to take stronger measures against criminals (van Dijk, 2019). As EU sanctions against cyberattackers might help deter state-sponsored and criminal cyberattacks, small state theorists such as Krasner and Crandall & Allan (Crandall & Allan, 2015, p. 363; Krasner, 1981, p. 122) would argue that it would be valuable for a small state like Denmark to push for the development of clear rules and norms regarding the EU cyber sanctions cooperation.

9.2.3 Europol - Role and operational function

Having examined possible cyberdefense measures within NATO and the EU, this section will illuminate the European law enforcement perspective by examining the police body of the EU, Europol. Europol has the responsibility of fighting cybercrime on a European level. Europol's purpose is to increase efficiency and cooperation between authorities in the EU member states on fighting all cross-border crime, including cybercrime. Europol was established with the Maastricht treaty in 1992 and currently covers a broad field from cybercrime to terrorism, financed by the common EU budget (EU forordning 2016/794 om Europol, 2016, p. 53). Led by a director and a board of direction, consisting of one member from each member state and a

member from the EC, decisions like the choice of director, budget and several year programming are passed with a majority of 2/3 in the board of direction (EU forordning 2016/794 om Europol, 2016). The expenditure of Europol is on a rise as it was €154 million in 2020, coming from €141 million in 2019 and €135 million in 2018 (Europol, 2020).

On an operational level, Europol is a supranational unit of the EU that collects information from the member states, relevant to fighting cross-border crime. Europol distributes the information directly to representatives of the member states, who then decide how to proceed, in cooperation with other relevant member states or on their own (EU forordning 2016/794 om Europol, 2016). Europol can distribute the given data to any other EU organs, 3rd countries (partner countries), international organizations and private partners (EU forordning 2016/794 om Europol, 2016). As an EU agency, Europol has the status of a legal entity and can be a part in litigations but is not a judicial body with prosecution power. Europol can distribute information and ask the given member state to litigate a case on the basis of the given information. All decisions made by the member states regarding the information provided by Europol, including if they chose to litigate or not, are logged and sent to the EU agency for Criminal Justice Cooperation, Eurojust[9] (EU forordning 2016/794 om Europol, 2016). As Europol and Eurojust are EU agencies with no prosecution power or legal body status, the information collected by Europol can only be litigated by member state authorities or the supranational EU Court of Justice.

9.2.3.1 Denmark's relationship with Europol

As the EU regulation on Europol from 2016 was set to make Europol supranational in 2017, the regulation conflicted with Denmark's EU opt-out on AFSJ, and as a result Denmark, had to step out as a member of Europol. A special agreement was made for Denmark to step out as a member of Europol and be considered a partner with the status as a 3rd country, meaning that Denmark will not have direct access to information stored by Europol (Europol, 2017, p. 2). The special agreement dictates that the area of cooperation between Denmark and Europol is the sharing of information, related to fighting cross-border crime (Europol, 2017). According to the agreement, all information from Europol to Denmark shall go through the national Danish authorities contact point in Copenhagen (Europol, 2017). The operational difference between the status of Denmark and a Europol member state is therefore that Denmark does not have direct access to Europol data but will have to go through a third link. Denmark will thus still be

[9] Denmark has a similar relationship to Eurojust as it has with Europol, as an observer-state.

notified with relevant information from Europol investigations and be a part of the Europol cooperation in general, as any other member state. On a higher institutional level, Denmark is left out of the decision-making process as it is not a member and therefore has no right to vote on any matters whatsoever in the board of directions (Europol, 2017). While Krasner may argue that a small state like Denmark would stand to gain political influence from entering into tighter cooperation in Europol (Krasner, 1981, p. 122), Dosenrode points out that small states tend to value intergovernmental cooperations to supranational ones (Dosenrode, 1994, p. 248), which explains Denmark's reluctance to engage fully in Europol after the 2017 change in Europol's status from intergovernmental to supranational.

9.2.3.2 The Europol collaboration's current value to Denmark and potential value

After Denmark's decision to step out of Europol and securing a special agreement, the Danish government ordered a review in 2019 from the Danish Department of Justice to determine what the special agreement meant in terms of cross-border crime-fighting. The report concludes that the Europol cooperation is of great operational value within the terms of the special agreement at the time (Justitsministeriet, 2019, p. 12). However, it is also concluded that it has had operational consequences for the Danish National Police to have stepped out of the Europol as a member. It is concluded that as a result to Denmark not being a member of Europol that the Danish police will be left behind the police of other EU member states (Justitsministeriet, 2019, p. 12).

One of the factors being pointed towards as negatives for the Danish National Police, is the increased time required in the process of acquiring data through a third part as a result of not having direct access. This is described as a significant obstacle for Danish Police work and will become more critical in the future as the Europol data systems will increase integration with its member states national police (Justitsministeriet, 2019, p. 2). It was furthermore concluded by the Danish National Police in 2016 that the European Police cooperation under Europol is developing rapidly, and with special regards to the technological opportunities Europol offers, that the members of Europol will have more effective tools available than the Danish Police and that the Danish Police will have limited options in making use of these tools (Statsministeriet, 2016, p. 1). The Danish National Police concludes the following on the impact of the use of Europol data in their investigations:

> *"It is assessed by the National Police, that the missing direct search access, including especially the missing access to QUEST* (red. Mobile Europol data base) *and the missing possibility to let information from Europol to be directly included as a*

> *supporting data source in the analytical and proactive crimefighting work, within a very short period of time will imply a significant limitation of the Danish Police's possibilities to fight cross-border crime compared to members of Europol."*[10] (Justitsministeriet, 2019, p. 10).

The Danish National Police therefore assesses to be in a place behind the members of Europol in terms of cross-border crime fighting, especially when it comes to the use of data in their analytical work. The increased use of data in Danish police investigations can be seen by the increase of searches made by the Danish police from 2017 to 2018 (Weichardt, 2019). The Danish National Police had an increased in the use of the EIS database[11] from around 88,000 searches in 2017 to 159,326 in 2018, which was the first full year where Denmark was not a member of Europol. It is further assessed that 2019 would have a further increase as the number of searches in 2018 was met before the end of 2019, where the article including these sources was released (Weichardt, 2019).

The Chief of the Danish National Police at the time, John Vestergaard, describes the reason for the increase as following in January 2019: "[…] *the challenge is, that we are increasingly data-based in our analysis work. It was meant that the databases of Europol should have been a part of that plan, and then they are not."*[12] (Weichardt, 2019). As Vestergaard explains, the Danish police's work is affected primarily in the field of data, which is the main resource Europol provides for its members with the current special agreement between Denmark and Europol. With the assessment by the Danish National Police and Danish Justice Department, also pointing to this particular weakness, it becomes evident that Denmark is vulnerable in terms of acquiring data for fighting cross-border crime compared to Europol members, which seems to underline Burton's point that small states, without international co-operation, lack the necessary tools to respond to global cybercrime (Burton, 2013, p. 224). To assess the current and potential European cybercrime threat and the importance of data in this context, the threat assessment of the operational cybercrime unit of Europol, the European Cybercrime Centre (EC3), is further examined.

[10] Translated from Danish by the authors.
[11] Europol Information System: Intelligence database for Europol member states and 3rd countries.
[12] Translated from Danish by the authors.

9.2.3.3 The European Cybercrime Centre and threat assessment

The EC3 is Europol's Operations Directorate and operational unit for fighting cybercrime. The process of the Europol Cyber Intelligence sharing is similar to the general Europol process where information is collected and shared with the relevant countries.

For targeted actions against cybercrime, the EU, in cooperation with the US and Canada, launched the Joint Cybercrime Actions Taskforce (J-CAT) in 2014. It counts 9 EU member states, in which Denmark is not a member, 7 non-EU partner countries and the EC3 of Europol. The aim of the taskforce is a strategic and operational cooperation to fight cybercrime, with a similar process to that of Europol, focused on gathering intelligence and starting investigations in cooperation with its members. From its start in 2014 it has completed 70 successful high-profile operations by 2019, including prosecuting the perpetrators behind the so-called IM-RAT Trojan Horse used across 124 countries (Europol, n.d.-c).

Evident by the EC joint communication to the European Parliament and EUCO on cyber resilience, deterrence and defense from 2017, the EC encourages the attempt to achieve cyber-deterrence by law enforcement. The EC points directly to the development of the EC3 of Europol to support cross-border cybercrime investigations (European Commission, 2017). As mentioned, a way of creating cyber-deterrence on a European level could be to show that cybercrime is punished and litigated successfully through Europol and the EC3, making cybercriminals think twice before committing cybercrime within the EU. This can be done through public opinion and media, in which Europol in general clearly makes an effort in showcasing its results (Europol, n.d.-b). The EC3 clearly uses the same tactics exemplified in the J-CAT taskforce cooperation, in which Denmark does not partake. The operations conducted by J-CAT are put out publicly and can have a deterring effect for cybercriminals as J-CAT shows its strength in numbers of litigations and legal actions it has supported and in high profile operations with an increasing number each year (Europol, n.d.-c). Along with the increasing number of successful operations conducted, Europol, however, assesses an increasing tendency in cybercrime on a European level.

According to Europol, cybercrime is an increasing threat, and data is considered *"*[…] *a key target, commodity and enabler for cybercrime."* (Europol, 2019, p. 8). EC3 publishes an annual Internet Organised Crime Threat Assessment (IOCTA), which is the flagship strategic report on key findings and developments in cybercrime. The primary focal point of the IOCTA 2019 points towards data as the turning point of most cyber threats. The assessment

of cybercrime as a crime area and the threat assessment of internet-dependent countries is further elaborated in the following way by Europol:

> *"According to the most recent Internet Organised Crime Threat Assessment (IOCTA), cybercrime is becoming more aggressive and confrontational* […] *The number and frequency of data breaches are on the rise, and this in turn is leading to more cases of fraud and extortion."* (Europol, n.d.-a).

Europol's assessment points towards data breaches, within all sectors, as being a key target for criminals, who are acting more aggressively and confrontationally. Furthermore, countries highly dependent on the internet, such as Denmark, are pointed towards in terms of having a growing risk of data breaches, since essential infrastructure like payment systems are online. The 2019 IOCTA furthers the importance of data in cybercrime:

> *"This year's IOCTA demonstrates that for all cybercrime, data remains the key element, both from a crime perspective and from an investigative perspective.* […] *Whereas criminals require data for most of their crimes, law enforcement needs access to relevant data for their investigations. Indeed, the ability of law enforcement agencies to access the data needed to conduct criminal investigations is an increasing challenge."* (Europol, 2019, p. 6)

The IOCTA points to data being important on both sides of a cybercrime, for the criminals and for the investigators. As mentioned, data is a crime enabler for a cybercriminal but is also an important tool used by law-enforcement in their investigations, in which technological development increases the difficulty of fighting cybercrime. Thus, because Denmark, as a third country, does not have direct access to Europol data, small state theorists Burton and Krasner would argue that Denmark would be at a considerable disadvantage in comparison to Europol members (Burton, 2013, p. 224; Kranser, 1981, p. 120).

However, the barriers of acquiring data is not solely a technological question according to the IOCTA:

> *"These barriers are often related to the principle of territoriality, which sets limits to the scope of jurisdiction and to the investigative powers which law enforcement and judiciary have at their disposal under their national law. As a result, the tools in the hands of investigators and prosecutors do not correspond to what would be*

> *needed to deal with data flows, for which questions of territoriality are of no relevance."* (Europol, 2019, p. 7).

The cross-border nature of cyberattacks erases the question of territoriality according to the IOCTA. Territoriality limits the capabilities of national law enforcement as national jurisdiction and the investigative powers are bound to their respective countries' territories. As a result, the tools needed for law-enforcement are not sufficient to deal with the current threat of data-based cyberattacks, due to the limitations of national jurisdiction being bound on territoriality. Cybercrime threats do not differ between sectors, and the fluid nature of cyberspace makes for a complex threat on supply chains. Europol expects growth in attacks on digitizes supply chains and calls for tightened synergies between cybersecurity agencies and law enforcement (Europol, 2019, p. 7). With this strategy, Europol puts a focus on addressing issues posed by the cross-border nature of cybercrime.

In terms of further policy recommendations, IOCTA 2019 points to the following areas of action for authorities:

> *"Enhanced cooperation and improved data sharing between law enforcement, computer security incident response teams and private partners will be the key to tackling complex cyberattacks* […]*"* (Europol, 2019, p. 10).

Europol points to enhanced cooperation and an improvement in data-sharing as being central. Closer cooperation is recommended for authorities and private partners for building cyber resilience, as well as on a European level in the fight against cross-border cybercrime. Europol suggests exploring all channels of cooperation, pointing directly to the capabilities of Europol and Eurojust, legal and operational, for resources-sharing and coordination purposes.

Conclusively, the issue of data accessibility is understood by Europol as being vital, and an area deemed vulnerable in the case of Denmark compared to Europol members. Data accessibility was assessed by the Danish Department of Justice as an area where Denmark currently lacks capabilities, with a projected increase in vulnerability in the future compared to Europol members by the aforementioned report on Danish law enforcement. Furthermore, the former mentioned assessment of former Chief of Danish National Police, Vestergaard, points to data as a key part of the analytical and crime preventive efforts of the Danish Police. With the current special agreement Denmark has with Europol the missing accessibility of data is illuminated by Vestergaard, to have had a negative effect on the capabilities of the Danish Police.

