CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Master Thesis

2022 **Kristýna Musilová**

CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Kristýna Musilová

Countering Hybrid Threats: Public-Private Cooperation in Norway and the Czech Republic

Master thesis

Prague 2022

Author: Bc. Kristýna Musilová

Supervisor: Mgr. Vojtěch Bahenský

Academic Year: 2021/2022

Bibliographic note

Musilová, K., 2022. *Countering Hybrid Threats: Public-Private Cooperation in Norway and the Czech Republic*. Master Thesis. Charles University, Faculty of Social Sciences, Institute of Political Studies. Supervisor: Mgr. Vojtěch Bahenský. 163 p.

Abstract

This thesis aims to present policy recommendations in the area of public-private cooperation to counter hybrid interference, especially cyber threats. Research of this kind is unique in Czech academia. There has not been a single published paper that would comprehensively tackle the issue of public-private cooperation as a tool to achieve societal resilience towards hybrid threats. The first part of the research is focused on the Norwegian cooperation model and identifies tools and mechanisms thanks to which was societal resilience-building successful. The second part of the thesis analyses the current situation in the Czech Republic and attempts to identify shortcomings in hybrid threat resilience. The core of the research consists of eighteen semi-structured interviews with the representatives of the Norwegian and Czech public and private sectors. The result is policy recommendations for the Czech government based on an open-source data analysis supplemented by information from the interviews. These recommendations specify applying Norwegian collaboration tools between the public and private sectors. The key suggestions are the implementation of the "system of POCs", preparation of crisis scenarios, which is to a certain extent follow-up of the so-called "standard operating procedures" prepared by the IZS ČR or setting up the "National Cyber Security Forum", which will enhance the dialogue between the public and private sectors.

Abstrakt

Cílem této diplomové práce je předložit doporučení v oblasti spolupráce soukromého a veřejného sektoru při čelení hybridnímu působení, zejména pak kybernetickým hrozbám. Výzkum tohoto typu je v českém akademickém prostředí unikátní—dosud nebyla publikována práce, která by se takto komplexně zabývala spoluprací veřejného a soukromého sektoru jakožto nástroje k docílení resilience společnosti při čelení hybridnímu působení. V první části se výzkum zabývá norským modelem spolupráce soukromého a veřejného sektoru a identifikuje nástroje a mechanismy, díky kterým je budování celospolečenské odolnosti v Norsku úspěšné. Tato případová studie je výrazným doplňujícím přínosem diplomové práce. Druhá část práce analyzuje současnou situaci v ČR a identifikuje nedostatky při čelení hybridním hrozbám. Nejzásadnějším přínosem celé práce je pak samotná výzkumná část, kterou tvoří osmnáct polostrukturovaných rozhovorů s představiteli norské a české veřejné správy a soukromých společností. Výsledkem analýzy otevřených zdrojů doplněných o data získaná prostřednictvím rozhovorů je soubor doporučení pro českou veřejnou správu. Tato doporučení specifikují, jakým způsobem lze aplikovat norské nástroje spolupráce veřejné správy a soukromého sektoru v Česku. Nejdůležitějšími doporučeními je implementace tzv. systému kontaktních bodů („*system of POCs*“), vytvoření krizových scénářů, které do jisté míry navazují na tzv. typové plány připravované IZS ČR, či založení Národního fóra kybernetické bezpečnosti, které podpoří dialog mezi veřejným sektorem a soukromou sférou v oblasti výměny informací a zkušeností.

Keywords

hybrid threats, public-private cooperation, Norway, the Czech Republic, cyber security, societal resilience, countering hybrid threats, state preparedness, crisis management

Klíčová slova

hybridní hrozby, spolupráce soukromého a veřejného sektoru, Norsko, Česká republika, kybernetická bezpečnost, společenská odolnost, čelení hybridnímu působení, připravenost státu, krizové řízení

Range of thesis: 186 806 characters

Declaration of Authorship

1. The author hereby declares that he compiled this thesis independently, using only the listed resources and literature.

2. The author hereby declares that all the sources and literature used have been properly cited.

3. The author hereby declares that the thesis has not been used to obtain a different or the same degree.

In Prague on May 3, 2022 Bc. Kristýna Musilová

Acknowledgements

First and foremost, I am extremely grateful to my supervisor, Mgr. Vojtěch Bahenský for his invaluable advice, support, and patience during working on my thesis. I would like to thank all the Institute of Political Science members. Their kind approach and continuous support have made all my years of studies a wonderful, enriching time full of inspiration and desire to improve.

My whole research would have been impossible without the interviewees' goodwill, kindness, and precious time. Even though I cannot mention your names, I am profoundly grateful to each one of you.

I want to thank my friends, who did bear with me during those difficult times and cheered me up when I needed it the most. Thank you that you believed in me when I did not.

Finally, I would like to express my deepest gratitude to my family, especially Lucie, Marek, Hana, Vladimíra, František and Štěpán. Thank you for your tremendous encouragement, understanding and unlimited support throughout my life. Without you, none of these would be possible. Maminko, Marku, babičko, dědečku—děkuji.

Content

List of Abbreviations

Abbreviation	English / Norwegian / Czech
BIS	Security Information Service (Bezpečnostní informační služba)
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CTHH	Center Against Terrorism and Hybrid Threats (Centrum proti terorismu a hybridním hrozbám)
DSB	The Norwegian Directorate for Civil Protection (Direktoratet for samfunnssikkerhet og beredskap)
FD	Norwegian Ministry of Defence (Forsvarsdepartementet)
ECSM	European Cyber Security Month
EDA	European Defence Agency
ENISA	European Union Agency for Cybersecurity
EU	European Union
ICT/IKT	Information and Communications Technology (Informasjons- og kommunikasjonsteknologi)
IMF	International Monetary Fund
IZS ČR	Integrated Rescue System of the Czech Republic (Integrovaný záchranný system České republiky)
ITU	International Telecommunications Union
JD	Norwegian Ministry of Justice and Public Security (Justis- og beredskapsdepartementet)
KDD	Norwegian Ministry of Local Government and Regional Development (Kommunal- og distriktsdepartementet)
MPO	Czech Ministry of Trade and Businness (Ministerstvo průmyslu a obchodu)
MVCR	Czech Ministry of Interior (Ministerstvo vnitra)

MZV	Czech Ministry of Foreign Affairs (Ministerstvo zahraničních věcí)
NATO	North Atlantic Treaty Organization
NBÚ	National Security Authority (Národní bezpečnostní úřad)
NCISA	National Cyber and Information Security Agency
NCSC	Norwegian National Cyber Security Centre
NGO	Non-governmental Organisation
NKÚ	Supreme Audit Office (Národní kontrolní úřad)
NORDEFCO	Nordic Defence Cooperation
NSM	Norwegian National Security Authority (Nasjonal sikkerhetsmyndighet)
NSR	Norwegian Business and Industry Security Council (Næringslivets Sikkerhetsråd)
NTNU	Norwegian University of Science and Technology
NÚKIB	National Cyber and Information Security Agency (Národní úřad pro kybernetickou a informační bezpečnost)
NUPI	Norwegian Institute of International Affairs (Norsk Utenrikspolitisk Institutt)
OECD	Organisation for Economic Co-operation and Development
OSCE	Organisation for Security and Cooperation in Europe
POC	Point of Contact
PPC	Public-Private Cooperation
PPP	Public-Private Partnerships
UD	Norwegian Ministry of Foreign Affairs (Utenriksdepartementets)
V4	Visegrad Four
WEF	World Economic Forum

List of Appendices

List of Tables

Introduction

Throughout the several last years, the concept of "hybrid threats" has become a popular buzzword to describe conventional warfare's complex reality combined with irregular tactics. In 2019, the Czech government issued a Strategy and an Action Plan for countering hybrid threats. Both these strategic documents consider "resilience" the crucial strategic objective when countering hybrid threats. The resilience should be achieved, *inter alia*, through "strengthening capabilities of the critical infrastructure elements to maintain their sufficient functionality for instances of being targeted by hybrid interference". However, a significant part of the critical infrastructure is owned, administered, and operated by the private sector. Hence, enhanced cooperation between the public and private sectors is essential. Yet, both abovementioned strategies completely omit this aspect of security and the matter of public-private cooperation.

Countering hybrid threats is a difficult task without a doubt. Following the events in 2014, several countries have re-invoked the concept of the so-called "total defence" in their approach to security, among others, Sweden, Norway, and Lithuania. Nordic countries have been historically the proponents of total defence, which is naturally built on involving all the parts of society in the national defence. Hence, Norway, Sweden, and Finland are at the forefront of these efforts to achieve a whole-of-society approach to security. In this thesis, Norway has been selected to serve as a case study for countering hybrid threats through the tools of public-private cooperation. The reasons are further elaborated below in subchapter 1.2.

So, why is this thesis investigating hybrid threats and public-private cooperation as a tool to counter them? In the last decade, hybrid threats have

gained strength and got into the focus of many states and organizations, not only the Nordic countries. Since 2016, the EU and NATO have identified countering hybrid threats as a priority. In Helsinki, the new Hybrid CoE was set up to facilitate and strengthen EU-NATO cooperation and provide a forum for strategic discussions and joint training and exercises. NATO perceives national resilience as an essential element of credible deterrence and proposes two deterring approaches to hybrid threats: *deterrence by denial* (where societal resilience would be a major element), and *deterrence by punishment* (which seeks to change the hostile behaviour of potential adversary, for instance through sanctions). Yet, despite the rising threat, practical attempts to build resilience or to adopt a whole-of-society approach to security are missing in the Czech political environment.

Given the Czech strategic documents, this thesis focuses on the approach of *deterrence by denial*, i.e., through the building of societal resilience. The thesis aims to answer the following research question: *What instruments from Norway's approach to public-private cooperation can the Czech Republic implement to enhance its resilience towards hybrid threats?* To provide an answer, the thesis firstly brings forward a case study of the Norwegian approach to public-private cooperation in terms of hybrid threats. Secondly, the author proposes policy recommendations for the Czech public stakeholders on enhancing societal resilience.

Resilience can be understood as putting the effort into improving the interaction between politics, citizens, and the armed forces; or creating a new basis for dialogue and cooperation with international organizations. In the Czech strategic documents, resilience is understood as the "*ability of a state and society to cope with a sustained and intensive hybrid interference without a significant negative impact, and to redress immediately and restore a full functionality in case*

damage occurs". Given the inherent nature of the hybrid threats, there are many ways of achieving resilience. Yet probably the most efficient strategy is implementing a whole-of-society approach to security. One means of implementing a whole-of-society approach is strengthening public-private cooperation. Though, public-private cooperation is practically missing in the Czech environment—at least in an institutionalised form. And without the cooperation between the public and private sectors, it is almost impossible to attain a whole-of-society approach. So, this thesis aims to fill the gap in the research and provide a case study on the Norwegian model that could serve as an inspiration for the Czech efforts to build resilience.

Let us look into the structure of the thesis. Firstly, the thesis introduces the research design, data, and research limits. The second chapter presents the current academic research on hybrid threats, concrete tools of hybrid warfare, and a debate on the relevant countermeasures. The third chapter analyses the current situation in the Czech Republic and identifies the gaps in public-private cooperation. The fourth chapter investigates the Norwegian model of public-private cooperation to counter hybrid/cyber threats and identifies the lessons learned. The main contribution of this descriptive chapter is presenting a coherent case study on the Norwegian approach, which is in this form unique in academia. The most essential part of the thesis is chapter 5, which summarises the research results and delivers the policy recommendations. The chapter draws from the open-source analysis of the Czech and Norwegian approaches to cybersecurity and is complemented by the data obtained from the eighteen semi-structured interviews conducted with Norwegian and Czech representatives from the public sector and private businesses. The thesis is concluded with a summary of the policy recommendations and the main contributions of the research.

1 Research Design

This chapter describes how the research will be conducted and sheds light on gathering and analysing data. The thesis is mainly policy-oriented. The research aims to provide Czech public authorities with policy recommendations on improving national resilience towards selected hybrid threats—cyber threats.

1.1 Research Question

The purpose of the thesis is to answer the following research question:

What instruments from Norway's approach to public-private cooperation can the Czech Republic implement to enhance national[1] resilience towards hybrid threats?

The main objective of the thesis is to propose *how* exactly can the Czech Republic amend its approach to the hybrid threats inspired by the instruments of public-private cooperation utilised in Norway. To provide a comprehensive explanation of the abovementioned research question, the thesis will also endeavour to answer the following sub-question:

What specific instruments of public-private cooperation utilise Norway? How and why do they work?

This sub-question explains the Norwegian security strategy regarding public-private cooperation and its roots in the total defence concept. Overall, the thesis seeks to understand and explore the conditions under which the

[1] By '*national*' is meant nation-state and its constituent elements, i.e., public institutions, critical infrastructure, private sector (businesses), and civil society (individuals).

resilience of the Czech Republic towards hybrid threats may be enhanced and identify why public-private cooperation works in Norway.

To sum up, the thesis aims to (i.) analyse the Norwegian approach to public-private cooperation to counter hybrid threats and (ii.) recommend policies for public-private partnership in the Czech Republic.

1.2 Data and Sources

This part explains how exactly the research was conducted, why was Norway selected to serve as a case study, who were the interviewees, how were they selected, and the sources of data. To summarise the research design of the thesis, the author interviewed Norwegian and Czech stakeholders profiled from the public sector, private companies, and academia. Based on an open-source analysis of the government documents and strategies *and* the data gathered from the interviews in Norway, the author presents a case study of public-private cooperation in Norway. Based on an open-source analysis of the current situation in the Czech Republic, the author proposes policy recommendations for the Czech Republic. The feasibility and desirability of these recommendations were verified through another set of interviews with the Czech stakeholders. Altogether, the author conducted 18 semi-structured interviews with the Norwegian and Czech stakeholders over a three-month period between February and April 2022.

Norway was selected as a model for the Czech Republic based on shared priorities in foreign politics (including NATO membership), similar perception of the current threats (cyberattacks, disinformation, supply chain safety as national security priorities), and relatable geopolitical situation considering the current threats (Norway shares the direct land and sea border

with Russia; the Czech Republic is a former Cold War satellite considered by Russia as its sphere of influence). As a small state, Norway has also traditionally relied on foreign allies (Riste 2005), similarly to the Czech Republic. Furthermore, Norway represents a country with a strong tradition of the total defence concept. Currently, Norway is rebuilding its civil defence by drafting strategies, designating coordinating institutions, imposing additional responsibilities on central, regional, and local entities, and developing cooperation between the private and public sectors (European Parliament 2021, p. 2). Hence, Norway serves as a valuable case study on implementing the total defence concept and how to build up societal resilience (European Parliament 2021, p. 2), which deserves academic attention.

Firstly, the thesis presents an open-source analysis of the current situation in the Czech Republic in terms of public-private cooperation. The open-source analysis is complemented by some information gained through the interviews with the Czech stakeholders. This is done to provide the reader with a coherent overview of the state of art in the Czech Republic. Then, by analysing the Czech resilience-building in the case of cyber threats, the author identifies the gaps in the Czech approach (subchapter 3.2). This Czech case study is done to identify the tools and mechanisms utilised in the Czech Republic with the goal of not reinventing the wheel. Secondly, the thesis identifies Norway's approach to public-private cooperation in countering hybrid threats. Conducting the case study of the Norwegian approach (chapter 4) together with the open-source analysis presented in chapter 3 allows the author to assess which of the instruments can be utilised in the Czech environment to enhance resilience. While every country has specific conditions allowing for particular policies, the interviews conducted in the

Czech Republic proved the feasibility of transposing the Norwegian measures into the Czech environment.

Conducting the case study of the Norwegian approach is done through an open-source analysis of the existing sources. The sources used are both primary and secondary—they include official documents issued by the government (in English and Norwegian), academic resources, independent analyses conducted by the think tanks and non-governmental organisations, and papers, press releases, and reports issued by international organisations (mainly NATO and the EU). While the data gained from interviews are the cornerstone of case study research, collecting data from other sources should be a strength of the case study as it allows for 'triangulation'. Triangulation enhances construct validity as each source of evidence may be 'tested' against each other (Marginson 2004, p. 329). By combining theories, methods, or observers in a research study, triangulation can "help ensure that fundamental biases arising from a single method, or a single observer are overcome" (Noble and Heale 2019, p. 67).

The open-source analysis provided answers on *how* the 'Norwegian model' of public-private cooperation supposedly works. To answer *whether* and *why* public-private cooperation works in Norway, the author conducted semi-structured interviews with Norwegian representatives profiled from the public sphere, private sector, and academia. In qualitative research as such, various methods of analysis may apply, for instance, interviews, focus groups, or observations. Considering the case of this thesis, semi-structured interviews represent a suitable method to gather data. Asking open-ended questions allows for exploring individual experiences or opinions regarding the researched phenomenon. As the interviewer does not follow one formalised list of questions, there is broader space for a discussion with the interviewees

and the potential to acquire more in-depth and valuable data (Edwards and Holland 2013).

So, to acquire valuable data from the interviews, the theoretical information gained from the open-source analysis was used to formulate questions. After developing the questions forming the basis of the interviews, the interviews were conducted online through a videoconferencing platform and lasted from half an hour to one hour. The interview respondents were selected using two techniques—purposeful sampling and snowball sampling. The following was used to select respondents for the study of public-private cooperation in Norway and the Czech Republic. All respondents:

- were present or former employees in the public sector (ministries, governmental bodies, or agencies) or private companies;
- held positions related to the issue of hybrid threats, especially cybersecurity;
- had at least two-year experiences in work;
- representatives from the private companies were selected only from the large businesses with more than 1000 employees to ensure they are important enough to cooperate with the government.

In addition, the author applied some specific criteria in the selection of respondents for each of the research groups (public sector, private businesses, academia). These criteria were intended to maximise the value of the information provided by the respondent (e.g., in a private company, a communication expert responsible for the strategic communication of the cyber-attack would probably offer more valuable information than an IT expert focusing solely on the technical aspect of the attack). Altogether, the author conducted ten interviews with Norwegian representatives divided into

three groups: (i.) public sector, (ii.) private businesses, (iii.) academia, and eight interviews with the Czech stakeholders.