According to small state theorists, European small states benefit highly from international cooperation with strong institutions, like the EU, and have a specific strong interest in effective EU policymaking as highlighted by Thorhallsson & Wivel (Thorhallsson & Wivel, 2006, p. 663). Evident by the examination of Europol and the assessment from the Danish National Police, Denmark would benefit highly from the Europol cooperation in terms of cybercrime law enforcement. In addition, Krasner argues that small states create and shape institutions to make up for their relative weakness (Krasner, 1981, p. 126). By entering into closer cooperation with Europol, Denmark would thus gain greater influence on the international fight against cybercrime and would arguably be able strengthen its cybersecurity by drawing on intelligence and expertise within Europol.

Evident in the function and nature of the Europol cooperation, any member and partner of the Europol cooperation benefits in terms of data and intelligence from all of the Europol members and partners. In isolated terms of data and intelligence, a small state like Denmark benefits from the overall power and efficiency of the whole Europol organization gaining data and intelligence from all members and partners, including European great powers as Germany and France, and to some extent the world leader and superpower USA, for whom Europol has an operational agreement with, including its Federal Bureau of Investigations (FBI) as a partner (Europol, n.d.-d; United States of America & Europol, 2001). Therefore, in terms of data and intelligence-sharing the Europol cooperation is highly beneficial for Denmark, though, due to Denmark's status as a third country, it lacks behind the members of Europol significantly in terms of data accessibility, which is affecting the current crime-fighting efforts and is projected to have a further significant increase especially in the field of cybercrime according to Danish authorities.

On a decision-making level, Denmark as a third country has no voting rights, meaning that Denmark has no influence whatsoever on the broader policy decision-making process or budget priorities within Europol. Following Krasner's points (Krasner, 1981, p. 143), this arguably means that Denmark is missing a great possibility of shaping institutional structures and principles to its benefits. Further, besides Denmark's lack in direct means of influence in this context, Denmark's missing influence in the decision-making of the Europol is also a barrier for norm-building efforts within Europol. With no possibilities of norm-building within Europol, Denmark does not have the ability to drive its policy preferences onwards or to cooperate with other small states with similar needs and policy preferences. Creating a bloc of small

states with similar policy preferences with the aim to create a domino effect, as argued by Thorhallson & Wivel (2006), could be considered effective and the EU is highlighted as an optimal arena for such efforts (Thorhallsson & Wivel, 2006, p. 664), but with its opt-out on AFSJ, though Europol would be an obvious arena, Denmark cannot fully utilize it to make up for its relative weakness in cyberspace.

The negative effects of Denmark not being a full member of Europol can be seen in the operational and the decision-making arenas of Europol. However, the reason for Denmark's decision to keep its EU opt-out on AFSJ and step out of Europol can be explained by small state theorists. Denmark stepped out of Europol as the status of Europol changed from being an intergovernmental organization to a supranational one, which conflicted with Denmark's EU opt on AFSJ. As argued by Rothstein and Vital, a small state might want to stay out of a supranational alliances unless absolutely necessary (Rothstein, 1968, p. 61; Vital, 1967/2006, pp. 84-85). Further argued by Dosenrode (1994) in the context of small states in the EU, small states tend to stay out of any cooperation that limits the small state's sovereignty and freedom and prefer international institutions where they can enter and leave as they please, as Denmark's current Europol status as a third country allows (Dosenrode, 1994, p. 248). The question is, therefore, if the cyberthreat, which is proved to be increasing and high by both Danish and EU authorities, will reach a level where Denmark's special agreement with Europol is no longer sufficient and it is assessed to be an absolute necessity to accept the concessions on national sovereignty to lift its opt-out to become a full member of Europol.

To summarize, there are several initiatives in the EU that can compensate for Denmark's relative weakness in cyberspace, which Denmark, however, paradoxically does not partake in. On the contrary, the analysis has shown that it is difficult to argue that NATO is the Danish cybersecurity guarantor. As shown, there are several PESCO initiatives, which could close the gaps that NATO does not cover for a small state like Denmark, and opportunities for Denmark to enhance its capabilities to fight cybercrime through Europol as well as gaining influence in its priorities. These findings make the thesis question why Denmark is not partaking in these EU initiatives, as it would be favorable for Denmark to make up for its relative weakness in cyberspace?

9.3 Danish reluctance to engage in closer EU cooperation

This section will illuminate if Denmark's reluctance to engage in deeper cooperation in the EU can be explained by looking at small states' ability and everlasting priority of ensuring self-

determination, as well as the relationship between domestic and external influence. It will commence by illuminating Danish cybersecurity capabilities and initiatives, followed by investigating US-Danish relations and lastly Danish domestic political reasons for not committing to closer EU cooperation.

9.3.1 Danish cybersecurity capacities and initiatives: a pursuit of self-determination?

This section will illuminate if Denmark's reluctance to engage in deeper cooperation in the EU can be explained by looking at a small state's ability to and everlasting priority of ensuring self-determination. Within small state theorists' articulation of whether small states should engage in international cooperation and alliances, an emphasis regarding self-determination and political maneuverability is evident. Baker Fox explains that small states should only engage in 'common causes' with larger entities if the state finds this to be absolutely necessary for its survival (Baker Fox, 1959, p. 1). Similarly, Vital argues that small states lose autonomy, independence and effective sovereignty when seeking protection through international cooperation (Vital, 1967/2006, pp. 79, 84-85). Based on a homogeneous understanding, Rothstein stresses that a small state should follow policies of non-alignment if it is not fundamentally threatened, since ensuring sovereignty is key for a small state to avoid being used as a pawn by great powers (Rothstein, 1968, p. 61).

Based on Rothstein, Vital and Baker Fox's arguments, small states should pursue a strategy of non-alignment to ensure their self-determination and maneuverability and only deviate from it, if they are threatened to the point where they cannot protect themselves. Following this line of argumentation, it will be investigated if the reason for Denmark's reluctance to engage in deep EU cooperation is based upon the assumption that Denmark is not threatened to the point where it cannot protect itself in cyberspace, thus favoring ensuring self-determination instead. However, as already established in the thesis, Denmark is facing serious cyberthreat against Danish interest (Centre for Cyber Security, 2019a, p. 2; Danish Defence Intelligence Service, 2019a, p. 8; Danish Ministry of Defence, 2018, pp. 2, 8-9). With these threats in mind, it is meaningful to explore Denmark's own ability to mitigate these threats in cyberspace. This will be done by examining Danish cybersecurity strategies, diplomatic efforts and the budgetary priorities and roles of Danish operative entities that have been established to mitigate the cyberthreat.

9.3.1.1 Centre for Cyber Security (CFCS)

Since 2011, the Ministry of Defence has been the authority with the main responsibility to coordinate efforts to ensure cybersecurity in Denmark (CXO, n.d.; DDIS, 2013). Furthermore, in 2014, a new regulatory framework was agreed upon to enhance the responsibilities and capabilities of the CFCS to investigate and prevent cyberattacks (CFSC, 2020). This framework and enhancement of the CFCS was highlighted by Aastrup Jensen of Venstre as groundbreaking in Denmark's ability to respond to cyberthreats (Interview Michael Aastrup Jensen, 2020, 4:00-7:45).

Operationally, the CFCS is the centerpiece of Danish efforts to handle cyberthreats (CFSC, 2020). The main objectives of the CFCS are to counter, prevent and protect against cyberattacks that target authorities and companies considered critical to Danish society (CFCS, 2016, p. 2; Interview Thomas Wulff of the CFCS, 2020, 6:30-7:30). The CFSC was established in 2012 and organized as a part of the DDIS. This structure is highlighted by the CFCS and former Minister of Defence Hjort Frederiksen of Venstre as important in ensuring intelligence from foreign intelligence agencies, proving vital for the CFCS's ability to counter, prevent and protect against foreign cyberattacks (CFCS, 2016, p. 2; Interview Claus Hjort Frederiksen, 2020, 4:00-6:00). In an interview between the authors and senior advisor Wulff of the CFCS, it was noted that there are different ways of organizing one's national cybersecurity authority. For example, Denmark's structure is similar to that of UK, whereas countries such as Germany and Sweden have organized their national cybersecurity authorities as civil institutions, resulting in different possibilities and limitations (Interview Thomas Wulff of the CFCS, 2020, 33:00-35:20). The Danish structure has, however, been criticized by Danish parliamentarian Nordqvist in 2019 for a lack of public transparency (Fagpressen, 2019).

Overall, the CFCS's method of ensuring its objectives is twofold. Firstly, it is advising private and public entities on how to increase their cybersecurity knowhow and capabilities in order to prevent cyberattacks or descale the effectiveness of an attack, as well as having regulatory oversight of the telecommunication sector (CFCS, 2016, pp. 2-3). Secondly, the CFCS monitors network activity in order to pinpoint advanced cyberattacks. If an attacked is deemed threatening by the CFCS, it will warn the targeted entity and advise how to address the threat, and in severe cases aid the targeted entity with a deployable operational groups of technical experts (CFCS, 2016, p. 2; Interview Thomas Wulff of the CFCS, 2020, 7:30-12:00). Though being an operational entity, the CFCS stresses that it is defensive in its core, and it does not conduct offensive cyberoperations (Interview Claus Hjort Frederiksen, 2020, 37:00-37:50).

Furthermore, the CFCS is tasked with publishing yearly cyberthreat assessments as well as contributing with public notification of specific cyberthreats (Centre for Cyber Security, 2019a). The latter is exemplified by a report published during the initial outbreak of the Covid-19 pandemic in March 2020 where the general cyberthreat increased as public and private employees were forced to work digitally from home, which made them more vulnerable to become targets to hostile cyberspace entities (CFCS, 2020a).

Moreover, the CFCS is partaking in international cooperation, primarily through NATO and the EU, where knowledge and expertise in technical and strategic matters are shared to ensure CFCS capabilities to increase and coordinate Danish cybersecurity efforts (CFCS, 2020b). This is exemplified by the CFCS having a permanent representative in ENISA's Management Board (ENISA, 2020, pp. 1-4), which also shows Denmark is able to fully cooperate in certain cybersecurity agencies in the EU regardless of its opt-outs. Moreover, in an interview with the authors, the CFCS noted that in every-day operational work, it is cooperating more with NATO than the EU, yet stressing ENISA as an important center of expertise-sharing and cybersecurity exercises (Interview Thomas Wulff of the CFCS, 2020, 21:30-23:30). The CFCS also assessed that the NIS directive is valuable in ensuring European network and information security but that the project is still in its initial implementation phase (Interview Thomas Wulff of the CFCS, 2020, 26:30-29:00). Notably, when asked how the CFCS values the possibility of cooperation through PESCO, it was answered that PESCO was not on their radar (Interview Thomas Wulff of the CFCS, 2020, 29:40-30:00). This could suggest that the PESCO initiatives are not perceived by the CFCS as initiatives with potential to strengthen Danish cybersecurity efforts as the national cybersecurity authority is not considering them. However, this lack of focus on PESCO is more likely a result of the fact that Denmark cannot partake in the PESCO initiatives, and therefore it is logically not something that is on the CFCS's radar.

Furthermore, it was also stressed that the CFCS does not operate or see any sense in separating cybersecurity into independent categories of cybercrime and cyberdefense (Interview Thomas Wulff of the CFCS, 2020, 32:30-33:00). Concurrently, the CFCS informed the authors that cooperation with Europol to counter cybercrime went through the Danish police, not the CFCS (Interview Thomas Wulff of the CFCS, 2020, 30:30-32:00), which arguably implies that there is either some sort of separation between cyberdefense and the handling of cybercrime, or that the CFCS does not have access to data in Europol to counter cybercrime.

To summarize, the CFCS does have protective capabilities against cyberthreats through expertise building, guidance to public and private entities, regulatory overview, threat

assessments, monitoring of networks as well as responding to hostile cyberthreats. In order to further assess Danish capabilities to secure itself in cyberspace, the following section will focus on Danish military spending on cybersecurity.

9.3.1.2 Recent Danish cyber initiatives and strategies

As discussed earlier in the thesis, Giegerich argues that it can be difficult to examine a state's cybersecurity capabilities as these are often structured in intelligence agencies and therefore clouded in secrecy (Danish Defense Committee, 2019, 2:20-2:30). However, it might prove useful to 'follow the money' to gain further insights of Denmark's cybersecurity capacity.

In the Danish Defense Agreement from 2018, it was agreed upon an overall 20% increase in the Danish defense budget over a five-year period (Danish Ministry of Defence, 2018, p. 3). With this agreement, 1.4 billion DKK is to be spend over five years to strengthen Danish cyberdefense capabilities with an overall reserve of an additional 500 million DKK set aside for education and research if found necessary (Danish Ministry of Defence, 2018, p. 10). A portion of this increased budget has been used to establishing a 'situation center' structured under the CFCS as a 24-hour manned entity to monitor cyberthreats (Danish Ministry of Defence, 2018, pp. 9-10). Further, a part of the budget was set aside to enhance the DDIS's offensive cyber capacities as well as strengthen cybersecurity expertise and prioritize guidance to public and private entities in order to increase cybersecurity capabilities. Moreover, resources were set aside to assure Danish participation in NATO's CCDCOE in Tallinn and the European Centre for Excellence for Countering Hybrid Threats in Helsinki (Danish Ministry of Defence, 2018, pp. 9-10). Arguably, in the defense agreement, Danish politicians follow Krasner's logic of utilizing international institutions to gain greater influence and compensate for Denmark's relative weakness in cyberspace (Krasner, 1981, p. 126).

As evident from the Defense Agreement, Denmark's cybersecurity capabilities have been prioritized, strengthening operational cybersecurity entities, enhancing IT-human capital and prioritizing knowledge-sharing through international cooperation. The large military budget increase could suggest that Denmark attempts to protect itself in cyberspace, rather than having to rely on international cooperation, ensuring Danish self-determination (Vital, 2006, pp. 84–85). However, the overall 20% increase in military spending should be seen in context of the NATO Wales declaration in 2014, where NATO members agreed to move towards spending 2% of their GDP on defense (NATO, 2014). In addition, the current US President Trump with his 'America First' policy questions US obligations to securing Europe

(Kaufman, 2017, p. 251), as well as stressing the need for NATO member states to spend additional resources on defending themselves, exemplified by Trump tweeting: "*All NATO Nations must meet their 2% commitment, and that must ultimately go to 4%.*" (Haltiwagner, 2019). It becomes evident that the NATO obligation to reach 2% of GDP on defense spending is the primary reason for the Danish 20% increase, as it is explicitly stated in the current Danish Foreign and Security Policy Strategy 2019-2020 that:

> […] *the 2014 NATO Summit obliges member states to work towards allocating 2% of GDP to defence* […] *like-minded countries, whose spending has been similar to Danish levels, will increase their defence spending. Therefore, we should expect that pressure to increase our defence spending will continue."* (Ministry of Foreign Affairs of Denmark, 2018a, p. 11).

As Handel argues, small state's foreign policy tend to be determined largely by the great power foreign policy and pressure (Handel, 1981/1990, p. 261). With this in mind, in Denmark's case, external pressure was more likely the reason for Denmark's overall 20% increase in military spending, rather than an example of a small state attempting to secure itself by its own means to preserve self-determination and avoid being reliant on international cooperation to protect itself from cyberthreats. In that regard, it seems favorable that the CFSC has been structured under the Ministry of Defense, rather than as civil unit as in Sweden or Germany as this means that any investment in the CFCS brings Denmark closer to its 2% GDP benchmark for defense spending. In this way, though the result of Denmark's increased spending on cybersecurity capabilities would theoretically suggest that Denmark is enhancing its ability to ensure self-determination (e.g. Vital, 1967/2006, pp. 84–85), the decision behind these investments is arguably grounded in pleasing the largest power in its military alliance by complying to US pressure on Denmark to increase its defense spending. This will be further discussed in the next section.

Moreover, Denmark has also implemented the NCISSs, with the first covering 2015-2016 and the overall frame of raising awareness of cyber and information security among private and public entities (Government of Denmark, 2018, p. 11). The second NCISS was implemented in May 2018, covering the period 2018-2021. This strategy highlights three main initiatives, i.e. 'Everyday Safety', 'Better Competencies' and 'Joint Efforts', in order to enhance Danish cyber and information security (Government of Denmark, 2018, p. 17). In short, 'Everyday Safety' means increasing the technological preparedness in critical sectors (Government of Denmark, 2018, pp. 20-25), 'Better Competencies' aim at ensuring the required knowledge

public and private entities rely on to handle the increasing cyberthreat level (Government of Denmark, 2018, pp. 28-33), and 'Joint Efforts' can be summed up as a strategic plan to ensure cybersecurity management in critical sectors and clearly pinpoint roles and responsibilities (Government of Denmark, 2018, pp. 36-45).

It should be noted that the publication of the Danish NCISS in May 2018 was also the deadline set by the EU to comply to the NIS directive to implement a national strategy for security of network and information systems (EC Europe, 2020; Nielsen, 2018). The argument that the Danish NCISS originates as a compliance to the NIS directive is reflected in the content as well. For example, the initiatives in the Danish NCISS focus on the maritime, finance, healthcare, energy, transport, telecommunication, and central governmental organizational sectors (Government of Denmark, 2018, p. 14), which are proscribed to be prioritized in the NIS directive (NIS Directive, 2016, pp. 1, 5).

Comparable with the Defense Agreement, it seems that external pressure has been the main reason for the creation of the Danish NCISS, yet the NCISS, similarly with the Defense Agreement, also entails initiatives that enhance Danish cybersecurity capabilities. In this way, it is noticeable that the arguably two most comprehensive initiatives to strengthen Danish cybersecurity capabilities have come as results of external influence by NATO and the EU respectively. This tendency is arguably reflective of how small states act within alliances, by trying to keep great powers commitment in the small state (Handel, 1981/1990, p. 122), rather than a way for Denmark to ensure self-determination by being able to protect itself from cyberthreats to the point, where it does not rely on international protection (Baker Fox, 1959, p. 1; Vital, 1967/2006, p. 79).

9.3.1.3 Danish cyber diplomacy and cyber norm-building

Building on Baker Fox's argument that small states should avoid engaging in 'common causes' with great powers and may therefore instead wish to utilize diplomatic efforts as a tool to increase their political influence and maneuverability (Baker Fox, 1959, pp. 1-3), it will be examined if Denmark is prioritizing diplomatic efforts to enhance its ability to secure itself in cyberspace. As Crandall and Allan (2015) show, it is possible for a small state to build cybersecurity norms with the aim of ensuring international rules (Crandall & Allan, 2015, p. 358), which generally favor small states (Goetschel, 2011, p. 326; Krasner, 1981, p. 122). In the current Danish Foreign and Security Policy Strategy, a desire for building cybersecurity norms is also stated:

> "*There is a lack of common understanding regarding responsible state behaviour in cyberspace. This increases the risk of misunderstandings and escalation.* […] *We have a clear interest in a secure, free and open global IT infrastructure based on common rules and cooperation* […]" (Government of Denmark, 2018b, p. 13).

The primary example of Danish cybersecurity norm-building would arguably be the Ministry of Foreign Affairs' 'TechPlomacy' initiative, which was established in 2017 (Ministry of Foreign Affairs of Denmark, n.d., 2018b). However, when investigating more closely, of what the so-called 'Tech Ambassador's' objectives are, it becomes evident that the emphasis is on strengthening Danish trade through cooperation with large tech companies (Ministry of Foreign Affairs of Denmark, 2018b). This can be further stressed by looking at where the Tech Ambassador is situated, being mainly in the Silicon Valley (The Trade Council, 2018), which is regarded as the world's leading tech developing area (Amadeo, 2019). The fact that the Danish Tech Ambassador is organized under the Danish Trade Council, whose main objective is to promote export opportunities for Danish companies (Ministry of Foreign Affairs of Denmark, 2020), suggests that the Danish 'TechPlomacy' initiative is more concerned with economic opportunities through digitization and technological innovation than addressing the security risks which digitization brings with it. Jacobsen (2017) argues that the lack of Danish international involvement in norm-building means that Denmark is counting on other countries to defend Danish interest in creating norms for state behavior in cyberspace (Jacobsen, 2017 p.13). However, in the Danish NCISS from 2018, it was decided to introduce two cyber attachés to the Danish Representation to the EU and a cybersecurity advisor to the already implemented Tech Ambassador in the Silicon Valley (The Danish Government, 2018 p. 44). This demonstrates a Danish priority to cybersecurity issues in diplomatic missions, though it is inarguably not comparable with the initiatives conducted by Estonia on the matter.

From a small state perspective, the lack of Danish norm-building in cybersecurity issues through diplomacy arguably means that Denmark is not utilizing its potential to increase its influence on the issues that arise from cyberspace (Crandall & Allan, 2015, p. 363). Furthermore, this thesis has not been able to find open sources of Danish politicians articulating or 'dramatizing' cybersecurity issues in a way that can be compared with the Estonian President for example (Ilves, 2013). The authors of the thesis have interviewed several Danish politicians and asked all of them, which initiatives they regard as having been important for Danish cybersecurity, though none of them mentioned the Danish TechPlomacy initiative despite the Ministry of Foreign Affairs highlighting the initiative as its most important cyber diplomatic project

(Ministry of Foreign Affairs of Denmark, n.d., 2018b). Though this cannot lead this thesis to conclude that the Danish politicians interviewed see the Danish TechPlomacy initiative as something unimportant for Danish cybersecurity just because they did not mention it, their lack of attention might simply suggest they do not prioritize it in their assessment of important Danish cybersecurity initiatives. Similarly, all politicians interviewed in the thesis were also asked which initiatives they suggest could strengthen Danish cybersecurity, though, again, none of them, apart from Hjort Frederiksen, suggested the importance of any cyber norm-building initiatives. As before, this cannot lead the thesis to conclude that the politicians interviewed do not find norm-building initiatives important, but it does suggest they prioritize different initiatives higher.

However, Hjort Frederiksen of Venstre explained that during his time as minister, Denmark followed a norm-building strategy that consisted of going public when a public authority was hacked. The reason for doing so is to establish the norm that it is important for large entities to report incidents of cyberattacks, so that the authorities that handle cybersecurity have a better knowledge of the extent of the problem in Denmark. Especially private businesses have strong incentives to keep secrets if their customer data has been compromised because of the fear of losing customers. Therefore, Hjort Frederiksen suggests that making public authorities commence sharing incidents of cyberattacks could entice private businesses to follow suit.

Hjort Frederiksen also stressed that Denmark should try to create broad norm acceptance as it is important to establish these norms internationally in order for it to be effective (Interview Claus Hjort Frederiksen, 2020, 12:20-20:50). Arguably, many businesses are global, and even if Denmark establishes these norms domestically, global businesses might still be incentivized to keep cyberattacks a secret, because of the fear of losing customers in foreign markets that do not share similar norms. This would arguably motivate a small state like Denmark to pursue broad acceptance of its domestic cyber norms (Finnemore & Sikkink, 1998, p. 6). Notably, Hjort Frederiksen's successor, the current Minister of Defence, Trine Bramsen of Socialdemokratiet, shares similar views. Bramsen established the National Cybersecurity Council in 2019, which is a forum where authorities, businesses and researchers are able to share experiences of cyber incidents with the aim of strengthening cybersecurity capabilities across public and private entities (CFSC, n.d.; CXO, n.d.).

To summarize, there are few examples of Danish norm-building in cybersecurity areas, though it is stated as a goal in the current Danish Foreign and Security Policy Strategy.

In diplomacy, the TechPlomacy initiative seems to be more focused on ensuring economic growth through cooperation with large tech companies, rather than the security risks digitization brings with it. However, the current initiatives to encourage public and private entities to share experience of cyber incidents are specific examples of norm-building that ensure greater cybersecurity. Currently, this seems to be an initiative solely focused on domestic matters, rather than international ones, but if Denmark were to follow Crandall & Allan's and Guang's points (Crandall & Allan, 2015, p. 353; Guang, 2020, p. 169), it may be fruitful for Denmark to attempt to stand out as a norm-builder on cybersecurity issues.

9.3.2 Does Denmark disregard EU initiatives to show loyalty to NATO?

When trying to understand why Denmark does not engage in deep cooperation with the EU on cybersecurity, it can be argued that the Danish unwillingness is rooted in a strategy of keeping a close relationship with NATO. As outlined by Handel, small states should always work towards increasing their influence with the great powers and increase the great power's commitment to the alliance (Handel, 1981/1990, pp. 121-123). In this way, Handel argues that if small states are unable to compel the great power to support it, the great power might lose interest in the alliance and withdraw, something that will have catastrophic consequences for the small state.

When looking at Denmark's approach of not integrating more of cybersecurity with that of the EU, Handel's logic might provide insights. To understand this, one must be aware of the dynamics between European defense cooperation, such as PESCO, and NATO. As the greatest power of NATO, the US has not always been overly fond of PESCO as it leaves the US outside of influence of a European defense cooperation on the rise. In a letter to the former High Commissioner of Foreign affairs and Security, Mogherini, the US undersecretaries of Defense and State, Lord and Thompson expressed their concerns that the increasing defensive cooperation in the EU could be damning the cooperation in NATO. "*It is vital* […] *that independent EU initiatives like EDF and Pesco do not detract from Nato activities and Nato-EU co-operation.*" (Chazan & Peel, 2019). It is worth noting that the former Defense Minister of Germany and current President of the EC, von der Leyen, did not agree with this analysis, stating that the PESCO states "[…] *are doing what our American friends have been demanding we do for years. Our task now is to convince our allies that Nato will only profit from the efforts to create a European Defence Union*." (Chazan & Peel, 2019). NATO Secretary-General Stoltenberg has taken the middle-ground approach, stating that he is concerned about the creation

of PESCO and the challenges that arise if the efforts made in both organizations are not properly coordinated (Hošek, 2017).

Former Danish Minister of Foreign Affairs Uffe Ellemann-Jensen of Venstre believes that prestige and reputation are critical for Danish foreign, defense and security policies (P. V. Jakobsen et al., 2020, pp. 262-263). Ellemann-Jensen believes that Danish action taken in the Persian Gulf in the 1990s, with its participation in the UN peacekeeping mission was a direct desire to prove to the US that Denmark wanted to repair and rebuild a close relationship with Washington. This relationship had had its difficulties as a consequence of Denmark's opposition to NATO's request to deploy nuclear weapons in Europe in the 1980s (P. V. Jakobsen et al., 2020, pp. 262-263). Clearly in line with Handel's arguments, by taking action in the Persian Gulf in the 1990s, Denmark attempted to increase US interests and commitments of coming to Danish aid.