The Norwegian respondents and their affiliations are shown in the table below. The two experts from academia are not cited in the thesis. While their information was interesting, it was not as relevant as the views of the public and private sector entities. Hence, they were not used in the thesis, but several of their pieces of advice helped the author to address relevant interviewees or find interesting sources.

Pseudonym of the representative	**Affiliation**	**Group**	**Date of interview**
JD representative #1	Ministry of Justice and Public Security (JD)	Public Sector	14 March 2022
JD representative #2	Ministry of Justice and Public Security (JD)	Public Sector	14 March 2022
UD representative	Ministry of Foreign Affairs (UD)	Public Sector	16 February 2022
KDD representative	Ministry of Local Government (KDD)	Public Sector	9 March 2022
NorSIS representative	Norsk Senter for informasjonssikring (NorSIS)	Public Sector	16 February 2022
DSB representative	The Norwegian Directorate for Civil Protection (DSB)	Public Sector	30 March 2022
Private sector representative #1	Energy Company	Private Business	23 February 2022
Private sector representative #2	Media Company	Private Business	25 February 2022
NUPI rep. #1	Norwegian Institute of International Affairs	Academia	9 February 2022
NUPI rep. #2	Norwegian Institute of International Affairs	Academia	15 February 2022

Table 1: List of the participants in the interviews conducted in Norway
Source: Author's list

The author has addressed all the Norwegian institutions responsible for the cybersecurity and protection of society against hybrid threats. Altogether, the author contacted 28 responsible personnel from the public and private sectors, of which ten agreed to be interviewed. The reasons to refuse were mainly security. The author contacted 12 private companies from the critical infrastructure. Unfortunately, only one of them provided the author with some information. The other company willing to talk to the author is not a part of the critical infrastructure. However, the representative's insight was a valuable asset.

Finally, based on the Norwegian case study and analysis of the gaps in the Czech approach, the author formulates the policy recommendations for the Czech Republic (chapter 5). To verify and confirm the feasibility and desirability of the author's proposals (i.e., whether they can work in the Czech environment or whether the measures already exist), the author interviewed the Czech stakeholders within the public and private sectors. The author conducted eight interviews. Five of them were with representatives from the public sector, and two of them were with representatives from private companies (of which one is part of the critical infrastructure). To gain more profound and valuable insight, the author conducted one interview with a representative from the Benešov Hospital, a victim of a severe cyberattack. Some information from the interviews was also used in chapter 3 on the Czech strategy to complement the open-source analysis and provide the reader with a coherent and consistent case study. The table on the next page outlines the representatives and their affiliations.

Pseudonym of the Representative	Affiliation	Group	Date of interviev
MV representative	Ministry of Interior (MV)	Public Sector	14 April 2022
NÚKIB representative	National Cyber and Information Security Agency (NÚKIB)	Public Sector	3 May 2022
MZV representative	Ministry of Foreign Affairs (MZV)	Public Sector	21 April 2022
MO representative	Ministry of Defence (MO)	Public Sector	11 April 2022
MPO representative	Ministry of Trade and Business (MPO)	Public Sector	13 April 2022
Benešov Hospital representative	Hospital of Rudolf and Stefanie in Benešov	Public Sector	30 April 2022
Private sector representative #3	Private Business (Communications)	Private Business	25 March 2022
Private sector representative #4	Private Business (Transportations)	Private Business	7 April 2022

Table 2: List of the participants in the interviews in the Czech Republic
Source: Author's list

The Norwegian and Czech interviews represented an essential source of information as the respondents possess crucial knowledge that is impossible to obtain by any other means. Several of the respondents provided the author with new documents that would be nearly impossible to find online and shared sensitive and personal information concerning cybersecurity in Norway and Czechia, not only about themselves but also third parties. Hence, to access this valuable yet sensitive information, the author promised confidentiality to the respondents. Upon the agreement the researcher and project participants settled upon during obtaining informed consent, the author does not mention the names of the respondents, only the institution

they represent.[3] As the participants were high-ranking representatives from the public sector, revealing their identity could potentially harm their careers as they shared their personal experience and opinion on how public-private cooperation work in Norway and the Czech Republic. So, to gain access to beneficial information, the author offered the respondents to anonymise their answers and only provide the reader with the name of the institution they represented to protect them.

1.3 Limits of the Research

Despite the author's utmost effort, she did not manage to conduct all the interviews as intended in the thesis project. The missing interviews are from the Norwegian Ministry of Defence (FD) and the Norwegian National Cyber Security Centre (NCSC). The author contacted all these authorities several times (by e-mail and phone). However, none of the persons reached did reply.

Secondly, regarding the research design, it would be beneficial to conduct more interviews with the Norwegian and Czech private companies. Though, the scope of the thesis did not allow to do a large-scale survey with the private business' representatives. Henceforth, a quantitative analysis remains a possibility for future research.

For the author, one of the main obstacles was the war in Ukraine that broke out in February 2022. Several institutions and private companies refused to talk to the author due to work overload and/or security reasons. Nonetheless,

[3] Ensuring the anonymity of the participants is one of the ethical standards of the research. For example, in October 2012, the American Political Science Association amended its Guide to Professional Ethics in Political Science to include new requirements for how scholars should present their research and the evidence upon which it is based, including the anonymisation of data sources that may be needed for ethical reasons or legal reasons.

in Norway, the companies are very transparent. All the information about their approach to cyber security and hybrid threats is available online. Hence, several companies rejected the interview as they could not provide the author with any new valuable information besides the already published information. However, in several cases, companies' representatives provided the author with interesting documents, videos, or materials not available online/challenging to reach (e.g., they were in Norwegian and/or accessible only on request).

Lastly, a tricky part may represent the interviews themselves. To conduct the interviews, the author utilised her experience and contacts from the Ministry of Defence to reach out to the relevant stakeholders. However, the author has never met with the respondents before the interviews. So, there was a potential lack of trust and suspicion during the interviews. This may lead to skewed answers, missing an essential piece of information, or providing the author with incomplete/misleading information. To avoid these potential research limits, the author cross-checked the data during the interviews with various representatives to get an accurate picture. In addition, the author attempted to confirm the correctness of the information with the primary and secondary sources.

2 Literature review

In the following chapter, the author aims to contextualise the topic—i.e., the concept of public-private cooperation as a means of countering hybrid threats—within the already existing stream of literature. The research on hybrid warfare, hybrid threats, and adequate countermeasures is immense. However, only a very few papers and works focus on public-private cooperation as a suitable way to counter hybrid threats. At the same time, no research or case study focuses on the concrete approaches adopted by the concrete countries, including Norway and Czechia.

Firstly, the author will introduce the concept of hybrid warfare, a phenomenon that has been at the centre of academic attention for several last years. The author takes the liberty to emphasise that the purpose of this paper is not to discuss the usefulness of the somewhat ill-defined concept of hybrid warfare. Nevertheless, it is necessary to envisage what exactly is meant by "hybrid threats" and the current state of the academic debate—mainly as both Norway and the Czech Republic[4] utilise the term "hybrid warfare" in their national security strategies. The first part will be followed by the research on the specific tools of hybrid warfare, which has been heavily discussed within the academic circles—and the Czech and Norwegian national documents. As hybrid warfare can include any non-kinetic[5] means of warfare, the thesis will later focus only on one selected tool of hybrid warfare—cyber threats. This

[4] Also, the crucial political and military organisations such as NATO and the EU at many places; see, for instance, a document issued in 2015 by the NATO Defense College called "NATO's Response to Hybrid Threats, edited by G. Lasconjarias and J. A. Larsen. Available at: http://www.ndc.nato.int/download/downloads.php?icode=471.

[5] According to several authors, "hybrid threats" may also include *kinetic* warfare, which only bears out the heavily criticised "fluidness" of the concept.

narrowing compared to the original intention of the thesis project is further explained in subchapter 2.2 (p. 37-38).

The third part of the review sheds light on the concept of public-private cooperation in Norway and what has been written about the specific countermeasures. A particular focus is put on the role of societal resilience.

The last part of the literature review outlines the theoretical framework of three pillars. This theory is used in chapter five to analyse the results, compare the Norwegian and Czech tools, and suggest suitable policy recommendations.

2.1 Debate on Hybrid Warfare: Old Wine in a New Bottle?

Shortly after the Russian annexation of Crimea in 2014, the term hybrid warfare rose to prominence among defence and policy circles, media, and the broad public. However, despite an increased interest in the buzzword, there is no agreed definition of hybrid warfare. The absence of one universal definition led to many similar concepts and debates over how to define and differ 'Gray Zone Aggression,' 'Hybrid Warfare,' 'Multi-Domain Warfare,' and 'Irregular Warfare.' According to some scholars (e.g., Stoker and Whiteside 2020; Puyvelde 2015; Paul, 2016; Cox, Bruscino and Ryan 2012; Caliskan and Liégeois 2020), debates on the nature of "hybrid warfare" are counterproductive; they attempt to separate the military and civil dimensions of the warfare. Briefly, according to these scholars, the label "hybrid warfare" is merely an "old wine in a new bottle" and is nowhere near to be a novel concept (e.g., Murray and Mansoor 2012). Also interesting is Cordesman's (2020, p. 7) statement that efforts to precisely define "hybrid warfare" completely ignore the fact that the history of war has often begun

after decades of competition at a *non-military* level. According to the critics, the term "hybrid warfare" does not make any sense as it is mainly tactically focused—and wars do not consist of just tactical systems (Cox, Bruscino, and Ryan 2012). Stoker and Whiteside (2020) then argue that as "hybrid warfare" describes almost every form of interstate competition, it becomes more confusing than clarifying.

While several authors dealt with the concepts like what was later marked as hybrid warfare in the early 2000s, their works went largely unnoticed. In 2005, the most influential author of hybrid warfare literature, Frank G. Hoffman, published his first article on the *Future Warfare: The Rise of Hybrid Wars*. Later, in 2007, irregular warfare operations garnered significant attention when Hoffman labelled them as "hybrid warfare" in his book *Conflict in the 21st Century*. However, with his co-author J. Mattis, Hoffman described hybrid warfare strictly in military terms as a different means of war (Hoffman & Mattis 2005, p. 1). Hoffman continued to focus on hybrid warfare, and his articles were the first to serve as academic material seriously concerning the issue of hybrid warfare. While his military-centric definition of hybrid warfare may be considered obsolete today, he indeed did draw the attention of other scholars. He kicked off the academic debate on the nature of hybrid warfare. Then, several scholars (e.g., Mansoor 2016; Chivvis 2017; Reichborn-Kjennerud and Cullen 2016; Giegerich 2016; Weissmann 2019, Schmidt 2014) came up with improved and up-to-date definitions of hybrid warfare.

So, what was the nature of the hybrid warfare debate between the late 2000s and early 2020s? While many scholars mainly focus on the military aspect of hybrid warfare and marginalise its relevance to other parts of warfare (e.g., psychological warfare, disinformation, cyber warfare), several scholars investigated hybrid warfare also from different sides than the complex

security (e.g., Danyk, Maliarchuk and Briggs 2017; Wither 2016; Daniel and Eberle 2018; Daskalov 2018). Yet almost all scholars conclude that "hybrid warfare" remains a vaguely defined concept lacking any measurable variables and rather causes confusion instead of clarifying the reality of modern warfare (Stoilova 2018, p. 138).

Still, many countries utilise the definition—despite its flaws. So, for the thesis, it is vital to present national definitions of the countries examined—the Czech Republic and Norway—as they directly influence the state's response to hybrid interference. As Czechia and Norway are member-states of the North-Atlantic Treaty Organization (NATO), NATO's definition is also mentioned. The reason is that both countries are cooperating within NATO, and countering hybrid threats is one of NATO's top priorities as of 2021 (Hagelstam 2018).

Czech definition of hybrid interference is defined in the *National Strategy for Countering Hybrid Interference* (*from now on,* the Strategy) adopted in 2021. Its wording is based on the definitions adopted by the EU and NATO. It goes as follows: "*[h]ybrid interference involves both covert and overt actions by the state as well as non-state actors (perpetrators of hybrid interference), which target vulnerable elements of democratic states and societies*. The perpetrators aim to "*disrupt the working of democratic institutions, the rule of law processes, and internal security*" by "utilisation *political, diplomatic, information, military, economic, financial, intelligence, and other tools*" (Ministry of Defence 2021, p. 4). While several other national documents operate with term "hybrid threats," Czech Strategy uses a subtler term "hybrid interference."

Norwegian definition of hybrid threats is not significantly different from the Czech one; however, besides using the term "hybrid threats," the Norwegian government also utilises "influence operations." The conceptual

definition describes hybrid threats as *"a mix of different instruments/means: diplomatic, military, economic, judicial, intelligence or information-related. Both state and non-state actors employ hybrid means or tactics. The blurred distinction between state and non-state activity adds to the challenge. Hybrid activities seek to create confusion, doubt, and chaos. The aim is to influence public opinion, hamper effective decision-making and undermine public trust and political unity. At worst, hybrid activities can challenge states' fundamental security and political integrity*" (Halvorsen 2020). As for the Norwegian academia and current research, most researchers focus on the region of the High North (mainly because of the 195-kilometre land border and 23-kilometer marine border between Norway and Russia). In the research, Russia and China are the primary sources of hybrid threats in the Arctic, mainly due to their long-term interests in the region, e.g., the Polar Silk Road project (Konyshev 2020, p. 141). As Russia and China are not keen on an open military confrontation in the Arctic, indirect influence methods through diplomacy, economic, and scientific cooperation are used to strengthen influence in the region (Konyshev and Kobzeva 2017).

So, to conclude this chapter, hybrid warfare is a well-liked label with the potential to encompass the whole complexity of any conflict—primarily because it is so vaguely formulated that basically anything may be considered a hybrid operation. Still, whatever we label it, hybrid operations remain a severe issue for the nations' security. The following subchapter outlines the current research on the "hybrid warfare toolbox" to dig deeper into the means and tools of hybrid operations.

2.2 Hybrid Warfare Toolbox: What is the Threat?

In this part of the literature review, the author will present concrete instruments and tools of hybrid warfare discussed in the literature. While the

purpose of the thesis is not to debate the definition of hybrid threats/warfare, it is essential to provide the reader with an outline of concrete tools and how hybrid war is fought. As the thesis aims to formulate policy recommendations to enhance national resilience towards hybrid threats, it is essential to identify what are the threats.

There are several possible ways how to categorise tools of hybrid threats. Based on the literature, the author identifies the three most used divisions of hybrid threats based on either: (i.) *intensity* of the hybrid activity, (ii.) *type of influence* (e.g., economic, political), and (iii.) use of either *conventional* or *unconventional* methods.

As for the *intensity*, Hybrid CoE (2020) differences between hybrid *influence*, *interference*, and *warfare.* Instruments of hybrid *influence* are defined as "tolerable hostile activities," those of hybrid *interference* as "intolerable hostile activities," and tools of hybrid *warfare* are "activities that trigger a conventional response."

The type of influence division is used by, e.g., Monaghan (2018, p. 86). Monaghan defines three contextual factors that reflect tools of hybrid activities: (i.) political (shifting balance of global and regional power), (ii.) economic (complex interdependence in the global economy creating more vulnerabilities), and (iii.) technological (modern societies are heavily dependent on digital technologies). Monaghan's division is not exhausting as the hybrid toolkit is vast, and several authors broaden these categories. Wigell (2019, p. 5) adds two more types: (iv.) clandestine diplomacy and (v.) disinformation. However, given the nature of disinformation and its spread dependent on the up-to-date technology—especially the Internet—several authors involve disinformation in the bracket of "technological" hybrid

activities. Also, clandestine diplomacy has traditionally been part of the political influence; hence, most authors involve it in the "political" tools.

Division based on *conventional* or *unconventional* methods is grounded in the simple dichotomy of whether the hybrid activity involves military and firepower. Conventional warfare consists of the military. In contrast, the unconventional approach usually utilises unconventional instruments such as fake news, economic pressure, or foreign electoral intervention.

None of these three divisions is perfect and all-embracing. However, a division based on the type of influence can provide the best clarity for the reader—primarily because it is the most specific and divides threats into four different categories.[6]

So, the four categories of hybrid tools are (i.) political, (ii.) economic, (iii.) technological, and (iv.) information. Firstly, as the tools of political influence, several authors (e.g., Chivvis 2017, p. 4; Qureshi 2020, p. 193) define—among other things—election interference, use of diplomacy to support preferred political parties or candidates, funding to think tanks, movements, protests, NGOs, etc., or high-level representatives' visits.

Secondly, economic sanctions, foreign aid, or IMF loans are employed as tools of economic influence (e.g., the United States (US) enjoys a significant impact over IMF loans and has often used economic sanctions to influence foreign politics). Sanctions, foreign aid, or IMF loans can hardly be considered a modern tool of hybrid warfare as they have been employed for decades. Gamechanger is the new global strategic balance shifting from the long US

[6] In the thesis, "clandestine diplomacy" is viewed as a part of "political" means of influence. Hence, only four categories of power will be used—political, economic, technological, information (which could be, however, also part of the technological bracket, but due to its vast importance, it is left as a free-standing category).

domination towards a multipolar economic society with China rising as a financing giant (Qureshi 2020, p. 194).