Ellemann-Jensen is, however, not the only Danish politician that uses this small state theoretical logic to explain Denmark's decision-making in the support of NATO and US-led military operations. The last six Prime Ministers, Poul Schlüter (C) (1982-1993), Poul Nyrup Rasmussen (A) (1993-2001), Ander Fogh Rasmussen (V) (2001-2009), Lars Løkke Rasmussen (V) (2009-2011 & 2015-2019), Helle Thorning-Schmidt (A) (2011-2015) and Mette Frederiksen (A) (2019-), have all used a similar logic to explain and create support for their NATO-US policies (P. V. Jakobsen et al., 2020, pp. 262-263).

It can be argued that this strategy was one of the arguments behind the implementation of the Danish Defense opt-out of the EU, as NATO was viewed as Denmark's sole security guarantor (Nissen et al., 2020, p. 13). With this strategy, Denmark has over the years considered itself to be a devoted and trustworthy NATO ally. For example, Denmark has supported the US in thick and thin over the last three decades which has led to Denmark supporting and contributing to all US-led NATO military operations since 1991 (Malmvig, 2019). Former US President Barack Obama used a familiar term of endearment in stating that Denmark "[…] *is a country that* […] *punches above its weight*." (Jyllands-Posten.dk, 2011). This approach has helped Denmark gain influence in NATO, and Denmark has in the last three decades established itself as an ally that is willing to pay what some perceive to be a 'moral debt' owed by Europe to the US for protecting it during the Cold War (Wivel and Crandall, 2019, p. 404).

Moreover, this strategy of gaining goodwill has, to some extent succeeded as it has given Denmark some leniency with NATO, meaning that Denmark has not been under

much pressure to live up to its 2% GDP benchmark in the military budget. As such, this strategy of maintaining goodwill may be one of the reasons why Denmark has been reluctant to engaging in closer EU defense cooperation, because the US has voiced concerns of PESCO.

However, the leniency towards European NATO partners has changed during Trump's presidency (P. V. Jakobsen et al., 2020, pp. 467-468), and some politicians in Denmark have started to question its pro-America policies after Trump became president (Fischer & Mouritzen, 2017, pp. 51–52; Interview Michael Aastrup Jensen, 2020, 15:30-17:00). Denmark has historically had broad consensuses when dealing with foreign policy, but this is something that seems to be challenged currently when it comes to increased cooperation within the EU on defense, seeing as disagreements between the two major parties, Venstre and Socialdemokratiet have started (Interview Claus Hjort Frederiksen, 2020, 26:20-27:30; Interview Christel Schaldemose, 2020, 5:00-6:00; Interview Michael Aastrup Jensen, 2020, 12:00-14:00; Niels Fuglsang, Appendix E).

To summarize, Denmark has taken an approach of almost solely utilizing the NATO alliance for its security, an approach that could be seen as Denmark neglecting other instruments to increase their security, including PESCO and the EU in general. Denmark has historically favored gaining influence in Washington and NATO. The approach taken by Denmark follows the logic of Handel in its attempt to keep US commitments to Danish interest (Handel, 1981/1990, pp. 122-123). However, with the current climate between Denmark and the US, some of the politicians interviewed for this thesis are starting to question the validity of the US as Denmark's sole security ally (Interview Karen Melchior, 2020, 8:00-11:30; Interview Michael Aastrup Jensen, 2020, 21:30-22:00). Nonetheless, only Melchior expressed a view that EU cooperation should be alternative, rather than complimentary, to NATO.

Though Denmark has historically attempted to gain good-will in the US, and this may, theoretically, be a reason for the Danish reluctance to engage in deep defense cooperation with the EU (see Handel, 1981/1990, pp. 122-123), it is worth nothing that 21 countries are members of both NATO and EU defense cooperation (NATO, 2020d). Thus, it seems difficult to argue that Danish reluctance to engage in deeper EU cooperation on defense stems from a fear of losing total US commitment, though it might result in a loss of good-will in the US.

9.3.3 Domestic political conditions for Danish reluctance to deep EU cooperation

As argued, the Danish EU defense opt-out prevents Denmark from taking part in the PESCO cooperation and to have a say on the EU CSDP. As argued, following a small state theoretical

logic (Krasner, 1981, p. 121), lifting the EU Defense opt-out could potentially improve Danish cybersecurity and make up for its relative weakness in cyberspace as it would allow Denmark to take advantage of CSDP initiatives and shape the defense policy of the EU and PESCO to its advantage.

Handel argues that small state foreign policy is largely controlled by great powers, whose foreign policy is controlled by domestic conditions (Handel, 1981/1990, p. 4). As argued, there may be several examples of Danish foreign policies being greatly influenced by great power politics, such as Denmark's strategy of gaining goodwill with the US, but as this section will elaborate, Danish domestic conditions seem to have a great impact on Denmark's reluctance to engage in deep EU cooperation on security matters.

As the current landscape looks, there seems to be a small majority (56%) in the Danish Parliament in favor of removing the EU defense opt-out (Folketinget, 2019b). By looking at their party programmes it is evident that Venstre, Radikale Venstre, Alternativet, Liberal Alliance and Konservative are in favor of removing the opt-out (Alternativet, n.d.; Det Konservative Folkeparti, n.d.; Liberal Alliance, n.d.; Radikale Venstre, n.d.; Venstre, n.d.). Socialistisk Folkeparti (SF) is, according to their party programme, open to having a discussion on the subject, but the spokesperson on defense, Holger K. Nielsen[13], declared that it was time to remove the opt-out during the election for the European Parliament in 2019 (Jydske Vestkysten, 2019; Socialistisk Folkeparti, n.d.). If Nielsen's views reflect that of the whole party, their, at-the-time 14 mandates, translating to 8% of the total mandates, the bloc in favor of removing the opt-out has a small majority of 98 mandates translating to 56% percent. The parties in favor of keeping the opt-out are the following: Socialdemokraterne, Enhedslisten and Dansk Folkeparti, translating into 77 mandates counting 44% of the parliament (Danmarks Radio, n.d.; Enhedslisten, 2019; Jyllands-Posten, 2019).

It can be concluded that on an official level, the Danish parliament is largely split in half on the issue of the Danish EU defense opt-out. However, Hjort Frederiksen and Aastrup Jensen from Venstre, assess there to be a broader consensus in the Danish Parliament in favor of removing the EU opt-out on defense, as they maintain that Socialdemokratiet is only reluctant due to tactical and political domestic reasons (Interview Claus Hjort Frederiksen, 2020,

[13] Notably, Nielsen was famous for his "Holger og konen siger nej til Unionen" campaign against European integration, which greatly influenced the national compromise which led to the four opt-outs (Holstein, 2018).

26:20-27:30; Interview Michael Aastrup Jensen, 2020, 12:00-14:00). Hjort Frederiksen states the following:

> *"I see many reasons to remove the defense opt-out. Time has totally run out for that opt-out, and I think that there is a broad majority in the Parliament that thinks that the time is right to remove the Defense opt-out. There are different assessments on whether it is desirable to have a referendum now on that matter – that is learnt by Brexit – and we also have the experience that a referendum can end with anything, so that is why the referendum is not held."* (Interview Claus Hjort Frederiksen, 2020).[14]

Hjort Frederiksen points towards the defense opt-out being outdated and only remaining because of domestic political reasons. He highlights Brexit as an external factor possibly influencing the Danish public opinion on EU matters and refers to the latest referendum Denmark had on its EU opt-out on AFSJ in 2015. The referendum of 2015 was held on whether to change the EU AFSJ opt-out to an opt-in. The referendum resulted in a no from the public, keeping the opt-out as it was. The result of the referendum came as a surprise for many as a majority of the parties in the Danish Parliament recommended to vote yes with a total of 111 mandates, translating to 63% (V, S, RV, K, SF, Å) against 64 mandates, translating to 37 % (DF, EL, LA) (Danmarks Statistik, 2015; Folketinget, 2015).

Arguably this shows that the 2015 referendum has left an impact and is present in the consciousness of Danish politicians when talking about a possible new referendum on EU matters. Interviewing EU parliamentarian Christel Schaldemose from Socialdemokraterne, she acknowledged the impact of the 2015 AFSJ referendum. However, despite being against having a referendum on the defense opt-out at the current moment, Schaldemose would vote in favor of removing the opt-out if the referendum came. Schaldemose stated that:

> *"I do not see the defense opt-out preventing us from cooperation* […]. *If we had a referendum, I would support removing it, but I do not see a reason to take that discussion. We know in general terms that it is hard to win a referendum with the public and there is no acute conditions that would cause having a referendum* […]

[14] Translated from Danish by the authors.

> *The problem of the defense opt-out it that it looks at security and defense in an old fashioned way."*[15] (Interview Christel Schaldemose, 2020, 5:00-6:40).

In terms of the defense opt-out, Schaldemose sees it as outdated and concedes that she would vote for removing it. However, she states that she would not support having a referendum because, as she argues, it would be hard to win and would require an acute reason for doing so. When asked about the EU AFSJ opt-out, Schaldemose furthers the impact of the 2015 referendum that asked the public whether to turn this opt-out into an opt-in, stating the following:

> *"The political reality in Denmark is not ripe for repeating a referendum that took place in 2015 in 2020, 5 years after. If so, something new and something extra would be required, and I do not believe that we are there yet to be completely honest.* […] *I would prefer if we removed the* [AFSJ] *opt-out, and I would vote yes to remove the AFSJ opt-out today, among other things, because it has weakened our possibility to be a part of Europol. But I do not think it can be removed, unfortunately."*[16] (Interview Christel Schaldemose, 2020, 12:45-13:30).

Highlighting the limitations regarding not being a member of Europol, among other things, Schaldemose would vote in favor of removing the AFSJ opt-out as well but acknowledges the difficulties with repeating a referendum only 5 years after. Aastrup Jensen of Venstre concedes to understand the current government's reasons for not having a referendum on the defense opt-out and states the following:

> *"We hope that we can pressure the government to take this subject up for discussion. I understand that the government does not dare from tactical reasons. And that is because they are nervous to get a no and that hurts a government to get a no, we* [Venstre] *know everything about that, and we tried it the last governing period. But this is more important than tactical political reasons."*[17] (Interview Michael Aastrup Jensen, 2020, 12:00-14:00).

As Aastrup Jensen highlights, the political lesson of the 2015 referendum was that it hurt the public support of the Venstre government to 'lose' a referendum that it and a majority of the parliament had backed. The 2015 referendum is also mentioned by Hjort Frederiksen of

[15] Translated from Danish by the authors.
[16] Translated from Danish by the authors.
[17] Translated from Danish by the authors

Venstre, who was a part of the government at the time, to have had an unpredictable result (Interview Claus Hjort Frederiksen, 2020, 26:20-27:30). Further, Schaldemose argues that the AFSJ referendum has stayed in the consciousness of politicians when talking about having referendums on EU matters in terms of both the Defense and AFSJ opt-outs (Interview Christel Schaldemose, 2020, 12:45-13:30).

Conclusively, it can be argued that the ghost of the 2015 referendum on the EU AFSJ opt-out is present in the consciousness amongst Danish politicians of the traditional government parties, Socialdemokratiet and Venstre, and has an impact on the hesitation to having another referendum regarding EU matters. Therefore, it can be argued that domestic matters and conditions have a great impact on Denmark's willingness to engage in deeper cooperation on cybersecurity with the EU, as such cooperation would require lifting or changing the optouts. When using small state theory on this matter, it can be concluded that the prevalent assumption of small state foreign policy being largely controlled by the policy of greater powers (see Handel, 1981/1990, p. 4) can be discussed. As argued in the previous section, Denmark's NATO and US relationship has had a great impact on Danish foreign and security policy since the 1990s and could have had an impact on why Denmark has remained reluctant to engage in deep EU cooperation on security. However, domestic conditions play a great part as public referendums are required to lift the opt-outs, and the ghost of the 2015 referendum is still haunting the Danish political opinion. Because of this, the Danish government cannot enter into closer cooperation with the EU on cybersecurity without fearing for the domestic political consequences if it chooses to back the lifting or reshaping of the opt-outs.

10 Conclusion

A common point found in small state literature is that a small state can make up for its relative weakness by utilizing alliances to guarantee its security (Baker Fox, 1959, p. 1; Rothstein, 1968, p. 61; Vital, 1967/2006, p. 79) as long as a contractual agreement is in place to keep the alliance obligated to make good on its commitments (Handel, 1981/1990, pp. 122-123). NATO is often considered Denmark's security guarantor, which would suggest that this guarantee also applies to cybersecurity matters. NATO has traditionally been built on an assumption that as an alliance, it ensures protection for all member states through deterrence rooted in article 5. NATO has assured that cyberspace is a realm of military operation, and that a severe cyberattack conducted against an ally would be assumed to be an attack on all NATO members. Thus, deterrence has become a central part of NATO's cybersecurity strategy.

The thesis finds that the cornerstone of NATO's commitment cannot be obtained, when cyberspace is regarded as an isolated realm of military operation, which would suggest that Denmark cannot utilize NATO as an alliance to guarantee its cybersecurity. Deterrence builds on one's adversary knowing one's retaliation capabilities, but for cyberweapons to be effective, the weapons must be unknown by the target adversary, making cyber deterrence in an isolated realm unobtainable. However, cyber deterrence may be obtained with the use of kinetic capabilities as a response to a severe cyberattack. Nonetheless, NATO finds itself unable to clearly define what constitutes a proportional response, according to international law, which is an obstacle for NATO's ability to respond with military force, thus weakening its deterring effect. NATO has followed a strategy of not articulating the threshold for how severe a cyberattack must be to justify a kinetic response based on the assumption that this uncertainty keeps adversaries from conducting serious cyberattacks.

Though NATO's ambiguous cyber deterrence strategy may have deterred adversaries from conducting severe cyberattacks comparable in scale to that of Estonia in 2007, it has not alleviated the fact that NATO members, such as Denmark, suffer from cyberattacks on a daily basis. Considering this, NATO cannot fully guarantee Danish cybersecurity, even though the alliance commits itself to secure its member states in cyberspace. Therefore, this would suggest that Denmark cannot utilize NATO as an alliance to fully compensate for its relative weakness in cyberspace. Similarly, the thesis finds that the EU cannot fully guarantee Danish cybersecurity, yet as the EU's cyber strategy intends to handle both cybercrime through legal actions as well as state-sponsored attacks through sanctions and defensive preventive capabilities, the EU may, in the future, prove useful for Denmark in countering its cybersecurity

issues.

Despite its inability to assure cyber deterrence, NATO, like the EU, provides initiatives for Denmark to compensate for its relative weakness in cyberspace. Krasner (1981, p. 123) argues that small states can make up for their relative weakness by participating and influencing the basic institutional structures and rules that govern the international movement and sharing of rules, services and technology. Notably, NATO with its CCDCOE and the EU with ENISA, Europol and several PESCO initiatives, facilitate platforms for sharing of research, intelligence and development, which could strengthen Danish cybersecurity capabilities. Denmark cooperates fully in NATO, whereas, paradoxically, though Denmark could potentially utilize several EU initiatives to enhance its cybersecurity capabilities in research and development, it only partakes fully in ENISA and the EU cyber sanctions regime. Thus, Denmark would be able to further compensate for its relative weakness in cyberspace through the EU yet chooses to not fully partake.

Furthermore, in terms of operational entities that concern cybersecurity, NATO and the EU do not provide equal opportunities for Denmark to compensate for its relative weakness in cyberspace. NATO's only operational entity that has capabilities to respond to cyberattacks, the NCIRC, is solely responsible for NATO's own network systems. As Alatalu (2016) argues, NATO needs a deployable, emergency entity with technical capacity to help NATO member states that have fallen victim to cyberattacks (Alalatu, 2016, p. 3). Such an exact entity, the CRRTs initiative, is set up in EU through PESCO cooperation. This initiative is voluntary, and member states enjoy veto rights to decide whether the cyber operational entity should be deployed. Notably, Dosenrode (1994) argues that small states may find international institutions advantageous in their pursuit of security as intergovernmental cooperation does not limit small states' sovereignty (Dosenrode, 1994, pp. 246-248). Based on this, PESCO's operational cyber emergency response entity would be favorable for Denmark to engage in to compensate for its relative weakness in cyberspace as it does not limit Danish sovereignty. This would make up for NATO's inability to guarantee cybersecurity with a deployable emergency entity. However, Denmark is not partaking in PESCO because of its opt-out on defense.

Moreover, the EU, unlike NATO, has developed operational entities that handle cybercrime issues. As an operational entity, Europol provides vital intelligence and data to counter cybercrime issues, making it an initiative through which Denmark could make up its relative weakness in handling cross-border cybercrime. The Danish National Police points out that an increasing part of their investigation relies on data analysis provided by Europol, leaving

Denmark more vulnerable than Europol members who enjoy full accessibility to intelligence. Following Krasner's argument (Krasner, 1981, p. 126), it would be favorable for Denmark to fully engage in Europol as it would enable Denmark to influence and alter institutional structures that govern international rules and practices. However, considering Dosenrode's (1994) view, Denmark's choice of not fully committing itself to Europol may be explained in a reluctance to lose national sovereignty, thus favoring self-determination over influence in an international institution that could potentially compensate for Denmark's relative weakness in cyberspace. The Danish choice of whether to engage fully in Europol cooperation or not reflects a dilemma for Denmark as a small state (e.g. Baker Fox 1959, Vital 1967/2006, Rothstein 1968) of whether to prioritize the pursuit of security or to maintain national self-determination. However, the Danish choice of engaging fully in PESCO does not reflect the same dilemma, since Denmark could, legally speaking, utilize the cooperation to strengthen its cybersecurity without losing national sovereignty (DIIS, 2019, p. 20).

Even though EU cooperation entails clear options for Denmark to compensate for its relative weakness in cyberspace, Denmark has been reluctant to engage in deep cooperation. According to the aforementioned dilemma, this would suggest that Denmark values the preservation of self-determination and political maneuverability higher than the value of enhancing cybersecurity through international cooperation. A simple explanation to this may be that Denmark feels confident enough in its own ability to secure itself in cyberspace as to allow itself to focus on the preservation of self-determination instead. Very little, however, supports this as a possibility, since issues in cyberspace, which know no territorial boundaries, cannot be resolved without international cooperation, a point which the Danish government as well as the National CFCS acknowledge (Danish Ministry of Defence, 2018, pp. 9–10; Interview Thomas Wulff of the CFCS, 2020, 27:30-28:00).

Furthermore, little-to-no evidence suggests that Denmark has followed a specific strategy of preserving self-determination and political maneuverability (Vital 1967/2006, pp. 84-85, Rothstein 1968, p. 61) in its pursuit of cybersecurity either. In fact, the thesis argues that the two most comprehensive Danish strategies, which enhance Danish cybersecurity capacities, have originated from external pressure. The 2018-2021 NCISS was implemented to comply with the EU's NIS directive, and the 2018-2023 DDA saw a 20% increase in defense spending as a result of pressure from the US. Though these strategies entail important initiatives that strengthen Denmark's ability to secure itself in cyberspace, e.g. enhancing the operational entity of the CFCS, it is difficult to argue that these initiatives are results of a Danish strategy aimed

specifically at preserving self-determination and political maneuverability. Furthermore, the thesis finds that Denmark has not utilized diplomacy as a tool of statecraft to follow a similar strategy (Baker Fox, 1959, p. 2) or build norms to compensate for its relative weakness in cyberspace (Crandall & Allan, 2015). As an example, the Danish TechPlomacy initiative seems to be more focused on ensuring economic growth through cooperation with large tech companies, rather than addressing the security risks digitization brings with it.

Moreover, the thesis finds little evidence that the Danish reluctance to engage in deep EU cooperation on cybersecurity stems from a Danish strategy of attempted to keep the US committed to Denmark and Danish security interests (Handel, 1981/1990, p. 122). As the US has previously voiced concerns of EU's PESCO framework, Denmark might feel reluctant to join the cooperation in order to not lose goodwill with its important NATO ally. However, the current 'America First' policy has questioned US obligations to secure Europe and Denmark, leaving several Danish politicians to increasingly favor closer European defense and security cooperation as complimentary to NATO (Interview Hjort Frederiksen, 2020, 27:30-30:50; Interview Lidegaard, 2020, 5:30-6:40; Interview Melchior, 2020, 9:30-11:30; Interview Weiss, 12:40-18:30, 2020; Interview Aastrup Jensen, 2020, 15:30-21:30).

Finding little evidence that Denmark pursues a specific strategy of ensuring self-determination and political maneuverability or a strategy of keeping US interests in Denmark high, the thesis does, however, find substantial evidence that the unwillingness to engage in closer EU cooperation stems from a general domestic reluctance to back referendums on removing the Danish defense and AFSJ opt-outs. The ghost of the 2015 referendum on the Danish AFSJ opt-out is still haunting the Danish government and suggests that domestic political-strategic concerns are the reasons for the government's reluctance to back Danish referendums on the removal of the defense and AFSJ opt-outs. This questions the prevalent small state theoretical assumption that a small state's foreign policy is primarily determined by great powers (Handel, 1981/1990 p. 4, 261).

In short, to give a succinct answer the research question of the thesis, i.e.:

From a small state perspective, how can the Danish state compensate for its relative weakness in cyberspace through EU and NATO cooperation, and why does Denmark not engage in deep cooperation with the EU on cybersecurity?

Though neither NATO nor the EU can guarantee Danish cybersecurity, NATO and especially the EU provide an array of initiatives through which Denmark can compensate for its relative weakness by cooperating on expertise and intelligence-sharing, capacity development and emergency response entities to cyberattacks, but due to a high domestic political risk for the Danish government of backing referendums on lifting the opt-outs on the AFSJ and Defence, Denmark has been reluctant to pursue the possibility of engaging in deep EU cooperation on cybersecurity.

11 Perspective and evaluation

This section intends to briefly evaluate academic contributions, theoretical and methodological considerations as well as limitations posed upon the process of writing the thesis because of the outbreak of a global pandemic.

This thesis attempts to contribute to filling a knowledge gap in the developing field of small state studies in cyberspace by looking at the unique case of Denmark as the only NATO and EU member state with opt-outs on Defence and AFSJ. The thesis has contributed by illuminating Danish cybersecurity policy and cooperation through NATO and the EU, and as such provides a new piece of the puzzle of small state cybersecurity studies. The thesis finds it favorable for other studies to be conducted, which further illuminate small state studies in cyberspace. As this thesis has used a single-case study method, it has left the thesis with lesser ground for broad generalization of how small state theory can be applied to address cybersecurity issues. Thus, other studies utilizing multiple-case study methods to compare small state behavior in cybersecurity issues would provide more useful insights for broader generalizations in the field. Had the authors had more time to conduct their research, this thesis would arguably lay a decent groundwork for broader studies of small states in cybersecurity.

Furthermore, cybersecurity remains a relatively new area of study in IR literature. As highlighted in the "Choice of theory" section of the methodology, this means that scholars are still, to this day, attempting to apply traditional IR theories, such as realism, liberalism and constructivism, to the realm of cyberspace in order to test the explanatory powers of an array of theories on issues related to cybersecurity. In earlier projects, the members of the group, either collectively or individually, have applied small state theory to the case of Danish foreign policy with much success. Further egged on by Burton (2013), who has shown the potential of looking at cybersecurity from a small state theoretical perspective, the group chose to apply a similar theoretical framework for its analysis of Danish cybersecurity policies. While the theoretical framework has, generally, provided valuable insights, evaluating upon the usefulness of the ability of the theory to explain cybersecurity issues in this thesis, it can be argued that its strengths are also its weaknesses. Since small state theory(ies) consist(s) of many different strings of theories, i.e. (neo)realism, (neo)liberalism and constructivism, it has proven useful in having multi-facetted explanatory effects. This has, however, at times, left the theory without consistent coherence as e.g. neorealist and neoliberal aspects of the theoretical framework sometimes clash. Through conducting its research, it became clear to the authors that both

NATO and the EU have developed or have begun developing strategies to deter potential adversaries from conducting cyberattacks against their member states. Though the thesis points to a stream of difficulties in creating reliable deterrence in cyberspace, applying neorealist deterrence theory to NATO and EU cybersecurity policies may allow for further valuable insights into the field. This might be a point for future research.

In addition, as this thesis is covering political matters, the authors set out with the ambition of gathering their own empirical data by interviewing politicians, experts and authorities to gain as much knowledge as possible. In February, the authors returned from internships in Brussels and the Danish representations in Iceland and Canada, where they combined had built a network of persons of interest, which they intended to utilize in order to gather empirical data. During the first month, the authors attended public political conferences and set up meetings in Aarhus and Copenhagen, which ensured connection to politicians utilized in the thesis as well as a partnership with The Danish Foreign Policy Society. The authors were invited to participate in conferences in Brussels and planned to interview Danish politicians at Christiansborg. However, the outbreak of the coronavirus put a stop to that. Despite of this, the authors succeeded in interviewing six politicians and the CFCS, digitally attending the Third Cybersec Brussels Leaders' Foresight conference, as well as receiving written replies from politicians, a PESCO member state representative, a Danish Ministry of Defence official and an ENISA member state representative. However, the lockdown severely constrained the ability of the thesis to gather its own empirical data, and combined with the fact that all libraries were shut down, outside conditions left the authors to rely on literature that was digitally available. Furthermore, the authors set out by meeting at the university to work every day, but due to Aalborg University shutting down and prohibiting students to meet, the authors were forced to work separately and digitally. This has had the consequence of roughly doubling the time and effort because of complicated coordination between the authors combined with technical issues.

12 Bibliography

Alatalu, S. (2016). NATO's new cyber domain challenge. *CYCON-U-S 2016*, 1–8.

Alexander, L. G. K. (2010). *Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command 1. Defense Reforms*.

Allison, G., & Treverton, G. F. (1992). *Rethinking America's Security: Beyond Cold War to the New World Order*. W. W. Norton & Company.

Alternativet. (n.d.). *EU-politik // Alternativet*.

Amadeo, K. (2019). Silicon Valley, America's Innovative Advantage. *The Balance*.