Thirdly, up-to-date technology catalyses the hybrid influence. Technology serves as a tool of hybrid interference at—at least—two levels: (i.) in the form of emerging and disruptive technologies (EDT); and (ii.) information and communications technology (ICT). They may work separately but also together to conduct unprecedented cyber-attacks and cyber warfare (Thiele and Schmid 2020, p. 3-5). Technological progress has always been the critical driving force behind military strategy. While technologically advanced countries have always had a distinct advantage in combat, they may be more vulnerable to specific attacks (Danyk, Maliarchuk and Briggs 2017, p. 10), especially in the era of EDT[7]. EDT are changing the nature of warfare, and states with the most advanced technologies will possess essential advantages at the strategic and operational levels. Cyber-attacks are rising as the technologies have become an inherent part of the civil and military sectors. Russia has access to the "cyber warriors" to hack into Western information systems to collect valuable information. The information then reinforces other hybrid tools—e.g., political (influence of the election) or economic. The cyber tools may also be used to directly manipulate (or otherwise affect) the ICT systems of other countries (Chivvis 2017, p. 3). Cyberattacks can destroy nuclear facilities, incapacitate radar systems, or hijack a satellite and disable government communications. Also, perpetrators usually do not have to face retribution or attribution (Qureshi 2020, p. 194). In recent years, cyber-attacks

[7] NATO, in its 2020 document *Science & Technology Trends 2020-2040,* defines eight categories of EDTs— Big Data, Artificial Intelligence, Autonomy, Quantum Technologies, Space Technologies, Hypersonics, Biotechnology and Novel Material (NATO 2020, p. 14-26).

perpetrated by Russian crime groups have targeted hospitals, energy grids, or even industrial facilities (Ilbiz and Kaunert 2021).

Fourthly, clandestine diplomacy is a form of covert action that involves fostering counter-elites (Wigell 2019, p. 5), traditional espionage as part of the hybrid methods, bribing and attempting to influence vulnerable political figures, i.e., supporting proxies (Chivvis 2017, p. 4), backing radical or secessionist political parties, nurturing protest movements and otherwise aiming to both weaken support for central government and to create a more polarised political environment (Wigell 2019, p. 5). Nonetheless, as abovementioned, clandestine diplomacy may be viewed as part of the political tools of hybrid influence.

Lastly, the digital revolution meant a significant change in people's lives as it increased connectivity. Changes in the way people communicate led to information warfare and large-scale disinformation campaigns.[8] Russian geopolitical expert Igor Panarin (Darczewska 2014 in Hammond-Errey 2019, p. 2) defines disinformation as "*spreading [of] manipulated or fabricated information (or a combination thereof)*"; Lothar Metzl, former Central Intelligence Agency's (CIA) leading expert on communist ideology and praxis, described disinformation in the 1970s as "*operations aiming at pollution of the opinion-making process in the West*" (1974, p. 921). Disinformation may have several strategic intents—e.g., to manipulate, deter, divide, distract, suggest, or provoke (Hammond-Errey 2019, p. 6). Truth distortion is a crucial component of wedging by disinformation, especially in political matters. By "hijacking" internet news sites and social media feeds with 'fake news and 'alternate'

[8] It is necessary to note that there was little novelty in the idea of disinformation campaigns, propaganda, and the use of information to achieve political goals. However, while information warfare is thousands of years old, modern media technology brings information warfare to a new, unprecedented level.

narratives of events, disinformation disseminator impedes target populations' ability to separate fact from fiction (Wigell 2019, p. 6). Both Norway and the Czech Republic classify hybrid interference from Russia to be the primary threat, especially the information operation and cyber-attacks (Bezpečnostní informační služba 2021, p. 14, and Norwegian Intelligence Service 2021, p. 16)[9].

Tools and instruments of the hybrid influence spectrum are vast, and there is no complete and exhausting list of all the means. The agents are usually combined, and actors are constantly trying to develop new ideas of naturally influencing others.[10] So, given the broad list of the instruments of hybrid interference, the difficulties with the attribution and definition, and the interconnectedness of the tools utilised, this thesis will focus only on a selected threat and relevant countermeasures.

According to the Security Information Service (Bezpečnostní informační služba, BIS) and its *Annual Report for 2020*, the most severe threats for the Czech Republic in 2020 were "cyberattacks of actors linked to foreign powers" and "disinformation activities which could weaken the democratic foundations of the rule of law" (BIS 2021, p. 9). Norway also classifies influence and operations in the cyber domain as one of the biggest threats (NIS 2021, p. 16-17). According to the World Economic Forum and *The Global Risks Report 2021*, cyber-attacks, IT infrastructure breakdown, data fraud or theft, or digital

[9] China is also considered an important actor; however, according to BIS, while China's goal is to build a sinocentristic global community that will respect China, Russia aims to destabilise and defeat its counterplayers. Hence, it poses a more significant threat to the Czech interests (BIS 2019, p. 8-9).

[10] It is impossible to provide the reader with a complete list of hybrid instruments, in the end, it is the nature of the hybrid operations that they are unconventional and very interfered. Several authors for example add other types of influence such as cultural influence, psychological warfare, legal interference, role of religion, drug warfare, forced population shifts, or fabrication warfare.

inequality pose one of the biggest global threats (WEF 2021, p. 14). The cyber domain's operation can erode community trust in science, threaten governability, and tear the social fabric (WEF 2021, p. 53). Hence, given the importance of the threats in the cyber domain, and based on the typology of influence described at the beginning of this subchapter[11], the thesis will mainly focus on the threats within the third presented category—*technological* threats. To simplify the matter and allow for the focus on the instruments of public-private cooperation, the thesis will focus on cyber threats. The reasons behind this are two: (i.) the tools to counter cyber threats, especially those regarding public-private cooperation, are with ease transferable to other dimensions of hybrid threats, and (ii.) the focus only on cyber threats allows for precise and dependable comparison of the Norwegian and Czech approach to the matter of public-private cooperation.

2.3 Countering Hybrid Threats: Concept of Public-Private Cooperation

The previous two chapters outlined the current academic debate on the hybrid threats and the specific tools of hybrid operations. This chapter aims to present the literature review on countermeasures. The chapter will focus on the concept of total defence in terms of hybrid threats, as it permeates the whole Norwegian security strategy. Then, the author attempts to outline the concept of societal resilience and public-private cooperation as a means of achieving it.

Firstly, let us look at the concept of total defence. Unfortunately, the academic research on the Norwegian total defence concept is not extensive, especially regarding hybrid threats. In his article, Wither (2020) discusses the

[11] Four categories of hybrid influence include (i.) political tools, (ii.) economic, (iii.) technological, and (iv.) disinformation.

total defence policies of all three Nordic states, Norway, Sweden, and Finland. However, Wither does not outline concrete instruments; he solely compares three models and answers the questions of whether they would be successful against external aggression (Wither 2020, p. 75). Generally, total defence is defined as the "*sum of all the civilian and military resources put to use for crisis management and in the event of aggression*." The system's core relies on the mutual support and cooperation between the armed forces and the civil sector. According to Szymanski (2020, p. 15), Norway is focusing on increasing crisis response readiness, involvement of the civil society and armed forces support for public authorities, the police, and the population.

Secondly, let us investigate the concept of societal resilience. When considering total defence and hybrid threats, the point of entry should be the recognition that the critical tasks that must be accomplished to defend against hybrid threats are beyond any single actor's capability and operational capacities. Hence, the cooperation of all parts of society (governments, private companies, non-governmental organisations, media, and individuals) is essential to achieve any success in countering hybrid interference. Hence, the ultimate countermeasure shall be enhancing cooperation across society—a crucial aspect of the total defence concept.

While several academic articles focus on the countermeasures to hybrid threats, almost none of them work with the concept of total defence. Several authors, though, highlight the importance of building societal resilience. Lauren Speranza, Director of Transatlantic Defense and Security at the Center for European Policy Analysis, recommends the creation of a new platform for cooperation between NATO, the EU, member states, and the private sector (2020, p. 14). The organisation would be based on the voluntary approach and served as a flexible forum that hinders collective progress in countering hybrid

threats. Speranza also proposes investments in civic education, media training, and civil preparedness. This effort should be inspired by Nordic and Baltic countries, especially their efforts including conducting national defence courses, issuing civil-defence brochures on handling hybrid interference, or developing civilian authorities that receive military training to detect and respond to hybrid activities (Speranza, p. 16).

Despite its importance, the concept of "societal resilience" is a similarly tough nut to crack as "hybrid warfare." Jiří Šedivý, former Czech Minister of Defence and current CEO of the European Defence Agency (EDA), divides the concept of 'resilience' into three domains: i.) *technical-organizational*, ii.) *environmental*, and iii.) *societal* (Šedivý 2018, p. 3). Norwegian scholar Christer Pursiainen introduced a similar three-layer division. However, Pursiainen differs between i.) *technological*, ii.) *organisational,* and iii.) *societal* domains of resilience. Based on his division, technological resilience includes CI and the respective facility operators. An organisational resilience involves the actors are businesses, especially those responsible for CI and supply chains. Lastly, societal resilience involves important actors such as national and local governments, communities, and households. CI resilience often overlaps with everyday civil protection. (Pursiainen 2018, p. 41).

Hanisch (2016, p. 3) defines three different features of resilience: i.) *coping capacities* (meaning overcoming disruptions reactively, rapidly, and flexibly), ii.) *adaptive capacities* (proactive and long-term adaptation of structures, processes, or modes of behaviour) and iii.) *transformative capacities* (societies do not adapt gradually but undergo radical change). This three-dimensional approach is shared among several scholars and organisations (e.g., Keck and Sakdapolrak 2013; Guerrero 2020; United Nations 2021; Oxfam 2017). According to Haavik, societal resilience is the "fourth age of safety." It was

established as an expansion of "societal safety" as resilience emphasises a local and decentralised responsibility for societal safety and security (Haavik, 2020, p. 2). In the early attempts in Norway to define societal safety, Olsen et al. (2007) operationalised societal safety to address critical infrastructures and critical societal institutions. Hence, social safety is "*the ability to maintain critical social functions, protect the life and health of citizens, and meet the citizens' basic requirements in a variety of stress situations*" (Olsen et al., 2007).

Pursiainen came up with a similar shift in 2018 (p. 632), as he describes the change in emphasis from critical infrastructure protection to that of resilience in Nordic countries. The author identifies the "Nordic model" of CI resilience as Norway, Sweden, Finland, and Denmark had "*based their policies on securing vital societal functions rather than the individual infrastructures that support these functions*." (Pursiainen 2018, p. 634). According to Haavik, societal resilience must build knowledge and methods for producing resilience through the networks where global risks are shaped—which implies a turn from robust infrastructures to the shaping of resilient societies through sustainable livelihood-, scientific- and political practices (Haavik 2020, p. 7). According to Braw (2021, p. 7), to be effective, resilience requires cooperation between government and private sector. However, societal resilience must involve all parts of society. Until recently, governments were reluctant to involve the population in resilience and instead adopted a whole-of-government approach to national crises (Braw 2021, p. 11). Hence, when embracing the whole-of-society approach, individuals, businesses, and organisations all play a part in building resilience.

Within the Czech academia, several scholars also focus on resilience to counter hybrid interference. In 2021, Bahenský and Ditrych proposed the "Netherlandic model" as an inspiration for the Czech model that should be

adopted as a follow-up to the Strategy's release. According to a policy paper by Bahenský and Ditrych (2021, p. 7), state institutions should cooperate more, meet frequently, and involve *secondment*—the interchange of the personnel within the ministries. Authors then propose joint exercises and deepening the cooperation between executive power and academia. Thus, creating a network of experts may contribute to the effectiveness of the future Czech model of countering hybrid threats.

Havlík (2020) describes the formation and integration of cyber forces and information operations into the Army of the Czech Republic structure. Havlík's main argument reflects the transition from the classical form of warfare to the new platform, represented mainly by cyberspace and hybrid operations. To ensure the operational capability and readiness of the Army of the Czech Republic, it is "*necessary to work on the protection of critical infrastructure and develop defensive and protective mechanisms and processes*" (Havlík 2020). Furthermore, in 2018, Daniel and Eberle mapped the 'Russian hybrid warfare' assemblage, a constellation of public and private actors that redefined the understanding of national security in the Czech Republic. In their article, the authors showed that the Czech security transformation was "rather messy" and that the emergence of Russian hybrid warfare as a prime security issue "was much less direct than it seems." While the authors do not focus directly on the policy recommendations for the Czech security strategy, they analyse how exactly the security strategy changed after Russia attacked Ukraine in 2014. They identify key actors informing the debate on security strategy (Daniel and Eberle 2018, p. 918-925). The authors have also identified several avenues for further investigation in their research, which leaves generous space for future papers, including this thesis' attempts.

So, considering everything, what is the integral approach when facing hybrid threats in the countries examined in the thesis? There has already been a significant shift in Norway towards resilience (e.g., Pursiainen 2018) instead of protecting critical infrastructure. Yet, critical infrastructure protection still prevails in the Czech Republic. So, the thesis aims to focus on building *societal resilience* as a practical response to hybrid threats—based on the Norway case study. When making a nation's resilience, the instrument of public-private cooperation is understood as one of the most effective means among scholars and international organisations (e.g., Brown et al. 2021; Smith 2016; World Bank 2017). The concept is further elaborated below.

Public-private cooperation (PPC)[12] as a means of resilience is a general idea of the last several decades. Nevertheless, cooperation between private actors, corporations and governments has existed since the inception of sovereign states, notably for tax collection. Although there have been attempts to define the concept, a formal definition is still missing. According to Carr, the politicians are reluctant to claim authority for the state to introduce stricter cyber-security measures by law, coupled with the private sector's aversion to accepting responsibility or liability for national security. So, the 'cooperation' or 'partnership' is left without clear lines of responsibility or accountability (Carr 2016, p. 43).

Some of the traditional definitions of public-private cooperation are "*a long-term contract between a private party and a government entity, for providing a public asset or service, in which the private party bears significant risk and management responsibility, and remuneration is linked to performance*" (World Bank 2014, p. 14), meaning that private party delivers and funds public

[12] Some scholars use the term public-private partnerships or PPP.

services using a capital asset (OECD 2012). However, in the thesis, PPC is understood differently. The principal goal of enhanced resilience is to protect critical infrastructure responsible for providing basic services to society. Without these essential services, vital society functions are endangered. The public sector oversees ensuring the well-being of society while critical infrastructures are usually wholly or partly in the hands of privatised or semi-privatized companies (Boin and McConnell 2007, p. 53). Hence, both public and private companies are responsible for providing resources and sharing responsibilities to protect critical infrastructure. To ensure a decent level of protection, a significant effort to promote cooperation between parties through PPC is required, though, primarily to bolster coordination and information sharing across the government-business divide (Busch and Givens 2012, p. 46-47). Having established the background to the concept of public-private cooperation, it is necessary to clarify what is meant by the term. Unsurprisingly, there is a wide range of diverse arrangements referred to as public-private cooperation. In this thesis, PPC is understood by Linder's definition of six distinctive uses of the term 'public-private partnership' linked to neo-liberal or neo-conservative ideological perspectives. One helpful type that sheds light on what is meant by public-private cooperation is *partnerships as power-sharing*. According to Linder, this type of PPC is based on cooperation where "*trust replaces the adversarial relations endemic to command-and-control regulation*" and "*where there is mutually beneficial sharing of responsibility, knowledge or risk*" (Linder 1999, p. 42-43).

2.4 Theoretical Framework

This subchapter aims to present the theoretical framework that will be used to analyse the Norwegian approach to countering hybrid threats (i.e., cyber

threats). The analysis of the Norwegian approach is based on the "three pillars of societal resilience" brought by several scholars (e.g., Fägersten in Hamilton 2016, p. 113-121; Wither 2020, p. 63-75; Flanagan et al. 2020, p. 25), NATO (*Enhancing the Resilience of Allied Societies Through Civil Preparedness* 2021, p. 7-10), EU (*Joint Framework on countering hybrid threats* 2016, p. 18), Norwegian government (*Long Term Defence Plan 2020*, p. 4-6, 16; *Support and Cooperation: A description of the total defence in Norway* 2018) or the Czech government (*National Strategy for Countering Hybrid Interference* 2021, p. 8). According to the "three-pillar approach", the societal resilience towards hybrid threats is built primarily on three pillars: (i.) awareness, (ii.) resilience, and (iii.) partnerships. As for awareness, it is crucial to increase knowledge and understanding of the tools and tactics, build situational awareness and ensure cross-sectoral communication between private businesses, organisations, and local actors. As for resilience, state authorities should work together to counter foreign interference. All the parts of society should aim to protect essential national functions and private businesses from digital attacks and protect the nation from hybrid threats. As the hybrid interference also crosses national borders, the third pillar is partnerships—both international and domestic. International partnerships provide an overarching structure for defence cooperation and allow for information sharing, exchange of personnel, know-how and experience. By cooperating both bilaterally and multilaterally inside the international organisations (e.g., NATO, Hybrid CoE, OSCE, or ITU), the countries become more resilient in terms of hybrid threats. They can respond more effectively as they may share the practice or ask for support.

The three-pillar model of countering hybrid threats is accompanied by the theory brought by Torgeir K. Haavik in 2020. Haavik's approach to societal resilience goes beyond addressing resilience at the scale of individuals and

organisations. According to Haavik, with its root metaphors derived from ecological systems, resilience should also be addressed at the societal or international scale. Hence, Haavik challenges the current dominating scopes and argues that societal resilience should go beyond critical infrastructures and the national and inter-organisational scope. Haavik focuses on the societal context of safety instead of the traditional approach that praises critical infrastructure. Expanding the discourse on societal safety and security that reaches out to a broader public audience addresses trends with significance not only for resilient critical infrastructures but also for socio-political resilience (Haavik 2020, p. 2). So, while the focus on critical infrastructures puts weight on protection and is inherently reactive, focusing on societal resilience allows addressing the processes where political decisions that influence global risks are made (Haavik 2020, p. 4).

Haavik's logic behind the theoretical shift in societal resilience is simple—those who control a society's critical infrastructure control the society. He illustrates the shift in the ICT case, which is often labelled "the infrastructure of infrastructures" (Almklov et al., 2018), as most other infrastructure critically depends on it. Hence, the ICT sector is interesting as most of it is owned, administered, and operated by the private sector. At the same time, governments are legally responsible for safeguarding critical infrastructure depending on the ICT. This setup also makes ICT an interesting case study for public-private cooperation as an instrument to counter hybrid threats.