Areng, L. (2014). Lilliputian States in Digital Affairs and Cyber Security. *The Tallinn Papers*, *4*, 1–11.

Baker Fox, A. (1959). *The Power of Small States: Diplomacy in World War II*. University of Chicago Press.

Balakrishnan, R. (2018). *Cyber Security for Small States – NAOC*.

Baldwin, D. A. (1995). Security Studies and the End of the Cold War. *World Politics*, *48*(1), 117–141.

Barigazzi, J. (2017, November 22). Mogherini hails 'historic' EU defense pact. *Politico*. https://www.politico.eu/article/federica-mogherini-defense-hails-historic-eu-defense-pact-as-23-countries-sign-up/

BBC. (2015). *Denmark votes No on adopting EU rules - BBC News*. https://www.bbc.com/news/world-europe-35002158

Bebber, L. C. R. (2018). *There is No Such Thing as Cyber Deterrence. Please Stop.* https://www.thecipherbrief.com/column_article/no-thing-cyber-deterrence-please-stop

Béraud-Sudreau, L., Efstathiou, Y.-S., & Hannigan, C. (2019). *Keeping the momentum in European defence collaboration: an early assessment of PESCO implementation* (Issues 1–18).

Bertelsen, R. G. (2018). *Professor: Danmark er en småstat mellem stormagter i Arktis*. Altinget. https://www.altinget.dk/arktis/artikel/professor-danmark-er-en-smaastat-mellem-stormagter-i-arktis

Brammer, H. (1987). *Danmark som småstat: muligheder og begrænsninger*. Gyldendal.

Bramsen, T. (2019). *Forsvarsminister Trine Bramsen til NATO-forsvarsministermøde*. Forsvarsministeriet. https://fmn.dk/nyheder/Pages/Danmark-stiller-med-substantielle-bidrag-til-NATOs-beredskabsstyrker.aspx

Brantly, A. F. (2018). The cyber deterrence problem. *2018 10th International Conference on Cyber Conflict (CyCon)*, *2018*-, 31–54.

Brent, L. (2019). *NATO's role in cyberspace*. NATO. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

Brinkmann, S. (2013). *Qualitative Interviewing*. Oxford University Press.

Burton, J. (2013). Small states and cyber security: The case of New Zealand. *Political Science*, *65*(2), 216–238. https://doi.org/10.1177/0032318713508491

Buzan, B. (1997). Rethinking Security After the Cold War. *Cooperation and Conflict*, *32*(1), 5–28.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publisher Inc.

Cavalty, M. D., Mauer, V., & Krishna-Hensel, S. F. (2007). *Power and Security in the Information Age*. Ashgate Publishing, Ltd.

CCDCOE. (2020). *About us*. CCDCOE. https://ccdcoe.org/about-us/

Centre for Cyber Security. (2017). *Undersøgelsesrapport* (Issue April). https://fe-ddis.dk/cfcs/nyheder/Pages/NyhederfraCFCS.aspx

Centre for Cyber Security. (2019a). *The Cyber Threat Against Denmark 2019*. https://fe-ddis.dk/cfcs/publikationer/Documents/The-Cyber-Threat-Against-Denmark-2019.pdf

Centre for Cyber Security. (2019b). *Trusselsvurderinger*. https://fe-ddis.dk/cfcs/publikationer/Documents/Cybertruslen-mod-Danmark-2019.pdf

CERT EU. (2019). *CERT-EU: Its channels of communication and its roles and responsibilities*. 1–4. https://cert.europa.eu/cert/custom/CERT for the European

Institutions.asc

CFCS. (2016). *Om Center for Cybersikkerhed*. https://fe-ddis.dk/CFCS/OMOS/Pages/Omos.aspx

CFCS. (2020a). *Cybertruslen ved hjemmearbejde set i lyset af COVID-19-situationen*. Fe.Ddis.Dk.

CFCS. (2020b). *Internationalt samarbejde om cybersikkerhed*. Fmn.Dk.

CFSC. (n.d.). *Cybersikkerhedsrådet*. Fe.Ddis.Dk.

CFSC. (2020). *Om Center for Cybersikkerhed*. Ministry of Defense.

Chazan, G., & Peel, M. (2019). *US warns against European joint military project | Financial Times*.

Choi, M., & Roulston, K. (2018). Qualitative Interviews. In U. Flick (Ed.), *The SAGE Handbook of Qualitative Data Collection* (pp. 233–249). SAGE Publications Ltd.

Christensen, K. K., & Liebetrau, T. (2016). *Security Meets Cyberspace: The Politics of Cyber Security*. Danish Political Science Association.

CISA. (2019). *What is Cybersecurity?* US. Department of Homeland Security.

Craig, A., & Valeriano, B. (2018). *Realism and Cyber Conflict: Security in the Digital Age* (D. Orsi, J. R. Avgustin, & M. Nurnus (eds.); pp. 85–102). E-International Relations.

Crandall, M., & Allan, C. (2015). Small states and big ideas: Estonia's battle for cybersecurity norms. *Contemporary Security Policy*, *36*(2), 346–368. https://doi.org/10.1080/13523260.2015.1061765

CXO. (n.d.). *Et kapløb med tiden*. CXOmagasinet.Dk.

CyberPeace Alliance. (2019). *Tallinn Manual — A Brief Review of the International Law Applicable to Cyber Operations*. Medium.

Danish Constitution. (n.d.). *The Constitutional Act is the Foundation of Danish Democracy*.

Danish Defence Intelligence Service. (2019a). *Efterretningsmæssig Risikovurdering 2019*.

Danish Defence Intelligence Service. (2019b). *Intelligence Risk Assessment 2019*. https://fe-

ddis.dk/SiteCollectionDocuments/FE/EfterretningsmaessigeRisikovurderinger/Intelligence Risk Assessment 2019.pdf

Danish Defense Committee. (2019). *Høring i Forsvarsudvalget om cybervåben i militære operationer 11-09-2019*. Folketinget.

Danish Ministry of Defence. (2018). *DEFENCE AGREEMENT 2018 - 2023*.

Danmarks Radio. (n.d.). *Bramsen vil beholde forsvarsforbehold: EU er "utrolig langsom", når der skal handles | Udland | DR*. Retrieved May 27, 2020, from https://www.dr.dk/nyheder/udland/bramsen-vil-beholde-forsvarsforbehold-eu-er-utrolig-langsom-naar-der-skal-handles

Danmarks Statistik. (2015). *Resultater - Hele landet - Folkeafstemning torsdag 3. december 2015 - Danmarks Statistik*. http://dst.dk/valg/Valg1664255/valgopg/valgopgHL.htm

Davis, S. (2019). *SCIENCE AND TECHNOLOGY COMMITTEE (STC) NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE General Report*.

DDIS. (2013). *Forsvarets Efterretningstjeneste Beretning 2011-2012*.

Deibert, R. J., & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, *4*(1), 15–32.

Det Konservative Folkeparti. (n.d.). *En europæisk generationskontrakt for fremtidens Danmark*. Retrieved May 27, 2020, from https://konservative.dk/politik/eu-program-2019-2024/

Doffman, Z. (2019). *Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First*.

Dosenrode, S. Z. von. (1994). Western European Small States in International Regimes. *History of European Ideas*, *19*(1–3), 245–252.

Drost, E. A. (2011). Validity and Reliability in Social Science Research. *Education, Research and Perspectives*, *38*(1), 105–125.

Dunn, J. (2020). The European Union's Permanent Structuted Cooperation: Implications for Transatlantic Security. *Strategic Forum*, *302*, 1–13.

EC Europe. (2020). *The Directive on security of network and information systems (NIS Directive)*. Ec.Europe.Eu.

Edwards, R., & Holland, J. (2013). *What is Qualitative Interviewing?* Bloomsbury Academic. http://dx.doi.org/10.5040/9781472545244

EEAS. (2018a). *New tool to address cyber threats: the EU's Rapid Response Force*. https://eeas.europa.eu/headquarters/headquarters-homepage/47525/eu-develop-cyber-rapid-response-force_en

EEAS. (2018b). *The Common Security and Defence Policy (CSDP)*. https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/431/common-security-and-defence-policy-csdp_en

Enhedslisten. (2019). *Efter forsvarsrapport: Enhedslisten ønsker forsvarsforbeholdet udvidet*. https://enhedslisten.dk/2019/12/06/efter-forsvarsrapport-enhedslisten-oensker-forsvarsforbeholdet-udvidet

ENISA. (2018). *Cyber Europe 2018: After Action Report* (Issue December). https://doi.org/10.2824/369640

ENISA. (2019). *ENISA PROGRAMMING DOCUMENT 2020-2022 Including Multiannual planning, Work programme 2020 and Multiannual staff planning*. https://doi.org/10.2824/52836

ENISA. (2020). *List of ENISA Management Board Representatives and Alternates*.

Eriksson, G., & Pettersson, U. (2017). Special Operations from a Small State Perspective : Future Security Challenges /. In *Special Operations from a Small State Perspective : Future Security Challenges /* (Elektronis). Springer International Publishing.

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review*, *27*(3), 221–244.

EU-oplysningen. (2019). *Hvad er EU's tre søjler? / Folketingets EU-Oplysning*. https://www.eu.dk/da/faq/alle-faqs/hvad-er-eus-tre-soejler

EU. Treaty on the Functioning of the European Union, (2012).

EU. NIS Directive, 6 Official Journal of the European Union 30 (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

European Commission. (n.d.). *European defence fund | Internal Market, Industry, Entrepreneurship and SMEs*. Retrieved May 27, 2020, from https://ec.europa.eu/growth/sectors/defence/european-defence-fund_en

European Commission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. https://doi.org/10.4271/2010-01-1021

European Commission. (2015). Consolidated Version of the Treaty on European Union, Core EU Legislation 13. https://doi.org/10.1007/978-1-137-54482-7_1

European Commission. (2017). *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450

European Commission. (2017). Notification on Permanent Structured Cooperation (PESCO) to the Council and to the High Representative of the Union for Foreign Affairs and Security Policy.

European Commission. (2018). Permanent Structured Cooperation (PESCO)'s projects - Overview, European Council 23. https://www.consilium.europa.eu/media/41333/pesco-projects-12-nov-2019.pdf

European Office - Foreign Ministry. (n.d.). *De danske EU forbehold*. Retrieved May 27, 2020, from https://um.dk/da/udenrigspolitik/eu/danmark-i-eu/de-danske-eu-forbehold/

European Values. (2014). *The Area of Freedom, Security and Justice - European Values Center for Security Policy*. https://www.europeanvalues.net/vyzkum/the-area-of-freedom-security-and-justice/

Europol. (n.d.-a). *Cybercrime | Crime areas | Europol*. Retrieved May 26, 2020, from https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

Europol. (n.d.-b). *Europol's 20 most noteworthy operations | Activities & Services*. Europol. Retrieved May 27, 2020, from https://www.europol.europa.eu/about-europol/europol-20-years/europols-20-most-noteworthy-operations

Europol. (n.d.-c). *Joint Cybercrime Action Taskforce (J-CAT) | Activities & Services | Services & Support | Europol*. Retrieved May 27, 2020, from https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce

Europol. (n.d.-d). *Partners & Agreements | Europol*. Retrieved May 27, 2020, from https://www.europol.europa.eu/partners-agreements

Europol. (2017). *Aggreement on Operational and Strategic Cooperation between the Kingdom of Denmark and the European Police Office*. https://www.europol.europa.eu/publications-documents/agreement-operational-and-strategic-cooperation-between-kingdom-of-denmark-and-europol%0A%0A%0A

Europol. (2019). Internet Organised Crime Threat Assessment (iOCTA) 2019. In *EUROPOL*.

Europol. (2020). *Europol's Budget*. https://www.europol.europa.eu/publications-documents/europol-budget

Fagpressen. (2019). *EU's cybersikkerhedscenter og cyberforsvarsaftale*. Fagpressen.Eu. http://fagpressen.eu/mandat-og-aftale-om-cybersikkerhed/?fbclid=IwAR124aOVIbq3sXIjFUcZ7xYFDhTPgwo_sEBXeS89vyKnoOpnxyHOpJGWcBM

Finkielman, J. (2019). Danmarks værn mod cyberkriser. *Udenrigs*, *3*, 25–30.

Finnemore, M., & Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organization*, *52*(4), 1–23. https://doi.org/10.1162/002081898550789

Fiott, D., Missiroli, A., & Tardy, T. (2017). Permanent Structured Cooperation: What's in a name? In *Chaillot Papers Nº 142* (Issue November). https://doi.org/10.2815/747538

Fischer, K., & Mouritzen, H. (2017). *DANISH FOREIGN POLICY YEARBOOK 2 017 Forsvarsudvalget 2016-17 FOU Alm.del Bilag 100 Offentligt*.

Fischerkeller, M. P., & Harknett, R. J. (2018). *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation*.

Flick, U. (2007). Qualitative Research Designs. In *Designing Qualitative Research* (pp. 1–15). SAGE Publications Ltd.

Flick, U. (2009). *An Introduction to Qualitative Research* (4th ed.). SAGE Publications, Inc.

Flick, U. (2018). Doing Qualitative Data Collection – Charting the Routes. In U. Flick (Ed.), *The SAGE Handbook of Qualitative Data Collection* (pp. 3–16). SAGE Publications, Inc.

Folketinget. (2015). *Resultatet af folketingsvalget 2015 / Folketinget*. https://www.ft.dk/aktuelt/nyheder/2015/06/valgidag.aspx

Folketinget. (2019a). *Er Danmark det eneste land, der har EU-forbehold*. https://www.eu.dk/da/faq/alle-faqs/er-danmark-det-eneste-land-der-har-eu-forbehold

Folketinget. (2019b). *Valgresultat 2019 / Folketinget*. https://www.ft.dk/aktuelt/nyheder/2019/06/valgresultat

Folketinget. (2020). *De danske forbehold*. https://www.eu.dk/da/danmark-i-eu/de-danske-forbehold

Fondation Robert Schuman. (2009). *To What Purpose the Lisbon Treaty?* https://www.robert-schuman.eu/en/dossiers-pedagogiques/traite-lisbonne/fiche1.pdf

Frederiksen, M. (2019). *Statsministerens samtaler med den nominerede Europa-Kommissionsformand, NATO's generalsekretær og FN's generalsekretær*. Statsministeriet. https://www.eu.dk/da/danmark-i-eu/de-danske-forbehold

Friis, K., & Ringmose, J. (2016). *Conflict in Cyber Space* (K. Friis & J. Ringmose (eds.)). Routledge.

Goetschel, L. (2011). Neutrals as brokers of peacebuilding ideas? *Cooperation and Conflict*, *46*(3), 312–333. https://doi.org/10.1177/0010836711416957

Gong, H., & Yang, X. (2017). *Reconfiguring Class, Gender, Ethnicity and Ethics in Chinese Internet Culture*. Routledge.

Government of Denmark. (2018). *Udenrigs- og Sikkerhedspolitisk Strategi 2019-2020*.

Guang, E. T. E. (2020). A Small State Perspective on the Evolving Nature of Cyber Conflict: Lessons from Singapore. *The Prism*, *8*(3), 158–171.

Haltiwagner, J. (2019, December). *Trump keeps criticizing NATO allies over spending.*

Here's how NATO's budget actually works. Businessinsider. https://www.businessinsider.com/how-nato-budget-is-funded-2018-7?r=US&IR=T

Handel, M. I. (1990). *Weak States in the International System*. Frank Cass & Co. Ltd.

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

Hasanov, A. H., Iskandarov, K. I., & Sadiyev, S. S. (2019). THE EVOLUTION OF NATO'S CYBER SECURITY POLICY AND FUTURE PROSPECTS. *Journal of Defense Resources Management*, *10*(1), 94–106.

Herd, G., & Kriendler, J. (2013). Understanding NATO in the 21st century : alliance strategies, security and global governance /. In *Understanding NATO in the 21st century : alliance strategies, security and global governance /*. Routledge.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital threats and Multinational Responses. *Journal of Strategic Security*, *4*(2), 49–60.

Interview Claus Hjort Frederiksen, (2020).

Holstein, E. (2018). *Holger K. Nielsen gør status efter 33 år på Borgen: Edinburgh-afstemningen kostede mig dyrt*. Altinget.Dk. https://www.altinget.dk/artikel/holger-k-goer-status-efter-33-aar-paa-borgen-edinburgh-afstemningen-kostede-mig-dyrt

Hošek, T. (2017). *Stoltenberg outlines three critical conditions for EU-NATO cooperation | European Security Journal*. https://www.esjnews.com/stoltenberg-eu-nato-cooperation

Hughes, D., & Colarik, A. M. (2016). Predicting the Proliferation of Cyber Weapons into Small States. *Joint Force Quarterly*, *83*(4), 19–26.

Iasiello, E. (2014). Is Cyber Deterrence an Illusory Course of Action? *Journal of Strategic Security*, *7*(1), 54–67. https://doi.org/10.5038/1944-0472.7.1.5

Ilves, T. H. (2013). *President Ilves at the Fletcher Institute: "In the cyber world, we have to find a balance between security, privacy and the free movement of information."* https://vp2006-2016.president.ee/en/media/press-releases/9459-president-ilves-at-the-fletcher-institute-in-the-cyber-world-we-have-to-find-a-balance-between-security-privacy-and-the-free-movement-of-information/index.html

Ingebritsen, C. (2002). Norm Entrepreneurs: Scandinavia's Role in World Politics. *Cooperation and Conflict*, *37*(1), 11–23. https://doi.org/10.1177/0010836702037001689

Interpol. (2019). *Cybercrime*. https://www.interpol.int/Crimes/Cybercrime

Ismail, N. (2019). *10 cyber security trends to look out for in 2020*. Information-Age. https://www.information-age.com/10-cyber-security-trends-look-2020-123463680/

Jacobsen, J. T. (2016). *Opbygning af offensiv cyberkapacitet NÆSTE SKRIDT FOR DANMARKS CYBERMILITÆR*.

Jacobsen, J. T. (2017a). *Danmark bør undgå en "digital Genèvekonvention"*.

Jacobsen, J. T. (2017b). *Prioritising Denmark's Cyber Policy: Denmark Should avoid a "Digital Geneva Convention."*

Jakobsen, B., Muguruza, B. T., de Magalhaes, D. C., Ballester, A., & Sweerts, M. (2019). Challenges to effective EU cybersecurity policy - Briefing Paper. In *European Court of Auditors* (Issue March). https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

Jakobsen, P. V. (2005). Stealing the Show: Peace Operation and Danish Defence Transformation after the Cold War. In T. Edmunds & M. Malešič (Eds.), *Defence Transformation in Europe Evolving Military Roles* (pp. 35–46). IOS Press.

Jakobsen, P. V., Ringsmose, J., & Saxi, H. L. (2020). Prestige-seeking small states: Danish and Norwegian military contributions to US-led operations. *European Journal of International Security*, *3*(2), 256–277. https://doi.org/10.1017/eis.2017.20

Janczewski, L. J., & Caelli, W. (2016). *Cyber Conflicts and Small States* (L. J. Janczewski & W. Caelli (eds.)). Routledge.

Jensen, E. T. (2017). THE TALLINN MANUAL 2.0: HIGHLIGHTS AND INSIGHTS. *Georgetown Journal of International Law*, *48*, 735–778.

Justitsministeriet. (2019). *Redegørelse til Folketinget om status over dansk politis situation i forhold til Europol*.

Jydske Vestkysten. (2019). *V og SF enige: Drop forsvars-forbehold | jv.dk*.

Jyllands-Posten.dk. (2011). *Obama praises Denmark with recycled cliché - News in English*. https://jyllands-posten.dk/uknews/article4501536.ece/

Jyllands-Posten. (2018). *Fakta: Hackerangreb kostede Mærsk over en milliard kroner*. Jyllands-Posten.Dk. https://jyllands-posten.dk/indland/ECE10312652/fakta-hackerangreb-kostede-maersk-over-en-milliard-kroner/

Jyllands-Posten. (2019). *DF vil have flere og ikke færre EU-forbehold - Politik*. https://jyllands-posten.dk/politik/ECE11383197/df-vil-have-flere-og-ikke-faerre-euforbehold/

Kassab, H. S. (2014). In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare. In J.-F. Kremer & B. Müller (Eds.), *Cyberspace and International Relations Theory, Prospects and Challenges* (Kremer & M, pp. 59–76).

Kaufman, J. P. (2017). The US perspective on NATO under Trump: lessons of the past and prospects for the future. *International Affairs*, *93*(2), 251–266.

Kennedy, B. L. (2018). Deduction, Induction, and Abduction. In U. Flick (Ed.), *The SAGE Handbook of Qualitative Data Collection* (pp. 49–64). SAGE Publications, Inc.

Knudsen, O. F. (2002). Small States, Latent and Extant: Towards a General Perspective. *Journal of International Relations & Development*, *5*(2).

Krasner, S. D. (1981). Transforming International Regimes: What the Third World Wants and Why. *International Studies*, *25*(1), 119–148.

Kremer, J.-F., & Müller, B. (2014). *Cyberspace and International Relations: Theory, Prospects and Challenges* (J.-F. Kremer & B. Müller (eds.)). Springer-Verlag.

Krunke, H. (2005). From Maastricht to Edinburgh: The Danish Solution. *European Constitutional Law Review*, *1*(3), 339–356.

Kühle, E. (2008). *Danmarkshistorie i Globalt Perspektiv*. Gyldendal.

Langø, H.-I. (2016). Competing academic approaches to cyber security. In K. Friis & J. Ringsmose (Eds.), *Conflict in Cyber space - Theoretical, Strategic and Legal Perspectives* (pp. 7–26). Routledge.

Lebow, R. N. (1988). Interdisciplinary Research and the Future of Peace and Security Studies. *Politial Psychology*, *9*(3), 507–525.

Lewis, J. A. (2018). *Rethinking Cybersecurity - Strategy, Mass Effect, and States*. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180108_Lewis_ReconsideringCybersecurity_Web.pdf

Liberal Alliance. (n.d.). *Forsvarspolitik - Liberal Alliance*. Retrieved May 27, 2020, from https://www.liberalalliance.dk/politik/forsvar/

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation.

Lidegaard, Martin, Interview, (2020).

Lidegaard, M. (2020). *Martin Lidegaard: Danmarks udenrigs-politiske topprioritet bør være Arktis*. Altinget. https://www.altinget.dk/arktis/artikel/martin-lidegaard-danmarks-udenrigspolitiske-topprioritet-boer-vaere-arktis

Liebetrau, T. (2019). *EU Cybersecurity Governance*. University of Copenhagen.

Lijphart, A. (1971). Comparative Politics and the Comparative Method. *The American Political Science Review*, *65*(3), 682–693.

Limnéll, J., & Salonius-Pasternak, C. (2016). *Briefing Paper Challenge for NATO-Cyber Article 5*.

Lithuanian Minister for Defence. (2018). *Declaration of Intent - CRRTs*. 1–2.

Long, T. (2017). It's not the size, it's the relationship: from 'small states' to asymmetry. *Int Polit*, *54*(2), 144–160.

Lykkeberg, R. (2017). *Danmark er pludselig blevet alene i verden*. Information. https://www.information.dk/debat/2017/06/danmark-pludselig-blevet-alene-verden

Lykketoft, M. (2019). *Lykketoft midt i Brexit-kaos: "Der er muligheder i enhver krise."* Lykketoft. https://www.avisen.dk/lykketoft-midt-i-soergeligt-brexit-kaos-eu-vigtigere_543233.aspx

Madsen, W. R., & Sørensen, C. (2019). *Kraftig stigning i aktiveringer af forsvarsforbeholdet* (p. 11). Tænketanken EUROPA.

Maldre, P. (2016). *Moving Toward NATO Deterrence for the Cyber Domain*. https://cepa.ecms.pl/files/?id_plik=2446

Malmvig, H. (2019). Through Thick and Thin: Will Danish Military Engagements with the U.S. Endure in the Middle East? - Foreign Policy Research Institute. *Https://Www.Fpri.Org/*.

Mcdowell, S., Nensey, Z., & Steinberg, P. (2014). Cooperative International Approaches to Network Security: Understanding and Assessing OECD and ITU Efforts to Promote Shared Cybersecurity. In *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 231–252). https://doi.org/10.1007/978-3-642-37481-4_13

McGuinness, D. (2017). *How a cyber attack transformed Estonia*. BBC NEWS. https://www.bbc.com/news/39655415

McKenzie, T. M. (2017). *Is Cyber Deterrence Possible?* https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF

Melchior, Karen, Interview, (2020).

Melzer, N. (2011). *Cyberwarfare and International Law*.

Midtgaard, K. (2005). *Småstat, magt og Sikkerhed: Danmark og FN 1949-65*. Syddansk Universitetsforlag.

Mikecz, R. (2012). Interviewing Elites: Addressing Methodological Issues. *Qualitative Inquiry*, *18*(6), 482–493.

Ministry of Foreign Affairs of Denmark. (n.d.). *About TechPlomacy*. Techamb.Um. Retrieved May 27, 2020, from https://techamb.um.dk/en/techplomacy/

Ministry of Foreign Affairs of Denmark. (2018a). *Foreign and Security Policy Strategy 2019-2020*.

Ministry of Foreign Affairs of Denmark. (2018b). *Techplomacy: Mød Danmarks teknologiske ambassadør*. Regeringen.Dk. https://www.regeringen.dk/nyheder/2018/techplomacy-moed-danmarks-teknologiske-ambassadoer/

Ministry of Foreign Affairs of Denmark. (2020). *The Trade Council*. Ministry of Foreign

Affairs. https://thetradecouncil.dk/

Moret, E., & Pawlak, P. (2017). *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?* (Issue July). https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime

Mouritzen, H. (2015, October). *Vores udenrigspolitik skal drives af substans - ikke kun positionering*. Politiken. https://politiken.dk/debat/kroniken/art5593824/Vores-udenrigspolitik-skal-drives-af-substans-ikke-kun-positionering

Nasra, S. (2010). *Weak Power, Great Influence: Small States in EU Foreign Policy. The Case of Belgium and Greece*.