The three-pillar division is significant for the chapter summarising the results (chapter 5). The three-pillar approach serves as a tool for analysing the Norwegian and Czech instruments of public-private cooperation to provide the reader with clarity. So, this three-pillar model aims to divide instruments

according to their end goals, which may ease the potential utilisation of the tools introduced into practice.

3 The Czech Republic: Current State of Affairs

This chapter aims to shed light on the current situation in the Czech Republic regarding public-private cooperation in terms of countering hybrid threats. Firstly, the chapter outlines Czech strategy and tool currently utilised. The chapter is concluded with conclusions and "gaps identified" in the Czech approach to the instruments of public-private cooperation.

On the one hand, the Czech Republic successfully established several public institutions that proved helpful in facing cyber threats, e.g., NÚKIB or CTHH. On the other hand, these institutions suffer from a lack of finances and personnel. They are difficult to approach from the outside, their communication is insufficient, and they lack effective measures to deepen public-private cooperation. These systemic and procedural deficiencies are further elaborated in the five subchapters below. In addition, besides the procedural issues, the Czech strategy of countering hybrid threats suffers from the lack of trust between the state, private sector, and citizens.

All in all, in the Czech Republic, there are barely any examples of functioning public-private cooperation. Nevertheless, most of these issues may be resolved by relatively simple solutions based on improving the already existing mechanisms. These solutions are introduced in the last chapter, 'Results', in a form of policy recommendations. They are based on the current situation in the Czech Republic (subchapter 3.2, p. 60) and the 'lessons learned' from Norway (chapter 4.2. p. 89).

3.1 Cybersecurity in the Czech Republic: Strategy

The Czech Republic possesses several well-written laws (e.g., the *Crisis Act* or the *Act on Cyber Security*), operates the National Cyber and Information Security Agency (NÚKIB), which is a respectable central administrative body for cyber security, and opened one of the first centres focusing on countering disinformation and foreign propaganda—Centre Against Terrorism and Hybrid Threats (CTHH).[13] However, in terms of public-private cooperation, lack of trust and engagement (especially on the side of the private companies and citizens) prevails. The Czech National Security Authority (NBÚ) itself states that the Czech state and its security apparatus experience low confidence from the public (NBÚ 2015, p. 12). According to the *National Cyber Security Strategy 2015-2020*, the Czech state is constantly building and increasing national capacities in the area of cybersecurity. Still, without cooperation with the private sector and academia, without intensive international cooperation and especially without the involvement of the population itself, the necessary effectiveness will be missing (NBÚ 2015, p. 6). So, even the NBÚ and NCKB (National Centre for Cyber Security, the institution that preceded NÚKIB) admit that without the trust and voluntary cooperation of the Czech citizens and the private sector with the cyber security entities, the whole concept of cyber security is irrelevant (NBÚ 2015, p. 19). This is also enhanced by the branched bureaucracy of the public authorities that seem inaccessible for private companies and individuals. For instance, when companies try to contact public bodies, they do not possess direct contact on the point of contact (POC) within the public institutions. Hence, the

[13] Czech Centre Against Terrorism and Hybrid Threats was active even before the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki. CTHH has been operational since January 2017; Hybrid CoE was opened in April 2017.

communication is not without difficulties (private company representative #4, personal communication, 7 April 2022, and MO representative, personal communication, 11 April 2022).

Currently, the Czech Republic possesses several instruments to counter hybrid threats. There is no research on assessing and analysing their efficiency, though. This is probably given by the relative novelty of the matter of hybrid threats in the Czech security environment. Just in 2021, the Government adopted the *National Strategy for Countering Hybrid Interference* (hereinafter as Hybrid Strategy) that defines instruments essential for the protection of vital, strategic and other critical interests in the Czech Republic against hostile hybrid interference (Ministry of Defence 2021a, p. 3). It complements the already existing system of security policy documents (e.g., the *Security Strategy of the Czech Republic*) by formulating a comprehensive national policy to counter hybrid interference (Ministry of Defence 2015). The Hybrid Strategy, among other things, focuses on the weakening of the political and international legal commitments in the area of security as some countries pursue their power-seeking goals through hybrid warfare methods (e.g., propaganda using traditional and new media, disinformation intelligence operations, cyber-attacks, political and economic pressures, etc.) (Ministry of Defence 2021, p. 13). In the Hybrid Strategy, the government pinpointed three strategic objectives: i.) resilient society, resilient state, resilient critical infrastructure, ii.) holistic approach, and iii.) capability of adequate and timely reaction. These goals are in line, e.g., with the objectives defined by General Philip M. Breedlove, former Supreme Allied Commander Europe of NATO Allied Command Operations, who in 2015 pointed out that resilience, readiness, and quick decision-making are fundamental to NATO's success (Breedlove in Lasconjarias and Larsen, eds., 2015). The strategic objectives are

to be fulfilled through the *Action Plan for National Strategy for Countering Hybrid Interference.* The Action Plan identifies 15 tasks to be accomplished in 2021-2025, but it does not specify how to complete them (Ministry of Defence 2021b, p. 5-6).

3.1.1 National Cyber and Information Security Agency

In terms of cybersecurity in the Czech Republic, the most significant shift came in 2017 when the National Cyber and Information Security Agency (NÚKIB) was established based on Act No. 205/2017 Coll., Amending Act No. 181/2014 Coll.[14], on cybersecurity and amendments to related acts (the so-called *Cyber Security Act*). In the Czech Republic, the Agency is the central administrative body for cyber security (NÚKIB 2021a). Before NÚKIB was founded, responsibility for cybersecurity did hold National Security Authority (NBÚ) (NÚKIB 2021a).

Based on the Cyber Security Act, private companies under this law (i.e., they are part of the CI or CII) are obliged to set up a "cybersecurity manager". A cybersecurity manager is responsible for information security management and serves as a kind of intermediate step between top management (strategic management level) and the operational level. So, the cybersecurity manager is responsible for information sharing inside of the company (NÚKIB 2020c, p. 5). Nevertheless, the cybersecurity manager does not serve as a POC for NÚKIB and other public authorities.

[14] Act No. 181/2014 Coll. is historically the first Czech complex law on cyber security. It prescribes specific methods and measures to the concrete public and private bodies to ensure the safety of their cyber infrastructure. Besides that, it recognises NÚKIB as the governing body for securing cyber security in the Czech Republic.

Czech cybersecurity strategy is guided by the "*National Cyber Security Strategy of the Czech Republic*" issued every five years by NÚKIB (and NCKB before NÚKIB was established). The first Cyber Security Strategy was published in 2011, the last one in 2021. These strategies are accompanied by the "Action Plans" that involve steps and measures to be implemented. For the thesis, the most relevant is the *2015-2020 National Cyber Security Strategy*—it is pretty recent on and already allows for the evaluation. While NÚKIB "managed to fulfil most of the tasks of the Action Plan 2015-2020", it was largely unsuccessful in fulfilling the tasks regarding public-private cooperation (NKÚ 2020, p. 8). For example, NÚKIB did not manage to create a platform for sharing information on cyber security threats and incidents (task C.5.02 of the *2015 Action Plan*) (NBÚ 2015b, p. 13) that would increase the trust between the public and private sector (NBÚ 2015a, p. 19). Judging from the NÚKIB's priorities in 2015-2020, the Czech state is undoubtedly aware of the necessity of public-private cooperation to enforce cybersecurity. Yet, it did not manage to establish working instruments of public-private cooperation, e.g., the platform for information-sharing that could be a beneficial improvement.

According to the *2021-2025 Cyber Security Strategy*, the vision of the Czech Republic is composed of three pillars: (i.) confidence in cyberspace, (ii.) strong and reliable partnerships, and (iii.) resilient society 4.0 (NÚKIB 2020a, p. 21). In terms of societal resilience, some of the strategic end-goals are "cooperation between the state, private sector and citizens" or the "creation of a base of the experts" (NÚKIB 2020, p. 21). This vision is reflected and concretised in the *2021-2025 Action Plan.*

The current Action Plan covers 15 tasks to be accomplished by 2025. In terms of public-private cooperation, the first task is to "create and manage a

national secured platform for communication and exchange of information" (NÚKIB 2021b, p. 3) which seems to be a follow-up of the unaccomplished task from the previous Action Plan 2015-2020. However, this time, the task does not specify *who* should be involved in the platform.[15] In terms of "confidence", one of the goals is also improved strategic communication. NÚKIB sets a goal to "carry out communication campaigns to support national goals in the area of cyber security" and to "create a methodology for strategic communication of the relevant actors on the national level in a case of cyber-attack and other threats" (NÚKIB 2021b, p. 4).

The Action Plan 2021-2025 mentions the private sector in six places (p. 4, 6, 9, 10, 13 and 16). However, only two tasks call for closer cooperation between the state and private companies.

3.1.2 Integrated Rescue System

In the 'technical-organizational' or 'technological' domain of resilience as defined by Pursiainen (2018, p. 41)[16] or Šedivý (2018, p. 3), the basic framework for resilience in the Czech Republic is represented by the Integrated Rescue System (IZS). The IZS is in the gesture of the Ministry of Interior, and within the EU and NATO, it is considered to be one of the best-working and most effective systems. The Finnish model of crisis preparedness inspired it, and during several past crises, it proved itself to be a well-working system. For times of crisis, IZS have ready "*Standard Operating Procedure of IZS Units During Joint Intervention*" (so-called standard operating procedure, or "*typová*

[15] In Action Plan 2020-2015, the private sector was explicitly mentioned to be the subject of the measure (p. 13).

[16] Based on Pursiainen's division, technological resilience includes CI and the respective facility operators. An organisational resilience involves the actors are businesses, especially those responsible for CI and supply chains.

činnost") that includes the "procedures of the IZS units during rescue and liquidation works regarding the type and nature of the emergency" (IZS 2022). The standard operating procedure defines which segments of IZS and what, and they count with 17 scenarios, including a dirty bomb threat, chemical attack, or active shooter.

Besides the standard operating procedures, there are also so-called model action plans, or "*typové plány*". In accordance with Government Decree No. 462/2000 Coll., a model action plan is a document by which the relevant ministry or other central administrative authority determines the recommended type of procedures and measures for resolving a specific type of crisis. The model action plans are developed for dealing with specific types of imminent crisis situations identified in *Threat Analysis for the Czech Republic*. This analysis identifies 22 potential crisis scenarios including the drought, floods, migration waves, terrorism, and "breach of security of critical information infrastructure" (IZS 2017). Similarly, the model action plans are written in a difficult, unapproachable language—the same as the standard operating procedures. In terms of the "Breach of Security of Critical Infrastructure" model action plan, it is a very generic document that does not specify any concrete scenario, and largely refers to the so-called Crisis Act (Act N. 240/2000 Coll. on Crisis Management; further elaborated below in this subchapter). The private sector is mentioned exactly in one place, stating that the "communication and information infrastructure is in the hands of the private sector, that also has the capacity to effectively solve most types of cyber security incidents" and that the entities with which is "necessary or appropriate to cooperate" are to be determined according to the nature of the

cyber-incident (NBÚ 2019, p. 8). According to the NBÚ[17], critical information infrastructure is largely linked to already identified critical infrastructure elements identified in the areas of energy, public administration, electronic communications and the financial market and currency. Hence, breaches of information security are similar in terms of the solution process: they are usually dealt with by the affected entity, NÚKIB and other institutions at the central level of the state (NBÚ 2019, p. 1). Henceforth, NBÚ refers to other "relevant model action plans" prepared by other responsible authorities. So, through the prism of the NBÚ and IZS, if there is a cyber-attack leading to the disruption of oil and oil product supplies, it does not matter that the initial cause of the crisis was a cyberattack. The outcomes are the very same in a situation where the primary cause is either a technical issue, blackout, or cyberattack—disruption of the oil and oil product supplies. This is not necessarily bad. Though, the lack of a proper cyberattack scenario led to much worse handling of the 2019-2020 cyberattacks on the Czech hospitals (MV representative, personal communication, 14 April 2022, and Benešov Hospital representative, personal communication, and 30 April 2022).

According to the MV representative, whole crisis management is "largely vertical organised, fragmented and difficult to grasp for the public". Based on the *Threat Analysis for the Czech Republic* issued by the Czech Ministry of Interior (the most recent one was published in 2015), the subordinate units, in this case, Regional Councils[18] prepare the crisis scenarios upon their specific situation financial and personnel capacities (MV representative, personal communication, 14 April 2022). However, for a citizen/private company, it is

[17] National Security Authority (NBÚ) is an authority responsible for recommending procedures and measures to solve this specific type of crisis.

[18] The Regional Council is the executive body of the Region within the area of independent authority.

difficult to get information about the scenarios (not all of them are public, yet there is no key to assess which are confident), and the Czech state is particularly non-transparent in providing information on its crisis management, preparedness, or exercises. Furthermore, the role of the citizens is completely omitted in the scenarios.

Besides the standard operating procedures, the Czech legal system also has several crisis management instruments. The most important one is Act N. 240/2000 Coll. on Crisis Management or the so-called "Crisis Act."[19] For the first time, the Crisis Act was applied on a larger scale when dealing with emergencies that arose in connection with the 1999 floods. For the second time, Crisis Act was used on a larger scale during the 2020-2021 coronavirus pandemic. The Act regulates the competencies and authority of state bodies, and it can limit the rights and freedoms of citizens guaranteed by the Charter of Fundamental Rights and Freedoms. So, it is an essential instrument for a crisis management that proved valuable and working. Nonetheless, it does not specify any instrument of public-private cooperation during a crisis and to a large extent omits any role of private businesses and citizens.

3.1.3 Center Against Terrorism and Hybrid Threats

The Czech Republic was among the first countries to launch a domestic effort to counter cyber-attacks, disinformation, and other hybrid threats by opening the Center Against Terrorism and Hybrid Threats (CTHH) within the Ministry

[19] "*Act specifies domain and jurisdiction of state authorities and of authorities of territorial self-governing units and rights and obligations of legal and natural entities during preparedness for crises, which are not related to the provision of defence of the Czech Republic against an external attack and during their solution and protection of critical infrastructure and responsibility for the breach of these obligations*." (Chapter 1, paragraph 1, Act N. 240/2000 Coll.).

of Interior in January 2017. The establishment of the CTHH is a direct consequence of the National Security Audit launched by the government in 2016. In the Audit, three specific chapters deal with this issue— *Influence of Foreign Powers*; *Hybrid Threats and Their Impact* and *Cyberthreats*. Overall, the issue of cybersecurity is broadly discussed throughout the Audit. The Audit considers cyberthreats to be one of the most severe threats to state authority, business corporations, and society (Ministry of Interior 2016, p. 96). Besides showing that Czech governmental bodies consider hybrid threats and cybercrimes serious risks, the report also indicates that at the time, cyberthreats were perceived as part of hybrid warfare. One of the most important outcomes of the audit was the establishment of CTHH, which followed the recommendation in the document to "*establish departments within relevant Government institutions for the evaluation of disinformation campaigns and other manifestations of foreign power influence*" (Ministry of Interior 2018, p. 61).

According to the Ministry of Interior, CTHH is a specialised analytical and communications unit that monitors threats directly related to internal security, e.g., terrorism, extremism, public gatherings, violation of public order, and different crimes such as disinformation campaigns. The CTHH evaluates detected challenges and proposes substantive and legislative solutions (Ministry of Interior 2021). In his article, Robbins describes the Czech Republic as "one of Europe's leaders in combatting Russian disinformation." He praises the Czech multifaceted strategy to respond to the hybrid threats—especially the work of CTHH, which is enhanced by the Czech Security Information Service (*Bezpečnostní informační služba*, or BIS), civil society group mobilisation, and research from think tanks (Robbins 2020). Yet, there is always room for improvement. The activities of the CTHH are insufficiently funded, and the CTHH does not get the public attention it deserves—which is given primarily

by the unsatisfactory communication with the public (MV representative, personal communication, 14 April 2022).

3.1.4 Cyber Security Exercises

The Czech Republic is also pioneering new forms of societal resilience. In 2021 the Czech government introduced joint military-industry grey-zone exercises under the auspices of the Ministry of Defence, NÚKIB, MPO and CTHH. The exercise is purely defensive and involves armed forces and invited representatives from the private sector. These exercises allow the government and private sector to train together to better handle forms of grey-zone aggression (Braw 2021, p. 11), set up new channels of communication, and build mutual trust.

The exercise was prepared to deepen "systematic cooperation between the state and strategic private companies". The purpose of these exercises is "cooperation between the state and top-management of the strategic companies to enhance the resilience of the Czech society". The exercises should be a part of a "three-level platform" consisting of (i.) information sharing, (ii.) educational workshops and (iii.) simulation of an attack. According to the Ministry of Defence, the exercise aims to find out whether the private companies have contingency plans for such a situation and to test them, train the ability of the company to communicate effectively with the public and the state, improve public-private cooperation and to enforce joint information sharing (Zachmeisterová and Táborský 2021).

Furthermore, NÚKIB is also organising cyber exercises. They aim to improve resilience toward cyber threats. The exercises are both sectoral (e.g., Electro Czech and Health Czech) and cross-sectoral. One of them is "Cyber Czech", a national technical exercise aimed at practising the practical skills in

defending the assigned network against cyber-attacks. The exercise is based on a prepared scenario that reflects real cyber threats and puts them in a fictitious geopolitical context (NÚKIB 2022). According to the NÚKIB representative, the exercises are popular among private companies. They voluntarily approach NÚKIB with the requests to participate in the exercises. Throughout the several last years, NÚKIB annually organised from 8 to 14 exercises. The number of exercises carried out is predominantly limited by the finances and personnel at NÚKIB. In future, NÚKIB's vision is to focus on the consultations and build the train-the-trainer concept (NÚKIB representative, personal communication, 3 May 2022). In this approach experts within the private companies are given training and then deliver that same training to their employees, so the skills and information are shared and learned by the relevant workers throughout the company.