NATO. (n.d.). *Smart Defence*. NATO.Int. https://www.nato.int/docu/review/Topics/EN/Smart-Defence.htm

NATO. (2014). *Wales Summit Declaration*. NATO.Int. https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO. (2019a). *Collective defence - Article 5*. NATO.Int. https://www.nato.int/cps/en/natohq/topics_110496.htm

NATO. (2019b). *NATO Cyber Defence*. https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO. (2019c). *NATO Cyber Defence (Fact Sheet)*. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf

NATO. (2020a). *Cyber defence*. https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO. (2020b). *Deterrence and defence*. NATO.Int. https://www.nato.int/cps/en/natohq/topics_133127.htm

NATO. (2020c). *Member countries*. NATO.Int. https://www.nato.int/cps/en/natohq/topics_52044.htm

NATO. (2020d). *Relations with the European Union*. NATO.Int. https://www.nato.int/cps/en/natohq/topics_49217.htm

NCI. (2013). *MN Cyber Defence Capability Development (MNCD2) Project Opening*

Ceremony 14 March 2013 NCI Agency, Brussels. NATO Communications and Information Agency. https://na.eventscloud.com/ehome/57649/104949/

NCI. (2015). *MN CD2 nations expand cyber defence coordination system functionalities*. NATO Communications and Information Agency. https://www.ncia.nato.int/about-us/newsroom/mn-cd2-nations-expand-cyber-defence-coordination-system-functionalities.html

Neumann, I. B., & Gstöhl, S. (2006). Introduction. In J. Beyer, S. Gstöhl, C. Ingebritsen, & I. Neumann (Eds.), *Small States in International Relations* (pp. 3–36). University of Washington Press.

Neumeyer, J. (2012). *Malta and the European Union: A small island state and its way into a ... - Julia Neumeyer - Google Bøger*.

Nielsen, P. H. (2018). *Hvad er NIS-direktivet egentlig?* Net1.Dk. https://www.net1.dk/nyheder/forsyning/hvad-er-nis-direktivet-egentlig/

Nissen, C., Banke, C. F. S., & Schmidt, J. L. (2020). *European defence cooperation and the Danish opt-out* (Issue April). Danish Institute for International Studies.

Nye Jr, J. S. (2016). The Evolution of the Internet: From Military Experiment to General Purpose Technology. *Journal of Cyber Policy*, *1*(2), 44–71. https://doi.org/10.1162/ISEC_a_00266

No. 2016/794, 53 (2016): EU forordning 2016/794 om Europol, Pub. L.

Olesen, T. B. (2013). *Danmark i EF 1973-1993*. Danmarkshistorien.Dk. https://danmarkshistorien.dk/leksikon-og-kilder/vis/materiale/danmark-i-ef-1973-1993/?fbclid=IwAR1SlKxzVrbTiN8OsnIBhneYYW_FFe4fF3gZ5VEHIlhyBdtNGl-2_x94vr0

Pank, S. C. (2019). *What is the scope of legal self-defense in International Law? Jus ad bellum with a special view to new frontiers for self-defense*. https://law.au.dk/fileadmin/Jura/dokumenter/forskning/rettid/Afh_2014/afh19-2014.pdf

Parks, L., & Schwoch, J. (2012). *Down to Earth*. Rotgers University Press.

Patrick, S. M. (2018). *NATO's Deterrence Problem: An Analog Strategy for a Digital Age*.

https://www.cfr.org/blog/natos-deterrence-problem-analog-strategy-digital-age

PESCO. (2020). *PESCO*. https://pesco.europa.eu

Petersen, E. S. (2009). *Det unge demokrati*. Danmarkshistorien.Dk. https://danmarkshistorien.dk/perioder/det-unge-demokrati-1848-1901/

Petersen, M. H. (2018). *Denmark always saw the UK as our best friend in the EU. Please don't leave us behind*. The Independent. https://www.independent.co.uk/voices/denmark-brexit-uk-eu-leave-friend-economic-deal-trade-europe-a8570336.html?fbclid=IwAR2gdWiNmzx9n1WzhE4I7CWLNgeqV5-FZ4vdvkdUWawk-NMqekS6o_EeBUo

Plantera, F. (2018). *NATO CCDCOE – Expertise and cooperation make our cyber space safer*. E-Estonia. https://e-estonia.com/nato-ccdcoe-expertise-cyber-space-safer/

Poulsen, H. (2009). *Udenrigs- og forsvarspolitik*. Danmarkshistorien.Dk. https://danmarkshistorien.dk/perioder/fra-systemskifte-til-besaettelse-1901-1940/udenrigs-og-forsvarspolitik/

Radikale Venstre. (n.d.). *Forsvar og sikkerhed*. Retrieved May 27, 2020, from https://fremad.radikale.dk/det-mener-vi-om/forsvar-og-sikkerhed/

Rasmussen, R. E. (2018). *16.084.426 hackerangreb ramte Danmark i 2017*. Altomdata.Dk. https://www.altomdata.dk/16-084-426-hackerangreb-ramte-danmark-2017/

Rasmussen, S. H., & Brunbech, P. Y. (2009a). Danmark og NATO i 1950'erne. In *Danmarkshistorien.dk*.

Rasmussen, S. H., & Brunbech, P. Y. (2009b). *Neutralitet, Norden eller NATO 1945-49*. Danmarkshistorien.Dk. https://danmarkshistorien.dk/perioder/kold-krig-og-velfaerdsstat-1945-1973/neutralitet-norden-eller-nato-1945-49/?fbclid=IwAR0vEPNDS4xxkCGQgxDOg1Ead7g9arhYHBLvP9LK9afrQf5Q0JvpkaYayWI

Renner, M. G. W. E. (2019). *NATO Cyber Policy Under Construction | SIGNAL Magazine*.

Rennison, C. M., & Hart, T. C. (2018). *Research Methods in Criminal Justice and Criminology*. Sage Publications.

Rivera, J. (2015). Achieving cyberdeterrence and the ability of small states to hold large states at risk. *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, *2015*-, 7–24.

Romm, J. J. (1993). *Defining National Security: The Nonmilitary Aspect*. Council of Foreign Relations Press.

Rothstein, R. L. (1968). *Alliances and Small Powers*. Columbia University Press.

Royal Danish Defence Academy. (2019). *Værnsfælles Doktrin for Militære Cyberspaceoperationer*.

Rynning, S. (2020). *National Expectations Regarding the European Defence Fund: the Danish Perspective*.

Saltzman, I. (2013). Cyber posturing and the offense-defense balance. *Contemporary Security Policy*, *34*(1), 40–63. https://doi.org/10.1080/13523260.2013.771031

Schaldemose, Christel, Interview, (2020).

Schmitt, M. N. (2011). CYBER OPERATIONS AND THE JUS AD BELLUM REVISITED. *Villanova Law Review*, *56*.

Schmitt, M. N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. In M. N. Schmitt (Ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press. https://doi.org/10.1017/9781316822524

Schreier, M. (2018). Sampling and Generalization. In U. Flick (Ed.), *The SAGE Handbook of Qualitative Data Collection* (pp. 84–97). SAGE Publications Ltd.

Schulze, E. (2018, September). When this country faced a suspected Russian cyberattack – it took some big steps to stop another. *Cnbc News*. https://www.cnbc.com/2018/09/21/when-this-country-faced-a-suspected-russian-cyberattack--it-took-some-big-steps-to-stop-another.html

Simmons, B., & Martin, L. (2002). International Organizations and Institutions. In B. Simmons, W. Carlsnaes, & T. Riesse (Eds.), *Handbook of International Relations* (pp. 326–351). SAGE Publications Ltd.

Snyder, G. H. (1961). *Deterrence and Defense*. Princeton University Press.

Socialistisk Folkeparti. (n.d.). *Internationalt og forsvar - Socialistisk Folkeparti*. Retrieved May 27, 2020, from https://sf.dk/det-vil-vi/internationalt-og-forsvar/

Statsministeriet. (2016). *Aftale om Danmarks tilknytning til Europol efter 1. maj 2017*. https://www.regeringen.dk/media/2740/aftale-om-europol-pdf.pdf

Steiner, H. (2016). *Cyber-Attacks as coercive instruments*.

Stoltenberg, J. (2019). *NATO will defend itself*. NATO. https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en

Swanborn, P. (2010). *Case Study Research: What, Why and How?* SAGE Publications, Inc.1-352.

Taddeo, M. (2018). The Limits of Deterrence Theory in Cyberspace. *Philosophy and Technology*, *31*(3), 339–355. https://doi.org/10.1007/s13347-017-0290-2

Tamkin, E. (2017, April). *10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?* Foreign Policy. https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

TFEU. (2008). EUR-Lex - 12008E/PRO/22 - EN. *Official Journal 115 , 09/05/2008 P. 0299 - 0303; .*

The Danish Government. (2018). *Danish Cyber and Information Security Strategy*. https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

The Economist. (2019). *Emmanuel Macron warns Europe: NATO is becoming brain-dead*. The Economist. https://www.economist.com/europe/2019/11/07/emmanuel-macron-warns-europe-nato-is-becoming-brain-dead

The European Union. (n.d.). *Regulations, Directives and other acts | European Union*. Retrieved May 27, 2020, from https://europa.eu/european-union/eu-law/legal-acts_en

The Trade Council. (2018). *TECHPLOMACY*. Ministry of Foreign Affairs.

Thorhallsson, B. (2000). *The Role of Small States in the European Union*. Routledge.

Thorhallsson, B. (2012). Small states in the UN Security Council: Means of Influence? *The Hague Journal of Diplomacy*, *7*(2), 135–160. https://doi.org/10.1163/187119112X628454

Thorhallsson, B., & Wivel, A. (2006). Small states in the european union: What do we know and what would we like to know? *Cambridge Review of International Affairs*, *19*(4), 651–668. https://doi.org/10.1080/09557570601003502

Tolga, İ. B. (2018). *Principles of Cyber Deterrence and the Challenges in Developing a Credible Cyber Deterrence Posture*.

Trimintzios, P., Chatzichristos, G., Portesti, S., Drogkaris, P., Palkmets, L., Liveri, D., & Dufkova, A. (2017). *Cybersecurity in the EU Common Security and Defence Policy (CSDP)*. http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

Tunggal, A. T. (2020). *What is a cyberattack?* UpGuard.Com. https://www.upguard.com/blog/cyber-attack?fbclid=IwAR0VNUaWWmXD4q19XXQbdxkthK13YnCSAG2WWiAII42n4jZ_GxY9jfOU8lk

Ullman, R. H. (1983). Redefining Security. *International Security*, *8*(1), 129–153.

United States of America, & Europol. (2001). *Agreement between The United States of America and The European Police Office*.

van Dijk, R. (2019). *The EU Cyber Diplomacy Toolbox: A Training in Collective Action*. https://jasoninstitute.com/2019/06/23/the-eu-cyber-diplomacy-toolbox-a-training-in-collective-action/

Vasiliauskaitė, E., & Šakūnas, T. (2018). *Memo for Mutual Assistance in Cyber Security*.

Vavra, S. (2019, August). *NATO cyber-operations center will be leaning on its members for offensive hacks*. CyberScoop.

Venstre. (n.d.). *Europapolitik - Venstre*. Retrieved May 27, 2020, from

https://www.venstre.dk/politik/venstre-mener/eu

Vital, D. (2006). The Inequality of States: a Study of the Small Power in International Relations. In J. Beyer, S. Gstöhl, C. Ingebritsen, & I. Neumann (Eds.), *Small States in International Relations* (pp. 77–88). University of Washington Press.

Wallace, D., & Visger, M. (2018). Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community. In *Journal of Law & Cyber Warfare* (Vol. 6, pp. 3–55). Lexeprint, Inc. https://doi.org/10.2307/26441289

Walt, S. M. (1991). The Renaissance of Security Studies. *International Studies*, *35*(2), 211–239.

Waltz, K. (1979). *Theory of International Politics*. Addison-Wesley Publishing Company.

Weichardt, B. (2019, January). *Dansk politi bruger Europol mere end nogensinde før*. Ritzaus Bureau.

Weiss, Pernille, Interview, (2020).

Wilkinson, J. R. (1956). Denmark and NATO: The Problem of a Small State in a Collective Security System. *International Organization*, *10*(3), 390–401.

Williams, P. (2004). Critical Security Studies. In *International Society and Its Critics* (pp. 1–18). Oxford University Press.

Wivel, A. (2014). Still Living in the Shadows of 1864? Danish Foreign Policy Doctrins and the Origins of Danmark's Pragmatic Activism. *Danish Foreign Policy Yearbook*, 109–139.

Wivel, A., & Crandall, M. (2019). Punching above their weight, but why? Explaining Denmark and Estonia in the transatlantic relationship. *Journal of Transatlantic Studies*, *17*(3), 392–419.

Woodcock, B., & Stapleton-Gray, R. (2011). National Internet Defense: Small States on the Skirmish Line. *ACMQueue*, *9*(1), 1–7.

Wulff, Thomas, Interview, (2020).

Yegin, M. (2019). *Turkey Between NATO and Russia: The Failed Balance* (pp. 1–4). SWP

comment.

Yin, R. K. (2009). *Case Study Research: Designs and Methods* (4th ed.). Sage Inc.

Yin, R. K. (2011). *Qualitative Research From Start to Finish*. The Guilford Press.

Zamarripa, E. (2020). The Permanent Structured Cooperation in the European Union. Its Real Potential Value. In J. M. Ramírez & J. Biziewski (Eds.), *Security and Defence in Europe* (pp. 87–95). Springer.

Aastrup Jensen, Michael, Interview, (2020).