3.1.5 National Cyber Security Month

The Czech Republic is part of the European Cyber Security Month (ECSM), the EU's annual campaign dedicated to promoting cyber security among citizens and organisations, aiming to provide up-to-date digital security information through awareness-raising and sharing good practices. As in other countries, ECSM takes place in October every year. Several events occur under the Ministry of Interior and NÚKIB, usually only for a week instead of a month, though.

In 2021, NÚKIB prepared campaigns aimed at the children and their approach to cybersecurity. Nonetheless, there were no other public events aimed at the private sector and no discussions or workshops bringing together representatives from the various sectors.

3.2 Chapter Conclusions: Gaps Identified

The five previous subchapters introduced the Czech approach to cyber-security and outlined the Czech attempts to build resilience through public-private cooperation. This subchapter aims to identify the gaps in the Czech strategy. It drafts from the abovementioned review of the tools utilised in the Czech Republic (chapter 3.1). So, based on the open-source analysis and the data obtained during the interviews with the Czech stakeholders, this chapter attempts to shed light on what could be done better.

To begin with, it must be said that Czech cybersecurity is well-developed. Nonetheless, there is always room for improvement. Firstly, let us dig a bit into the functioning of the NÚKIB. It is an organisation respected both in the Czech Republic and abroad. According to NKÚ, it is successful in fulfilling its tasks as it accomplished most of the objectives defined in the *2015-2020 Action Plan* (NKÚ 2020, p. 3). So, what are the gaps? This institution, established in 2017, somewhat usurped the monopoly on cyber security. That is not necessarily bad but brings enormous responsibility alongside. Four problematic issues could—when solved—quite easily contribute to improving the resilience of Czech society. They are (i.) information-sharing and transparency, (ii.) lack of experts in the public space and (iii.) external communication, (iv.) lack of specialised personnel capacities.

So, the first of the shortcomings is information-sharing and transparency. NÚKIB does not publish any information on the cyber-attacks in the Czech Republic. The reason is simple. If it did so, it would lose the trust of the private companies that otherwise reach out for assistance. The private company representative #4 (the company is part of the critical infrastructure in transportation) did agree. According to the representative, it is difficult to be

transparent about the cyber-attacks in the Czech Republic. Even the company represented does not report less severe incidents because of the trust, only discuss them in person on the right occasions. The situation is also tricky as the companies fear the penalty in the form of a fine.

On the other hand, according to the representative, there must be a "scarecrow" as, without it, the companies would not have a serious incentive to comply with the NÚKIB's regulations (private company representative #4, personal communication, 7 April 2022). The only exemption was a 2019 ransomware attack on the Benešov hospital. The cyberattack stopped the working of the hospital, it took almost a month to resume its operability, and the damage was 40-50 million Czech crowns (NÚKIB 2019, p. 18). This concrete case was one of the very little NÚKIB did inform the public. NÚKIB's and private businesses' approach to cybersecurity is rational. Nevertheless, as the Norwegian example later shows, openness and transparency about the attack may be the way to enhance the resilience of the nation towards cyber threats (see more in chapter 4.1.7 on the case of Norsk Hydro).

The second issue that concerns NÚKIB is that in the Czech Republic, there is a lack of independent cyber security experts that would have the trust of the public (private sector representative #3, personal communication, 25 March 2022). The NÚKIB should be able to provide the public with cyber-security experts that can address the issues understandably and calmly. These experts could also pay visits to the schools, give lectures, etc. According to private company representative #4, the lack of experts also affects the state's authority. As the government does not "show off" any high-quality experts within the field of cyber-security, for the companies, it is difficult to trust the state (private company representative #4, personal communication, 7 April 2022). Hence, by exposing NÚKIB's experts to the public, the state could enhance its authority

and create a new image of a professional, capable partner with the proper expertise. However, this is not happening. To provide further evidence, the Norwegian example later shows how vital these independent experts are to build trust (especially in chapters 4.1.3 and 4.1.6).

The third deficiency is NÚKIB's communication. According to several private companies' representatives, it is not among the best. On the outside, NÚKIB does not seem "user-friendly" (private company representatives #3 and #4, personal communication, 25 March 2022 and 7 April 2022). The communication is high-level and contains essential information without any doubt, but it tends to be "boring and tedious" (private company representative #3, personal communication, 25 March 2022). If NÚKIB seems unapproachable from the outside, it is difficult to inspire confidence and build trust between the public and private sectors. Lastly, according to the National Security Audit, one of the NÚKIB's tasks in the 2015-2020 Action Plan was to create a platform for sharing information that will converge information and knowledge so it will be able to identify a potential hybrid campaign. According to the Audit, it was not necessary to establish a new institution, just to create a specific capacity of people with the required expertise within existing institutions. (Ministry of Interior 2018, p. 138). None of this happened, and this task was incorporated into the 2020-2025 Action Plan. According to private company representative #4, such a platform would be handy and could seriously improve the state's resilience toward cyber/hybrid threats (personal communication, 7 April 2022).

Lastly, the ability of NÚKIB to fulfil cyber security key activities heavily depends on professional and highly specialized personnel capacities. Yet the provision and maintenance of the professionals remain problematic for the public authorities in the long run. Between the years 2015 and 2020, the

turnover of the personnel capacities went up to 10 % (NKÚ 2020, p. 4-5). If NÚKIB as a highly specialised agency of the Czech public administration cannot attract and retain the professional staff, any of the three above mentioned deficiencies can hardly be remedied. However, according to the NÚKIB representative, the lack of highly qualified personnel is problematic not only for NÚKIB but also for private businesses. Also, NÚKIB emphasises the quality, not the quantity of the employees (NÚKIB representative, personal communication, 3 May 2022). Hence, the staff is limited in size but able to deliver great performances.

Secondly, let us discuss IZS and its functioning. Integrated Rescue System is working rather well in the Czech Republic. The Czech Republic has several well-written laws that make crisis management easier. Firefighters (representing one part of the IZS) are the most trusted occupation in Czech society. Also, IZS have ready standard operating procedures that assign the responsibilities and improve preparedness and readiness in times of crisis. Yet, there is vast room for improvement. The 17 scenarios do not include several important events, e.g., large cyber security attacks, nuclear accidents, or supply failures. The second issue is that the standard operating procedure only includes state actors (e.g., members of the IZS, Ministeries, governmental agencies), but not the *other* parts of the society who play a crucial role during a large-scale crisis—private businesses, citizens, and others (NGOs, etc.). Moreover, the scenarios are very analytical and not intended for the public. So, if the citizens want to learn what to do in times of crisis, they are only provided with the standard operating procedure written in a difficult, expert language. Lastly, the standard operating procedures are outdated. They do not consider newly established institutions, including NÚKIB, and they reflect

neither new legislation nor the changes within ministries' administrations (e.g., creation and disappearance of new positions, departments, and unions).

Thirdly, let us look more into the National Cyber Security Exercises. According to the NÚKIB representative, this initiative is working well and NÚKIB is organising several cyber exercises for the critical infrastructure companies. It also brings together companies across the sectors to train together—as they probably would have to during a real-life crisis. However, no overarching body oversees the exercises and monitors the companies involved, only NÚKIB. So, while the Ministry of Defence organises exercises for the defence industry companies, other ministries may organise their own exercises that are not centrally organised, managed or evaluated. Nonetheless, this is more a problem of the Czech public authorities and their internal cooperation, than the cooperation between public and private sectors. According to the MV representative, the exercises are not very popular. It is difficult to organise them, they are financially demanding and require a proactive approach from the other ministries that lack. According to the MV representative, there are two significant concerns: first, the finances to organise the exercise itself, and second, the finances to close the gaps found during the exercises. Hence, the prevention is not widespread as it is financially demanding and requires cooperation across the ministries and sectors. What could help is an incentive from the level of the prime minister—if the prime minister and the government decide that exercises (and improved public-private cooperation) are crucial to enhance societal resilience, the organisation of the exercises would be smoother (MV representative, personal communication, 14 April 2022).

Lastly, Cyber Security Month. In other European countries—and Norway, especially— ECSM is a popular whole-of-society instrument. In the Czech

Republic, it is not even a month, but a "National Security Week". Some of the activities organised in 2021 by NÚKIB include online educational comic books and online educational courses for children (NÚKIB 2021c). The author could not find any conference, discussion or in-real event organised on ECSM. Also, there is no accessible information on how the digital courses were utilised, how successful they were, or even how many kindergartens/schools use them. None of the private company representatives was aware of the existence of this "week". However, they found it very interesting and would personally like to participate in the events (private company representatives #4 and #5, personal communication, 25 March 2022 and 7 April 2022). Unfortunately, also the NÚKIB representative acknowledged that the general awareness of the ECSM is very low in the Czech Republic (personal communication, 3 May 2022). So, while there is a clear intention to take part in the ECSM (both from the public and private sector) and focus on cyber security (and hence, to enhance Czech cyberculture and same strategic thinking), the outcome is, at minimum, dubious.

In conclusion, one must admit that the Czech Republic has solid basics to become successful in the resilience towards cyber threats. There is still serious work to be done, though. The table on the next page summarises the findings of this chapter and points out the issues that were identified as the most fundamental to be improved.

Instrument/Institution	Gaps Identified
NÚKIB	• Not publishing any detailed information on the cyber-attacks in the Czech Republic. • Not providing independent cyber-security experts to explain issues to the public. • Tedious external communication and difficult language. • Lacking platform for sharing information between the public and private sector.
IZS ČR	• Non-existent crisis scenario covering cyber incidents. • Omission of the crucial parts of society (private businesses, citizens) in the standard operating procedures. • Difficult, inaccessible language of the crisis documents; unesthetic and unfriendly design. • Unable to bring together actors across the sector to improve the exercises and public-private cooperation.
National Cyber Security Exercises	• Lack of cyber exercises that would bring together actors across the sectors. • Small-scale exercises that are limited by the NÚKIB's lack of staff and underfinancing.
European Cyber Security Month	• One week of events instead of a month. • Not enough public attention: nobody is aware of the "Cyber Security Month". • Not enough activities for public: lectures, discussions, movie projections, lessons, etc.

Table 3: Summary of the gaps identified in the Czech security environment
Source: Author's Findings

4 Norway: State of the Art

The aim of this chapter is to present a case study on the Norwegian approach to the public-cooperation in terms of cyber threats; and to explain how and why do these tools work. Firstly, the chapter outlines fundamental documents. Secondly, the Norwegian strategy is presented, including the specific instruments of public-private cooperation. The chapter is concluded with conclusions and "lessons learned" from the Norwegian approach to public-private cooperation.

Norway is perceived and regarded as being able to "punch above its weight" because of its mix of high-end capabilities for a country of its size, and a mature total defence concept—Norway's strategy for crisis management involving all parts of the society (both military and civilian) in national defence (RAND 2020). Norway's total defence policy is revoking Cold War-era planning based on close cooperation between military and civilian institutions but in additional security and societal context. Total defence combines the armed forces and civil society in a comprehensive whole-of-society approach to security that intends to deter an attack by making a target state a challenging prospect for an aggressor.

Norwegian strategy towards hybrid/cyber threats is constantly evolving. One of the most significant changes is a discourse shift in conceptualisation from "Critical Security Infrastructures" to "Critical Security Functions" in the 2018 *National Security Act*. This novel understanding of critical services was intended to reflect current threats and to allow Norway to get the tools to secure these vital services. The shift in understanding of essential services could be partly seen as a response to increasing concerns with the hybrid threats. Norway is exposed to larger states, most notably Russia and China.

As the relationships are continually worsening, both are regularly pointed to as actors in cyberspace in yearly reports by the intelligence services, mainly through cyber espionage. The close geographical proximity to Russia arguably guides the cyber security efforts when a shift from deterrence to societal resilience is necessary (Gjesvik 2021, p. 147).

In 2018, Norway published its latest total defence reference manual prepared jointly by the Ministry of Defence (FD) and Ministry of Justice and Public Security (JD), which provides the most far-reaching, publicly available source of information on total defence from all Nordic countries (Norwegian Ministry of Defence & Ministry of Justice 2018). As a small nation, Norway understands that its armed forces do not possess all the necessary resources to fight a war and will be heavily dependent on civilian personnel, the public sector, businesses, and industry (Wither 2020, p. 67). For instance, in 2017–2018, the Norwegian Defence Forces signed several agreements with both public and private actors, such as the Norwegian Public Roads Administration regarding, e.g., the availability of reserve bridges, and with *Bring* and *Martinsen Transport AS* on transportation of defence materiel (Møller 2019, p. 250).

In 2020, the Norwegian Ministry of Defence released its latest *Long Term Defence Plan 2020*. Together with the *Setting the Course for Norwegian Foreign and Security Policy*, a government white paper issued in 2016, and *Risk in a Safe and Secure Society*, a government white paper on public security also published in 2016, it forms part of the Government's work to strengthen security and emergency preparedness. This strategic report, updated every four years, is designed to ensure that the armed forces of Norway are well prepared for an ever-changing international security environment. According to the Defence Plan, the defence of Norway relies on a "modern and well-prepared Total

Defence Concept" that "builds national resilience and reduces vulnerabilities when faced with hybrid threats" (Ministry of Defence 2020, p. 4). Norway's security is dependent on a Total Defence framework, which "enables relevant civilian assets to support the national and allied defence efforts during peacetime, crisis, and armed conflict" (Ministry of Defence 2020, p. 2). Furthermore, the principle of civilian support to the Norwegian Armed Forces in times of crisis is described as "the core of the total defence concept" (Ministry of Defence & Ministry of Justice 2018, p. 31) and "the private and public sectors need to work together to strengthen resilience towards existing and emerging threats" (Ministry of Defence & Ministry of Justice 2018, p. 16).

4.1 Cybersecurity in Norway: Strategy

This subchapter aims to answer what specific instruments of public-private cooperation utilise the Norwegian government; and how and why they work. The analysis is conducted based on an open-source analysis and the data from the ten interviews with Norwegian stakeholders.

Norwegian approach to cyber security is placed within the western understanding of multi-stakeholder cooperation between public and private actors. This approach stems from a high degree of private ownership over critical infrastructures. So, cybersecurity is conceptualised as an "assemblage" of various actors (Gjesvik 2021, p. 145). The Norwegian societal cyber security rests on four fundamental principles: responsibility, similarity, proximity, and cooperation. *Responsibility* guides that the organisation in charge of day-to-day matters should also be responsible in the event of a crisis; *similarity* indicates that organising for managing situations should resemble the regular organisation; *proximity* means that any problems should be resolved at the lowest possible level; and finally, *cooperation* indicating that every authority

and actor involved in security holds the responsibility to ensure the best possible cooperation between actors (Gjesvik 2021, p. 145).

Norway's cybersecurity policy currently consists of two strategy documents, the *National Cyber Security Strategy for Norway* issued in 2019 by the Norwegian Ministry of Justice and Public Security (a two-part list of measures back strategy) and the *International Cyber Strategy* published in 2017 by the Ministry of Foreign Affairs. International Cyber Strategy sets out Norway's governing principles and strategic priorities relating to the whole spectrum of *international* cyber policy issues: e.g., cyber security, innovation, and the economy, international cooperation to combat cybercrime, security policy, or development and human rights (Permanent Delegation of Norway to NATO 2019).

For the thesis, National Cyber Security Strategy for Norway is more interesting. It emphasises working together to reinforce cyber security in society and defines five strategic goals in terms of cybersecurity: (i.) Norwegian companies protect themselves against cyber incidents, (ii.) critical societal functions are backed by reliable digital infrastructure, (iii.) cyber security is aligned with the needs of society, (iv.) organisations can detect and handle cyber-attacks, and (v.) police have the power to prevent and combat cyber-crimes. This strategy also reinforces public-private, civilian-military and international cooperation. Private companies often develop digital services and products, and a substantial part of Norway's critical digital infrastructure is owned and operated by private actors. As a result, essential security decisions are made by non-state actors, which calls for an extensive public-private partnership. As an increased collaboration inevitably leads to better situational awareness and better decisions, governmental bodies and the business community should work together to identify and discuss cyber

security challenges. Any cooperation between state and private businesses "should carry obligations for both parties and be based on transparency, trust, and mutuality" (Ministry of Justice and Public Security 2019a, p. 9).

A two-part List of Measures accompanies this 2019 Strategy. Part one describes fifty-one key steps that support the strategy, and part two lists ten basic measures that both public and private companies are recommended to implement. Among the most critical measures in the field of public-private cooperation are the following: establishing National Cyber Security Centre, appointing a cyber security committee, ongoing support to NorSIS (Norwegian Center for Information Security) and nettvett.no service, organising annual National Cyber Security Awareness Month, launching Norwegian Cyber Range (NCR), conducting National Cyber Security Exercises, a continuation of the consultancy activities under the auspices of the Norwegian National Security Authority (NSM), and transparent evaluation of unwanted cyber incidents. (Norwegian Ministries 2019b, p. 8-32). The second part involves ten measures that private businesses are recommended to implement to improve companies' ability to protect themselves against unwanted cyber incidents, and every company should follow them.

In Norway, three ministries are mainly responsible for cyber security: the Ministry of Justice and Public Security (JD), the Ministry of Defence (FD), and the Ministry of Foreign Affairs (UD). The JD is responsible for coordinating cyber security in the civilian sector. In practice, there is a structure where each ministry is responsible for protecting its domains. The Ministry of Justice and Public Security has a "coordinating" role in ensuring that the overall security work is sufficient (Gjesvik 2021, p. 145). The JD holds special responsibility for national cyber security and outlines the government's policy for cyber security, including requirements and recommendations for both public and

private companies. The FD holds responsibility for cyber security in the defence sector. The UD is responsible for Norwegian foreign and security policy, including coordinating Norway's positions in international arenas where challenges in cyberspace are discussed (Norwegian Ministries 2019a, p. 6, 22). However, there is one ministry with a "special" role. Ministry of Local Government and Regional Development (KDD) is accountable for promoting a more robust, more comprehensive approach to cyber security in public administration. It also has coordination responsibility for the government's ICT policy. According to the KDD representative, it should have a more important role and be more involved within the responsibilities of the "Big Three", as KDD's primary role is the responsibility for telecommunications (including satellites, internet services, 5G networks, cyber, etc.) (KDD representative, personal communication, 9 March 2022).

However, according to the National Cyber Security Strategy for Norway, cyber security should primarily be a responsibility at a company level. At the same time, all government ministries are responsible for enforcing cyber security in their sector (Norwegian Ministries 2019a, p. 22). In this regard, a crucial initiative in cybersecurity is the establishment of sector-specific response communities, so-called "system of POCs" (UD representative, personal communication, 16 February 2022). This initiative aims to (i.) ensure that each ministry safeguards that the required cybersecurity measures are followed, and secondly, that each ministry actively involves the private sector in the preparation and realisation of measures (Norwegian Ministries 2019b, p. 7). Hence, ministries must work closely with government agencies and private sector stakeholders to coordinate planned cyber security measures with other ministries (Norwegian Ministries 2019b, p. 26). The ambition behind this "system of POCs" is to have the capacity to support their

respective sectors and to serve as hubs for information and the flow of data between companies within the industry, between industries, and between sectoral and national level (meaning especially NorCERT) (Norwegian Ministries 2019b, p. 26). To ensure the workability of this initiative, a point of contact ("POC") is set up within every ministry. This POC is then responsible for the cyber incidents and communication with both government and its bodies and stakeholders from the private business within the sector. So, the POC is mainly responsible for issuing warnings within the industry and then reporting to the NSM and NorCERT. So, every POC communicates directly with the private companies within its sector, ministries that have primary responsibility for cybersecurity (JD, UD, FD), NorCERT, and other governmental agencies (e.g., DSB). This architecture proved to be well-functioning, as the private companies always know whom to contact in case of a cyberattack. The same also works in the case of other hybrid threats. In such a situation, the POC warns the companies within the sector and shares the information and private companies' experience with the public authorities (UD representative, personal communication, 16 February 2022). A large part of the companies has their security and compliance departments responsible for their incidents. Usually, the director of these "*sikkerhet og samsvar*" (security and compliance) departments serve as the POC for the public sector and the employees inside of the company (private sector representative #1, personal communication, 25 February 2022).

To sum up, the cybersecurity challenges may be resolved by emphasising collaboration and partnerships among the relevant stakeholders. In Norway, this is allowed especially by the sector-specific response communities. As the Norwegian approach to cybersecurity emphasises, among other things, all ministries and private businesses working together to reinforce cyber security,

there is a high level of mutual trust and personal networks between the public and private sectors. The concrete measures and principles explaining *how* and *why* the Norwegian approach works in practice are elaborated in the following subchapter.

4.1.1 National Cyber Security Center

National Cyber Security Center (NCSC) is a part of the Norwegian Security Authority (NSM) under the Ministry of Justice and Public Security auspices. The NSM is the national specialist authority for ICT security. It produces an annual report on the state of security. In this report, the NSM considers risks applying to vital societal functions and critical infrastructure and information that should be protected. According to the Ministry of Justice and Public Security representative, the controlling function share two ministries—JD and FD. This civil-military division is unique, as generally, national responsibility for cybersecurity is held by the civilian authorities. This share of responsibility allows for closer cooperation between the cybersecurity apparatus, an excellent sharing of information, and an extensive network of contacts (JD representative #1, personal communication, March 14, 2022). These structural factors make public-private cooperation easier and contribute to the high trust between the public and private sectors.

Several private companies in Norway directly cooperate with NSM, especially those responsible for critical infrastructure or critical societal function. According to a representative from one of the largest communications companies in Norway, NSM is primarily focusing on private businesses on the critical level responsible for critical societal functions (see more on critical infrastructure below in chapter 4.1.6). This communications company is defined as providing "important societal function", and it follows

the NSM guidelines for ICT security. Still, it is not cooperating with the NSM on a day-to-day basis. However, the private company has direct contact with the NCSC and NorCERT and does know a concrete POC within the NCSC if they are under cyberattack or other external threat (private sector representative #2, personal communication, 25 February 2022).

National Cyber Security Center under the NSM is the Norwegian point of contact in ICT threats and cyber security incidents, and its goal is to enhance Norway's resilience in cyberspace. According to the *National Cyber Security Strategy for Norway*, establishing this centre is "a key measure to increase private-public partnership in cyber security" (Norwegian Ministeries 2019b, p. 10). The centre represents a reinforcement of the work NSM is already doing, and it is home to the Norwegian Computer Emergency Response Team—NorCERT. NorCERT's three main activities are responding to cyber threats through the 24/7 technical threat operation centre, detecting data breaches in critical infrastructure across sectors, and providing network analysis and counterintelligence (NSM 2021).

4.1.2 The Norwegian Directorate for Civil Protection

The Norwegian Directorate for Civil Protection (*Direktoratet for samfunnssikkerhet og beredskap,* DSB) is a Norwegian government agency under the Ministry of Justice and Public Security. DSB's general purpose is to protect Norwegian citizens from accidents, disasters, and other incidents. It is accountable for prevention, crisis management, studies and analysis, civil and military cooperation, and cyber security (DSB 2022). Its responsibility covers local, regional, and national preparedness and emergency planning, fire safety, electrical safety, and handling and transporting hazardous substances. Interestingly, the head office of DSB is located in Tønsberg, a city

approximately one hour drive from Norway's capital. According to the DSB representative, its location contributes to the decentralisation of the Norwegian public authorities. It enhances the feeling of "proximity" to the citizens and legal persons across the country (personal communication, 30 March 2022).

In 2018, DSB embraced a concept of 'total defence' based on the collaboration between the military and civilian resources to ensure societal safety. In Norway, societal safety addresses critical infrastructures and critical societal institutions (Haavik 2020, p. 3). According to the Norwegian Official Report NOU 2006:6 called "*When security comes first: Protecting Norway's critical infrastructure and critical social functions*", critical infrastructure is defined as the "facilities and systems that are necessary to maintain society's critical functions, which in turn cover society's basic needs and the population's sense of security" (DSB 2012, p. 9). This includes, among other things, food, water, and heat supplies, ensuring national security and crisis management, defence, ICT security, maintaining the democratic rule of law, maintaining financial stability, and protecting the environment (DSB 2016, p. 10-19).

By its work, DSB largely contributes to ensuring society's critical functions. One of the instruments is publishing the studies and analyses that contribute to the citizens' sense of security. In 2019, DSB published its last *Analyses of Crisis Scenarios*, a document analysing and assessing threats that may affect Norwegian society. It is one of four Norwegian threat assessment documents.

On more than 200 pages, the analysis produced by DSB covers natural accidents, terrorism, supply failures, nuclear accidents, aggression by a foreign state, or cyberattacks. For the thesis, the chapter on cyberattacks is of particular interest. The analysis provides two cyberattacks scenarios on financial infrastructure and electronic communications infrastructure. Both

scenarios describe the course of events, time, scope and point out similar events in the past. It involves assessments of likelihood, vulnerability, and consequences. It also analyses impacts on the economy, life and health, and societal stability. Besides the comprehensive evaluation of consequences, the analysis also presents possible measures taken right away. For example, after the study was conducted, the Ministry of Finance amended the regulations to ensure that banks must have solutions in place that can meet any increased demand for cash should the electronic payment systems fail (DSB 2016, p. 202). Enhancing resilience through civil preparedness is crucial. Not only does a resilient country become more difficult to target, but also its society shows a higher level of trust in government and its decisions during a crisis. This was shown especially with the COVID-19 pandemic when countries with the higher trust of their citizens proved to be more resilient to the pandemic (Lenton et al. 2022).

According to the KDD representative, scenarios that are updated every year contribute to the cooperation between the public and private sector and make collaboration during crises easier as "everybody knows what to expect and what to do" (KDD representative, personal communication, 9 March 2022).

4.1.3 Norwegian Business & Industry Security Council

According to the UD Representative, Norwegian Business & Industry Security Council (*Næringslivets Sikkerhetsråd*, NSR) is one of the most valuable bodies in fostering public-private cooperation in Norway (personal communication, 16 February 2022). The main NSR's task is to facilitate collaboration across sectors and industries, ease the communication and networking between the public and private sectors, and prevent and combat the business community's

security threats. NSR aims to facilitate cooperation across sectors and industries and better equip the business community to assess risk and resist current security threats. Through the "Security Conference," breakfast seminars, lectures, publications, courses, and informal meetings, NSR facilitates networks between business actors and government officials (Næringslivets sikkerhetsråd 2022a). The NSR represents companies with over 300 000 employees. The members include strategic companies from the sectors such as energy (e.g., AS Norske Shell, Statkraft AS), finances (e.g., DNB Bank, Norges Bank), communications (e.g., Telenor ASA, Telia Norge AS), services (e.g., Microsoft Norge AS, Deloitte AS), or transportation (e.g., PostNord AS, Ruter AS). Hence, NSR provides a platform for the cooperation of the public and private sectors in their efforts to combat industrial espionage, cyberattacks, theft, fraud, corruption, and more (Næringslivets sikkerhetsråd 2022b).

NSR has six committees that represent an expert panel of security managers and professionals with experience in security. The committees provide the necessary expertise and represent the "connection" between the Norwegian business sector and the relevant government authorities. NSR has the Information Security Committee that consists of business leaders, security managers, and professionals profiled from private IT companies in terms of cybersecurity. NSR is also closely collaborating with the National Cyber Security Center (NCSC). Through this collaboration, partners in the NCSC are contributing to strengthening security cooperation in the private and public sectors and thus contribute to protecting society in the digital space (Nasjonalt cybersikkerhetssenter 2021).

According to the UD representative, the functioning of the NSR is beneficial in advancing public-private cooperation in Norway due to two

reasons: (i.) the regular meetings between the leaders from the private sector with the representatives from the public authorities contribute to joint trust, and (ii.) it fosters personal ties between representatives from the public and private industry (personal communication, 16 February 2022). Trust and unique relationships are fundamental driving forces of cooperation between the public and private sectors. This statement is also supported by Nilsen, Security Director in Telenor Norge. According to Nilsen, "*formal and established partnerships are critical to success when it comes to the events that cause vital societal functions to collapse*" (Nilsen 2018b).

As the Norwegian state apparatus is relatively small, effective, and open to be accessed from the "outside" (meaning, e.g., by the private sector), the representatives from the private companies know whom to contact (UD representative, personal communication, 16 February 2022). This is also given by the initiative of sector-specific responsibility (see above), which allows for better interpersonal ties between the public and private sectors. As every ministry is directly responsible for cybersecurity in its industry (e.g., the Ministry of Petroleum and Energy is responsible for following the cybersecurity measures in the private energy companies), which overall allows for better communication and a higher level of mutual trust (UD representative, personal communication, 16 February 2022).

4.1.4 National Cyber Security Exercise

The civil-military exercises are a natural part of the Norwegian total defence concept. Trident Juncture 2018, a NATO-led military exercise held in 2018 with an article 5 scenarios, was a recent test of Norway's total defence system and the cooperation during a crisis (Masters 2018). Private companies have been invited to participate during all exercise phases, i.e., both during

the preparations and during the exercise itself. During the exercise and the simulated crisis, critical infrastructure companies were in the same main security room as the highest governmental representatives and military personnel. Private companies were actively participating in finding solutions and their execution (UD representative, personal communication, 16 February 2022). This is an excellent example of practical public-private cooperation and how it should be carried out. According to Hanne Tangen Nilsen, Security Director in Telenor Norge[20], strengthening cooperation with the public sector is crucial. Telenor and The Norwegian Cyber Defence Force cooperated closely during the 2018 Trident Juncture exercise, which "*contribute[d] to strengthening national emergency preparedness*". According to Nilsen, Telenor and other private critical infrastructure actors must be given a permanent place in the total defence. Formalised and binding cooperation between state and private companies is crucial for enhanced societal resilience (Nilsen 2018a).

Moreover, a new national cyber security exercise was implemented in 2018. It was conducted to primarily reinforce public-private collaboration on cyber security incident management. The starting point of the training is a more robust public-private partnership. Therefore, the exercise involves private companies planning, designing, and executing the activity. Key owners of critical digital infrastructure and other selected private companies are invited to participate early to work with the authorities to define the

[20] Telenor is a Norwegian majority state-owned multinational telecommunications company; and one of the world's largest mobile telecommunications companies. Telenor Norge owns and manages socially critical infrastructure which, together with its mobile services, fixed networks and broadband, is critical for Norwegian society to function. Almost 80 percent of all data traffic in Norway goes through Telenor services and infrastructure.

exercise's objectives and framework (JD representative #2, personal communication, 14 March 2022). JD, FD, and UD hold assignment responsibility for the exercise. DSB is responsible for the planning process and the actual execution of the exercise in close collaboration with partners such as NSM (Norwegian Ministeries 2019b, p. 27).

The exercise took place in 2019 and 2020, but in 2020, it was significantly reduced due to the COVID-19 pandemic. However, according to JD representative #2, the exercise successfully achieved the desired ends despite the reduction. The planning phase takes 1 to 2 years, and the preparation is the essential part of the exercise. During the planning phase, different stakeholders get together to map the preparedness and prepare the exercise itself. This allows for closer collaboration and establishing new networks of contacts. Hence, there is lots of extra value even during the preparation (JD representative #2, personal communication, 14 March 2022), and the fact that the exercise was not carried out on its full scale was not such an issue.

Furthermore, in 2019, the JD prepared a tabletop exercise that is free and accessible online for all private companies (JD representative #1, personal communication, 14 March 2022). The platform "ovelse.no" is owned by the DSB and is operated by the Norwegian Cyber Range at the Norwegian University of Science and Technology (NTNU). Exercises to achieve better digital security include several scenarios that have been developed in collaboration between DSB, NTNU, NorSIS, and the NSM (ovelse.no, 2021). The exercises are pretty popular, and while JD does not possess specific statistics on how often the tabletop exercise is used, they have received positive feedback from private companies (JD representative #1, personal communication, 14 March 2022).

These initiatives organised by the state are helpful in two ways. Firstly, it improves the trust of the companies and public in the state, as the Norwegian public authorities show their capabilities and capacities. According to the NorSIS representative, private businesses are motivated to approach the state because they know that it has this extra-added value of know-how and ability. Hence, private companies *trust* the state (personal communication, 16 February 2022). Secondly, exercises are incredibly helpful in networking and setting personal ties that enforce trust and cooperation—both between national and international (UD representative, personal communication, 16 February 2022).

4.1.5 National Cyber Security Awareness Month

National Cyber Security Awareness Month is an annual campaign to educate the public about the importance of cybersecurity. The campaign is coordinated by the European Union Agency for Cybersecurity (ENISA) and is supported by the European Commission and other partners from the public and private sectors. Throughout October every year, the European Security Month (ECSM) brings together EU member states, governmental organisations, the private sector and academia to "promote healthy online habits" (NorSIS 2021b).

In Norway, this important public-private initiative is coordinated by the Norwegian Center for Information Security (NorSIS) on behalf of the Ministry of Justice and Public Security (NorSIS 2021a). Training lessons are provided for employees every year, and many other actors usually participate. For example, The Arctic University of Norway offers all employees and students a course on cyber security (UiT 2021). In 2018, more than 250 000 employees attended the lessons and lectures in 330 companies (Norwegian Ministeries 2019b, p. 18). According to several public sector stakeholders and private

sector representatives, "Security Month" (as referred to by the interviewees) have a functional public focus (private sector representative, personal communication, 25 February 2022). It is a popular and successful measure with many events, discussions, and workshops primarily attended by the public (NorSIS representative, personal communication, 16 February 2022). It is one of the priorities of the public authorities in terms of public-private cooperation (especially NorSIS, and JD, who holds the primary responsibility). Also, the private sector is eager to cooperate in the organisation of the accompanying events and take part in the initiatives planned by the state—e.g., professionals and experts in the field of ICT security give away free lectures, pay the schools and public sector representatives with a visit, or offer free open courses (private sector representative, personal communication, 25 February 2022).

Besides Security Month, NorSIS holds responsibility for other initiatives; for instance, one of its services is Nettvett.no, a website with advice and guidance on safer Internet use. The information is aimed at individuals from children to adults and small and medium-sized businesses. The NorSIS also organises "Security Divas", a conference for and with women to strengthen the security environment. According to the former NorSIS employee, NorSIS is very useful and popular when reaching out to the public. It is incredibly successful in contributing to the cyberculture, another element crucial for national cyber resilience. As the human factor is fundamental to cybersecurity, improved cyberculture and effective cybersecurity practices are essential when building a society resilient toward cyber and other hybrid threats (NorSIS representative, personal communication, 16 February 2022).

4.1.6 National Cyber Security Forum

In 2018, the Norwegian government set up a partnership forum called National Cyber Security Forum (Forum for Nasjonal IKT-Sikkerhet) that comprises private companies, public authorities, and academic representatives. The parties represent the business community that either owns or manages critical digital infrastructure or critical societal functions and parties that play crucial roles in research and education. This public-private partnership forum aims to ensure that strategic issues connected to the cyber security challenges are discussed between private companies and public authorities. The platform should "promote openness, trust, and interaction between public and private operators about sharing information and discussing problem issues related to cyber security." It also establishes new cooperation among the authorities at the ministerial level and between selected companies. (Norwegian Ministries 2019b, p. 14).

The Forum generally meets three times a year, and the primary responsibility for the functioning holds the JD (JD representative #2, personal communication, 14 March 2022). Around 20 private companies participate in the Forum, and high-level participants from the companies attend the Forum. The participants are also changing regularly, so the government do not work with the same group of people all the time. The companies taking part in the Forum are selected through a thorough selection process allowing to choose from companies throughout the spectrum: companies responsible for critical infrastructure, representatives from the academia, and large companies from the supply chain side (JD representative #1, personal communication, 14 March 2022). According to JD representative #2, the cooperation is relatively easy as the companies themselves strive for participation and "everybody wants to participate" in the Forum (personal communication, 14 March 2022).

According to the UD representative, this is given mainly by the feeling of prestige to be part of the Forum, more accessible access to the security information and networks of contacts, the possibility to influence the policy outcomes, motivation to share know-how from the state on handling cyber incidents, and financial incentive as for the companies it is cheaper to get information and experience directly from the state (UD representative, personal communication, 16 February 2022) than to pay security consultants. It is also important to note that juridical persons may apply for security clearance to access the classified information in Norway. The process of acquiring security clearance is the same for legal persons as for natural persons (JD representative #1, personal communication, 2022).

As for the private sector, the Forum is very well appraised by the private companies. According to Nilsen, Security Director in Telenor Norge, the government is doing an excellent job strengthening public-private cybersecurity cooperation. She especially mentions establishing the National Cyber Security Forum as a perfect example of functioning public-private cooperation. According to Nilsen, there is great interest in national security and preparedness from politicians, authorities, the media, customers, and organisations (Nilsen 2018b).

4.1.7 Strategic Communication

"Strategic communication" is a similar buzzword as "hybrid warfare" and deserves to be defined. Hallahan et al. introduced the term in 2007 as "the purposeful use of communication by an organization to fulfil its mission" (p. 3). According to Halloran (2007, p. 7), successful strategic communication assumes a defensible policy, a respectable identity, and a core value. According to Zerfass et al. (2018, p. 487), strategic communication

encompasses "all communication that is substantial for the survival and sustained success of an entity". Strategic communication is a "purposeful use of communication by an entity to engage in conversations of strategic significance to its goals". These entities include all kinds of organizations—governments, private businesses, or non-profits, as well as social movements and known individuals in the public sphere (Zerfass et al. 2018, p. 487). All in all, strategic communication is one of the fundamental elements contributing to the so-called shared strategic thinking. "Shared strategic thinking" in society can provide a pillar around which governments, private businesses and actor entities may articulate their own policies, activities, and priorities. It helps to drive cooperation among different actors as they, for instance, share their views on threats. Hence, shared strategic thinking encourages the society to work together and cooperate to shape the policies.

Most current discussions on public-private cooperation are related to enhancing societal resilience and procedural possibilities. However, non-kinetic means of warfare (and cyberattacks, in particular) are a new terrain enabling a variety of physical and social constructions (Kuusisto and Kuusisto 2013). To make sense of the recent phenomenon of hybrid threats, high-quality, understandable and accessible strategic communication is required from public authorities and private companies. According to the KDD representative, a specialist director responsible for digital security in Norway with long experience from one of the largest Norwegian telecommunications companies, strategic communication is an essential element in building trust between the public and private sector (personal communication, March 9, 2022). A severe cyber incident may require national handling that also involves the need for communication with the population and the media under established procedures for central crisis management. Strategic

communication must be carried out to prevent unnecessary damage to reputation and trust. According to several public authorities' representatives, strategic communication is a cornerstone of building trust in society and between the public and private sectors (UD representative, personal communication, 16 February 2022 and KDD representative, private communication, March 9, 2022).

In Norway, the gamechanger was the 2019 cyberattack on the Norsk Hydro (private company representative, personal communication, February 23, 2022). The attack affected the entire global organisation and stopped several areas of production. Hydro closely cooperates with the Norwegian National Security Authority (NSM) and other relevant Norwegian and international authorities. This is the basic procedure followed by many other companies. What was different was Hydro's approach to the external communication of the attack. According to the KDD representative, Hydro's strategy changed the cyberculture when it was incredibly open about the attack and the consequences. Before the Hydro attack, companies were reluctant to publicly inform about the attacks out of fear they would lose credibility, customers, and trust. But quite the contrary, the Hydro's openness about the attack helped them to look more responsible and credible. Excellent communication between Hydro and responsible governmental authorities helped to act fast and publish a joint media message that prevented any communication mishap. Since then, other companies have taken Hydro as an example and talked openly about cyberattacks (KDD representative, personal communication, 9 March 2022). They are very keen on cooperating with the state primarily as it is cheaper and easier than dealing with the potential consequences of a cyberattack (NorSIS representative, personal communication, 16 February 2022). This openness also contributes to the joint

trust in society, i.e., between the triangle of private businesses, public authorities, and the public (KDD representative, personal communication, 9 March 2022).

Generally, communication between the public and private sectors is working very well in Norway. The government possesses reports and specific guidelines on sharing classified information with private companies (JD representative, personal communication, 9 March 2022). Unfortunately, the policies are not public and cannot be accessed if one is not a governmental employee. The UD representative shared that almost all Norwegian public authorities use a classic Traffic Light Protocol (TLP) that allows them to easily control the spread of information and decide which information can be distributed among private companies. According to the UD representative, this easy access to the government reports and documents also helps build trust among the public and private stakeholders (UD representative, personal communication, 16 February 2022).

The constantly ongoing dialogue supports strategic communication between the state and private businesses. Given the excellent level of communication during peace times, companies and the state are capable of cooperation during a crisis. The critical element in strategic communication is trust—, especially when preparing a joint message for the media and public. Communication is fuelling trust. A good example is the discussions about regulations in Norway—whenever there is a need for a new legally founded regulation, the discussion forum between the private sector and government is initiated. So, the dialogue serves for the good of both government and the private sector, and most importantly, it positively affects joint trust and communication channels. A high level of trust and a wide net of contacts among the stakeholders contributes to the excellent level of cooperation

during the crisis. Finally, the dialogue allows for a balance between what the state *needs* and what private businesses *want*. So, when the regulation is put in place, it does not go behind the companies' backs, increasing trust (KDD representative, personal communication, 9 March 2022).

4.1.8 International Cooperation

The Norwegian Ministry of Foreign Affairs (UD) is a body responsible for international cooperation in cybersecurity and hybrid threats (JD representative #1, personal communication, 14 March 2022). The UD is responsible for foreign and security policy, including coordinating Norway's position on challenges in cybersecurity and hybrid threats (Norwegian Ministries 2019a, p. 22).

Norway is part of the Nordic Defence Cooperation (NORDEFCO), which provides an overarching structure for defence cooperation. It provides a framework for collaboration to enhance territorial defence capabilities, and its focus is collective defence in the region (Wither 2020, p. 73). Although no specifics are provided, increased total defence cooperation and improved resilience against hybrid challenges and growing cyber threats are core ambitions in NORDEFCO's *Vision 2025* (NORDEFCO 2018, p. 6). According to the UD representative, NORDEFCO is an essential platform for sharing information between Nordic countries. It is an organisation that allows for joint support and help, as the cyber and hybrid threats are inherently transnational and cross-border issues. Inside NORDEFCO, countries exchange their experience and know-how (UD representative, personal communication, 16 February 2022), which is beneficial for improving the best practices. In terms of public-private cooperation, the exchange of experience and know-how through international cooperation fosters the trust of citizens and private

businesses in the Norwegian public authorities. Norwegian public authorities intensively cooperate mainly with high digitally developed countries (i.e., Finland, Denmark, Sweden and Iceland), which significantly improves the state's cybersecurity capability and improves the position of Norway's public sector as a high-quality, reliable and trustworthy partner for the private sector (UD representative, private cooperation, 16 February 2022).

However, even in Norway's case, the cooperation is not without challenges. Differing NATO affiliations are the main obstacle to deeper collaboration in the NORDEFCO. Hence, solid bilateral relations between non-NATO member countries—Finland and Sweden—have developed outside NORDEFCO's multilateral framework. Different planning priorities, rules for classified information, other national standards, an absence of political trust at the state level and slow decision-making, in general, have complicated closer military cooperation (Forsberg 2013, pp. 1178–1179). This Norwegian "take-home message" is essential for the later part of the thesis, where the author proposes concrete policy recommendations for the Czech Republic.

4.2 Chapter Conclusions: Lessons Learned

This subchapter aims to analyse the instruments from Norway altogether and identify *why* they work so that they can serve as an inspiration for the Czech approach. The analysis of the Norwegian approach to public-private cooperation to enhance resilience to hybrid threats proved the Norwegian model to be working and well-appraised both by the public authorities and private businesses. So, what means and approaches from Norway can be used in the Czech environment? The table below summarises instruments of the public-private cooperation identified in Norway based on the three-pillar

division (see more in chapter 2.4 on the theoretical framework). The most interesting ones are shown in bold:

Awareness	Resilience	Partnerships
• **Crisis Scenarios**	• **System of POCs**	• International Cooperation
• **Strategic Communication**	• National Cyber Security Forum	• Norwegian Business & Industry Security Council (NSR)
• Cyber Security Awareness Month	• National Cyber Security Exercise	

Table 4: Instruments of public-private cooperation utilised in Norway sorted into the three-pillar model
Source: Author's findings

So, why do these instruments of public-private cooperation work? The most important take-home note is that the Norwegian approach has two crucial steppingstones: *trust* and the *whole-of-society approach*. Everybody is invited to the table in the Norwegian strategy to counter hybrid threats. This is crucial—without trust, it is almost impossible to achieve resilience. The different parts of society will not cooperate when they do not trust each other. Lack of trust and personal networks would damage the flow of information and make any kind of public-private cooperation nearly impossible.

It is also important to note that all the instruments and mechanisms identified are usable in the case of cybersecurity and elsewhere. They can be easily transformed into instruments that counter disinformation, economic pressure, the safety of value chains and several other hybrid means of warfare. The important information is that all the tools are primarily based on trust, shared strategic thinking, dialogue, effective strategic communication, understandable and straightforward institutional procedures, and the principle of no one leaving behind. What is good is that all these mechanisms are transferable to other political and socio-economic environments, including

the Czech one. The next chapter will shed light on how to get the most from the Norwegian model and enhance Czech resilience towards hybrid threats.

In conclusion, it is necessary to note that, according to the interviewees, the Norwegian approach also has room for improvement. Often mentioned was even closer cooperation between public authorities or further improvement of the networks between different ministries. Another deficiency might be the unwillingness to update the traditional total defence concept. Several representatives felt that public authorities tend to stick with the pre-1990s conceptualisation despite the new concept. This is one of the challenges for Norwegian society. However, overall, the public-private cooperation works remarkably in Norway—based on the interviews with representatives from the public sector, private businesses, Norwegian positions in the international rankings and its results when facing real-life hybrid interference.

5 Results

The previous two chapters shed light on the concrete instruments utilised in Norway and the Czech Republic. Chapter 3.2 attempted to identify the gaps in the Czech cybersecurity strategy for countering hybrid threats. Chapter 4.2 summarises what can be learned from Norway and its approach. This chapter aims to synthesise the findings to provide an answer for the research question of the thesis, which is *what approaches from Norway's concept of total defence can the Czech Republic (and perhaps other countries) implement to enhance resilience towards hybrid threats*? Based on the "lessons learned" from Norway (chapter 4.2) and an analysis of the current situation in the Czech Republic (chapter 3.1) in terms of public-private cooperation, the author identified eight *good practices* that could be implemented in the Czech Republic to enhance national resilience towards hybrid threats. Besides the abovementioned chapters, this part drafts on the interviews with Czech and Norwegian representatives profiled from the public and private sectors.

While the Czech Republic has several institutions responsible for handling hybrid threats (e.g., CTHH), particularly cyber threats (NÚKIB), there is always room for improvement. The policy recommendations are divided into three categories based on what should be their end goal and what is their purpose. The categories are based on the three-pillar model of resilience introduced in chapter 1.2 of the thesis (p. 22). Once again, the categories are (i.) *raising awareness*, (ii.) *building resilience*, and (iii.) *improving partnerships*. Firstly, the table below compares the current situation in Norway and the Czech Republic. The policy recommendations follow after the table.

	Norway	The Czech Republic
Institutions Responsible for Cybersecurity	• Ministry of Justice and Public Security (JD) • National Security Authority (NSM) • National Cyber Security Center (NCSC)	• National Cyber and Information Security Agency (NÚKIB)
Instruments of Public-Private Cooperation	• Cyber Security Exercises • Cyber Security Month • Crisis Scenarios • Norwegian Business & Industry Security Council • National Cyber Security Forum • Sector-Specific Responsibility	• Cyber Security Exercises • Cyber Security Week • IZS Standard Operating Procedure
International Cooperation	• NATO • CoE Helsinki • OECD • NORDEFCO	• NATO • CoE Helsinki • OECD • V4 • EU

Table 5: The Norwegian Model vs the Czech Model
Source: Author's analysis based on the data from the interviews

The "trust" is not explicitly mentioned, despite being a prevalent answer in the interviews on the question "Why does public-private cooperation work in Norway?". Norwegian historical and cultural experience is quite different from the Czech. In Norway, trust is one of the founding elements and not necessarily something the government would try to achieve "manually". In Norway, trust is historically present. However, that does not mean that the government does not work on improving it and does not attach importance to the issue of trust in society. The only difference is that Norway's high level of trust allows for the easier achievement of a decent level of public-private

cooperation. This could be a severe concern for the case of the Czech Republic, as the interviewees commonly mentioned the lack of trust as the major obstacle. Nevertheless, the lessons learned showed that several instruments might work even without *a priori* trust. They should contribute to higher levels of trust between the government and private businesses along the way.

So, the three subchapters below identify the most important lessons learned from the interviews with the Norwegian and Czech stakeholders. While they draft on the previous chapters 3 and 4 and somewhat repeat what was already said in chapters 3.2 and 4.2, at this place author attempts to synthesise her findings to describe good practices and define policy recommendations.

5.1 How to Raise Awareness

Firstly, let us focus on raising awareness as awareness should be the first step when achieving a resilient society. When raising awareness about cyber security and hybrid threats, increasing knowledge about the topic is crucial. Another essential element in raising awareness is ensuring cross-sectoral communication between private businesses, organisations, and local actors. Based on the interviews, Norwegian stakeholders are doing very well in raising awareness across the society. From the interviews, three main mechanisms that improved awareness in Norway were identified: (i.) an attentive approach to cyberculture, (ii.) shared strategic thinking and (iii.) a shared feeling of responsibility among the society.

> *Good Practice: Build cyberculture by involving all parts of society to make (cyber)security a hot topic*
>
> Cyberculture in Norway involves all levels of society. It is considered an essential part of education in Norway. Hence, both the youngest and

eldest in the community are educated in cybersecurity. However, this was not always a standard. In 2016, NorSIS published a critical document on cyberculture that analysed risks in society, behavioural patterns, and suggested solutions. One of the crucial recommendations of the study is that cyber security culture can be shaped early in life and result in a more resilient society. So, the government should increase its efforts to educate society: children, the elderly, private businesses' representatives, and governmental staff. According to the NorSIS representative, cyberculture is on a decent level in Norway, which also positively affects the shared strategic thinking in the society. According to the NorSIS representative, educating society is one of the best steppingstones when raising awareness and building resilience (personal communication, 16 February 2022). According to (Czech) private company representative #4, educating the citizens is "the most important way how to improve cyberculture in the Czech Republic, and achieve better resilience" (personal communication, 7 April 2022).

The most straightforward institutional measure is Cyber Security Awareness Month to improve knowledge and education levels in cybersecurity. Every year, private businesses and the state are brought together to prepare discussions, workshops and lectures on cyber security. The organisation of the "Security Month" in October not only supports public-private cooperation by enhancing joint trust and networks but also improves the education levels of the society (children, seniors, employees in the companies that are not critical to the state). In Norway, Security Month is incredibly popular. All interviewees the author talked to were aware of the event and its purpose (a large part of them also went through some of the

courses/lessons at some point in their career/education). However, this was not the case in the Czech environment. In the Czech Republic, none of the interviewees was aware of "Cyber Month", which is quite unfortunate. However, both private company representatives #3 and #4 supported the idea of conferences, workshops, cultural events, or discussions focused on cybersecurity and involving all parts of society (personal communication, 25 March 2022, and 7 April 2022). To conclude this part, Cyber Security Awareness Month raises public awareness and improves the cyberculture and contributes to the image of the state as a trustworthy and reliable actor with specific expertise.

Hereafter, based on the Norwegian approach and the opinion of the Czech stakeholders, the **policy recommendations** are as follows:

- (i.) NÚKIB, MV, IZS and other relevant state organs should focus more on the ECSM: bring together various stakeholders both from the public and private sector, organise lectures, conferences, discussions, etc.;
- (ii.) secure sufficient finances to bring attention to the cybersecurity to make it a popular topic across the citizens and sectors;
- (iii.) bring together all parts of society (government, private companies, NGOs) to work together on the events.

Good Practice: Ensure reliable, trustworthy, and well-targeted strategic communication to advance shared strategic thinking

The outstanding level of cybersecurity in Norway is allowed, among other things, thanks to the excellent strategic communication carried out by both the public sector and private businesses. However, the

strategic communication at such a high level did not appear out of nowhere—it is mainly due to *shared strategic thinking*. When ensuring cybersecurity, the crucial issue is how private companies can consider security beyond the company's interests. Suppose there is shared strategic thinking about the threats among the public actors. In that case, private businesses, citizens, and all the parts of the society can think and act in a coordinated manner that benefits all the members of society. Also, the public authorities are more willing to lean on the private actors if they share the understanding of threats and vice versa. So, when the public and private sectors agree on the threat, they can engage constructively and cooperate for the best outcomes.

Strategic communication is one of the mechanisms enforcing shared strategic thinking. In Norway, strategic communication works primarily through three mechanisms: (i.) Strategic Communication Office under the Prime Minister's Office, (ii.) System of POCs (further elaborated in the subchapter 5.2) and (iii.) Crisis Scenarios (elaborated below). Same strategic thinking is one of the strengths of Norwegian society and can be achieved, among others, by efficient communication from the state toward other actors.

Nonetheless, according to private company representative #3 and MO representative, the Czech state fails to achieve functioning strategic communication based on cooperation (personal communication, 25 March 2022 and 11 April 2022). According to private company representative #4, the communication is good except at the nation-level, meaning that NÚKIB's strategic communication. Yet the private company must be active and reach out to NÚKIB to discuss the information provided in order not to be only a passive recipient. Also,

the representative referred that even NÚKIB's communication is difficult and "deserves to be fine-tuned" (personal communication, 7 April 2022).

So, to achieve reliable and well-targeted strategic communication, the **policy recommendations** are as follows:

- (i.) improve the communication channels and networks between the public sector and private companies so that during a crisis, the sectors will cooperate and support each other;
- (ii.) the Office of the Government of the Czech Republic should establish Strategic Communication Office directly under its auspices; this Office should serve as a governing body of the public authorities' strategic communication to ensure coordination;
- (iii.) continuously enforce cyberculture to achieve shared strategic thinking in the society (use the recommendations above on cyberculture).

Good Practice: Have crisis scenarios ready to strengthen the shared feeling of responsibility among the society

A shared feeling of responsibility is one of the "mechanisms" that resonated throughout the interviews. In Norway, all members of society share a sense that they "themselves" are responsible for their country's well-being. So, when it comes to (cyber)security and countering hybrid threats, society is eager to work on joint safety. What also resonated through the interviews is that it is difficult to achieve this feeling in society—, and it is a long haul.

However, several interviewees mentioned crisis scenarios. This instrument prepared by the DSB is a successful tool of public-private cooperation contributing to (i.) the same strategic thinking of the threat and (ii.) a shared feeling of responsibility. In the scenarios, the DSB very clearly explains different kinds of threats and why they concern every member of society. To illustrate the importance of this instrument, the scenarios were beneficial several times in Norwegian history, traditionally during natural disasters. In 2020, the scenarios were used during the COVID-19 pandemic for the first time on a large scale and proved incredibly valuable both for the public and private sectors. The "playbook" prescribed all parts of the society their obligations and responsibilities, which allowed for the easier handling of the crisis. As the scenarios attach every member of the society (public authorities, private businesses, citizens) to their role during the crisis, this instrument enhances the shared feeling of responsibility. Then, when a crisis comes, society is well-aware of the threat beforehand and has a sense of security, safety, preparedness, and readiness.

According to private company representative #4, the existence of such scenarios would be helpful. PCR #4 confirmed that the standard operating procedures used by IZS ČR are too complex and do not allow easy application in practice (e.g., for exercises or even actual use during a crisis). Nevertheless, the existence of "more practical and "story-based" scenarios would be useful, as it could provide the private companies with direct "tutorials" on handling real-life events and crises" (personal communication, 7 April 2022). The interview with the MV representative approved the author's findings regarding the standard operating procedure and the Norwegian crisis scenarios.

While the MV representative was sceptical at first, after presenting the author's results from Norway, he/she agreed that the existence of a document inspired by the Norwegian "playbook" would be advantageous. The MV representative also admitted that these scenarios could improve MV and IZS communication with the public, as currently, it is neither good nor easy to grasp (personal communication, 14 April 2022).

So, to enforce the shared feeling of responsibility and achieve the shared strategic thinking on what are the threats, the **policy recommendations** are as follows:

(i.) use the already existing standard operating procedures by IZS to prepare real-life scenarios inspired by the DSB Crisis Scenarios publication;

(ii.) update the scenarios, the responsible subjects and the processes every year;

(iii.) use the scenarios for the state-organised exercises (not only in cyber security but also for other (hybrid) threats).

5.2 How to Build Resilience

Trust is a cornerstone of every attempt to achieve a resilient society when building resilience. In the interviews, trust was mentioned at many different levels—interpersonal, interinstitutional and intersocietal. Trust is essential for the government's employees to cooperate, share information and exchange know-how effectively. It is necessary for private companies to trust the government's intentions and for public authorities to trust private businesses that they will not prioritise their interests over security interests. Also, the

citizens need to trust the state that they are acting in their interest and not abusing power at the expanses of the other parts of society.

Several interviewees mentioned that *trust* is not an issue in Norway. Trust is present as it is. Nonetheless, for the interviewees was challenging to identify why. Mostly they agreed on a combination of historical and socio-economic factors enhanced by the climate conditions; the representatives from the public sector usually mentioned "dialogue" in society, informal personal networks and informal structures established through the institutional tools of public-private cooperation (i.e., forums, exercises, seminars and workshop). The author attempted to synthesise the answers from the Norwegian respondents to identify "best practices" from Norway that could improve trust between the public and private sectors, and enhance resilience towards hybrid/cyber threats.

> *Good Practice: Set up new communication channels and personal networks by introducing sector-specific responsibility*
>
> Small bureaucratic apparatus, personal networks, excellent communication channels. These three mechanisms were mentioned in the interviews several times as some of the crucial aspects for resilience to function. These mechanisms are supported by sector-specific responsibility, the so-called "system of POCs". Every ministry has one POC for the private businesses within the given sector in this instrument. Hence, the private companies know whom to contact during a crisis, and government can access and communicate with the private sector through these POCs.
>
> As mentioned above, the system of one person responsible for cybersecurity inside the public authority and ditto inside of the private sector help to build trust in three ways. Firstly, the bureaucratic

apparatus in Norway is relatively small, so the information flow works well both *inside* of a ministry and *inter* ministries. The governmental representatives mostly know each other by name, especially those with a focus on the same area. In Norway, the government also has a public and online accessible Depkatalog, a "catalogue" containing contact information for the Prime Minister's office, ministries, and other governmental organisations. Depkatalog also provides information on which ministry, departments and sections are the individuals working on. So, for instance, if the ministerial POC needs to get a report to provide the private company with, they have access to a catalogue of the public sector employees and direct contact with them. According to the MV and MO representatives, such an instrument could be helpful both for the employees inside of the ministries and those from other ministries/public institutions/private companies (personal communication, 11 April 2022 and 14 April 2022).

Secondly, in the system of POCs, the private sector representative always communicates with the same person, which unavoidably leads to a certain level of personal connection that enhances the sense of reliability and trustworthiness not only of the person but the whole governmental institution. Lastly, the communication channel is only between two people (ministerial POC and cybersecurity/communication manager). Hence, the risk of misunderstanding is significantly reduced. The clarity of the information transmitted and the reliable cooperation itself mainly contribute to the joint trust.

In the Czech Republic, a similar instrument is ordered by the Cyber Security Act, which requires every company under this act to set up a

cybersecurity manager. However, this cybersecurity manager only functions inside the private company to share the information coming from NÚKIB, and there is no POC at the level of the public sector (i.e., ministries). According to the private sector representative #4, such an institutional instrument would be beneficial in three ways: firstly, it would simplify communication as everybody would know whom to contact. Secondly, it would improve the personal networks and ties of the private sector employees with the public sector. Thirdly, sector-specific responsibility can improve the state's authority as it will be shown as a unitary, cooperating entity that could pass on the information "inside" (personal communication, 7 April 2022). All the improvements identified by PCR #4 would increase the trust of the private sector in the Czech state. According to the MO representative, such an instrument would be handy for the public authorities, improve communication and joint trust, and smoother the exchange of information. Furthermore, the system of POCs would enhance the communication and confidence of the ministries that tend to be a bit overlooked, for instance, the Ministry of Culture or the Ministry of the Environment (MO representative, personal communication, 11 April 2022).

So, to set up new communication channels and personal networks between the public and private sectors, the **policy recommendations** are as follows:

(i.) introduce a similar "system of POCs" as in Norway—set up a point of contact at every ministry that would be responsible for communication and cooperation with the private companies within the given sector;

(ii.) improve the cooperation and communication both *inside* and *outside* the public sector by introducing a general catalogue of the public sector employees with their position, function and contact details.

Good Practice: Improve the dialogue between public authorities and private businesses

When improving and building trust between the public and private sectors, ongoing dialogue is essential. According to the Norwegian stakeholders, dialogue must be present in both meanings—as a conversation and formal talks between two parties. A good practice that could inspire others is the ad hoc forums held whenever new legislation is approved. Inviting private businesses to the table and sharing information largely contributes to mutual trust. It also enables the excellent outcomes of the institutions as everybody is part of the process of decision-making. Hence, this inclusive and whole-of-society approach may serve as a foundation for enhancing trust in society elsewhere.

The most efficient public-private cooperation tool is the National Cyber Security Forum (see more in chapter 4.1.6). The forum is beneficial mainly in three ways. Thanks to the forum, close collaboration between public and private actors is allowed. As the representatives meet at least three times a year, the contacts are intensive. Thanks to the meetings, private business representatives have a chance to establish relations with public authorities and vice versa. Secondly, the Forum serves as a meeting place to exchange information, know-how and experience. This helps to identify possible opportunities for collaboration and enforces the state's position as an

authority worth cooperating with. Thirdly, the Forum provides a space for dialogue, where the concerns might be raised and resolved right away. This improves joint trust and contributes to the feeling of reciprocity. According to private company representative #4, the existence of such a forum in the Czech environment would be beneficial. According to PCR #4, the cooperation between the representative's company and the public institutions works excellent primarily because of the representative's excellent personal contacts. PCR #4 affirmed that this is not a standard.

According to PCR #4, the existence of an official institutional instrument to deepen personal networks would be incredibly beneficial. PCR #4 also expressed interest in taking part in this Forum if it exists in the Czech Republic under the auspices of the Czech governmental bodies. According to PCR #4, such an instrument would help to increase joint trust between the public and private sectors (personal communication, 7 April 2022). Likewise, the MO and MPO representatives approved the author's findings from Norway and the Czech private businesses representatives. They agreed that such a forum in the Czech Republic would be an essential enhancement and a valuable tool for improving the dialogue, which is currently insufficient (personal communication, 11 April 2022 and 13 April 2022).

In addition, PCR #4 acquainted the author with the ISACA association, a body similar to the Forum introduced in the thesis. While the association is not coordinated from the state's position, it is a clear example that such a body is necessary for Czech companies to improve their ties with the public authorities. In Norway, dialogue is one of the main grounds to build trust in Norwegian society. Introducing such a

kind of forum (not only for cyber security but in other fields, too) in the Czech environment to enhance public-private cooperation may be one of the most efficient ways to improve trust in Czech society and among public and private actors. This was confirmed by the public and private sector representatives interviewed in the thesis.

Thus, to improve the dialogue between the public and private sectors, the **policy recommendations** are as follows:

(i.) set up a partnership forum ("Czech National Cyber Security Forum") under the auspices of the Ministry of Interior (that will comprise the public authorities, the business representatives, and academia;

(ii.) promote openness, trust and cooperation between public and private actors through the established forum;

(iii.) establish a dialogue through the new collaboration between the authorities at the ministerial level and between companies' representatives.

Good Practice: Initiate national cyber security exercises that would be of the whole-of-society type

Another interesting and valuable tool of public-private cooperation identified is the national cyber security exercises. Norwegian stakeholders from the government identified exercise as a crucial instrument for improving national resilience towards cyber/hybrid threats. The exercises enhance trust between the actors involved, but given the exercises themselves, they help private businesses and the government prepare for a crisis. The exercises are an excellent tool for

identifying gaps in security in a safe, "model" environment. Also, the private companies are of the same importance as the government, which also improves the trust of the private actors.

In Norway, private businesses are involved during all exercise phases, from planning to its execution. During the exercise itself, selected companies are in a "security room" with the government trying to find a solution. This clearly shows the government's level of trust in the private businesses the state shares its methods, procedures, and security information. Also noteworthy is that the exercises are not sector-specific organised; quite the contrary. During a crisis scenario, companies across the sectors are invited to participate in simulating as "real" environment as possible. Cyber exercises in the Czech Republic are sector-specific, so companies from the energy sector do not train to cooperate with companies in the communications sector. This is a significant shortage that could be easily remedied, though.

According to private company representative #4, the company did not participate in any of the exercises as it was not invited. It even was not aware of particular exercises within the area of transportation (personal communication, 7 April 2022). The only more extensive publicly covered exercise was the one organised by the Ministry of Defence for the strategic companies for the defence of the Czech Republic. This initiative is meaningful and praiseworthy, yet the exercises should be centrally organised—or at least NÚKIB or other public authorities should coordinate the ministries.

According to the MV representative, the Ministry of Interior would be eager to organise more exercises (while cooperating with NÚKIB). Nevertheless, there is a concern with joint cooperation at three levels:

(i.) cooperation *inside* of the ministry, (ii.) cooperation *between* ministries, and (iii.) cooperation between ministries *and* private businesses. So, to make the exercises a whole-of-society activity, the Czech Republic must start with the exercises at the highest level, inside the ministry and government. These exercises would improve the trust and personal networks necessary to proceed with the cooperation to the next level. The table below outlines the three "levels of exercises" to improve the cooperation inside the public sector and consequently achieve an enhanced level of public-private cooperation. At the first and second levels, the highest political presence is essential during the exercises at the ministry/between ministries. To make the exercises work, they must be attended by the ministers of the given ministries and at least some of their deputy ministers (MV representative, personal communication, 14 April 2022). The practice from Norway showed that this is the best way to improve cooperation and trust inside the public bodies. According to the JD representative, in Norway, the exercises were commenced at the highest level within the state (ministers and prime minister took part). That was a perfect case of "leading by example", which contributed to improved communication and trust that smoothed public-private cooperation (personal communication, 14 March 2022).

First level		Second level		Third level
Exercise at the ministerial level	→	Exercise at the ministry + ministry level	→	Exercise at the ministries + private sector level

Table 6: Three levels of starting the exercises in the Czech conditions
Source: Author's Findings

Thus, to initiate national cyber security exercises that would be of the whole-of-society type, the **policy recommendations** are as follows:

(i.) start with the exercises at the very top level—inside of the ministry at the present of the minister;

(ii.) allocate enough finances to organise the cross-sectoral exercises themselves and to fill the security gaps revealed during the exercise;

(iii.) proceed to organise exercises between ministries and private actors while responsibility is held the Ministry of Interior.

5.3 How to Improve Partnerships

Given the size and population of Norway and the Czech Republic, partnerships are crucial to ensure security. For both countries, membership in NATO is a cornerstone of security. However, both Norway and Czechia are members of other regional and international organisations. Norway is actively supporting EU-NATO cooperation (despite not being an EU member) and takes part in the "Centre of Excellence for Countering Hybrid Threats" (Hybrid CoE) in Helsinki. It is also a member of the Organization for Security and Cooperation in Europe (OSCE) and the International Telecommunications Union (ITU). As for the regional cooperation, it is a member of NORDEFCO. The Czech Republic is a member of the NATO and EU, Hybrid CoE, OSCE and ITU. Furthermore, it takes part in a regional alliance Visegrad Four (V4), whose purpose is outdated and questionable nowadays.

Most of the hybrid threats—and cyber threats, in particular—are inherently transborder, so their handling requires domestic and international partnerships. In Norway, regional, international, and public-private

cooperation is essential. International cooperation is carried out primarily through NATO. Regional cooperation is rooted in the NORDEFCO, an alliance for defence cooperation. Domestic partnerships are developed through the Norwegian Business & Industry Security Council (NSR). While collaboration is working well in Norway, the Czech Republic has a significant advantage here: the European Union (MZV representative, 21 April 2022).

Good Practice: Deepen international cooperation with like-minded countries

Several Czech interviewees called for greater regional cooperation to enable an exchange of information, resources, and a share of competencies and responsibility. International collaboration mainly focuses on the public authorities, yet private businesses may also profit from the partnership. According to the MZV representative, the Czech international cooperation is excellent, especially in the EU and NATO. In terms of cyber security, there is much higher eagerness to cooperate than in other domains. Hence, any collaboration is much easier. Also, according to the MZV representative, the cooperation does not necessarily need to be "regional", as the cyber/hybrid threats are inherently transborder (personal communication, 21 April 2022). In the case of Norway, the NORDEFCO cooperation works great because like-minded countries are cooperating within the alliance. In the Czech case — considering the growing disagreements within the V4—partnership with Canada, Australia, Japan, or South Korea makes much more sense than regional cooperation with countries that do not share the same strategic thinking. Another alternative could be the "Austerlitz format" (also "North-Trilateral" or "Slavkov Trilateral"), loose cooperation between the Czech Republic, Slovakia, and Austria. Nonetheless, according to the MZV representative, there are no proposals or

intentions to deepen defence / cyber security cooperation in this alliance (personal communication, 21 April 2022).

Yet, despite lacking regional cooperation, the Czech cooperation abroad is excellent. The Czech Republic has several cyber attachés that NÚKIB appoints. Also, collaboration inside the European Union is working well—which somewhat compensates for Norway's advantages from the NORDEFCO.

So, to conclude this part, the international cooperation is on a very decent level both in Norway and Czechia. Hence, in this case, Norway does not serve as an example for the Czech Republic, as the Czech Republic could also serve as a model for Norway. Besides that, international cooperation is an instrument of the public authorities and does not directly affect private companies. So, the level of international cooperation is not relevant as an instrument of public-private cooperation. Yet, it is interesting to compare the Czech and Norwegian cases.

Good Practice: Improve voluntary cooperation through the economic motivation

In Norway, private businesses are well-aware that cooperation with the state is necessary and beneficial. The capital invested in cybersecurity is worth the safety, as the potential losses caused by a cyber-attack would be much higher (which the case of the Norsk Hydro cyberattack in 2019 proved to be the correct assumption). According to private company representative #4, in the Czech Republic, the economic benefits of cybersecurity are not as straightforward as they are in Norway. Suppose the private company does not fall under the Cyber

Security Act. In that case, it usually does not care about cybersecurity until it is too late—usually because of the lack of finances that could be used better elsewhere (personal communication, 7 April 2022). According to private sector representative #4, the problem is also the return on investment in cybersecurity (personal communication, 8 April 2022). When a private company invests money into its cybersecurity, it is usually perceived as a cost with almost zero financial return. This is one of the most significant issues in the cyber defence of private businesses. Still, there are several good practices that the Norwegian example proved to work.

One of the best working examples is the Norwegian Business & Industry Security Council. The role and functioning of the NSR are parallel to the National Cyber Security Forum, but there are several significant differences. The NSR is privately funded, and every company can apply to become a member. It brings together private companies across the sector, public authorities, and academia. Through the joint discussions, networking events, workshops, and lectures on various topics (not only cyber security but also, e.g., personal safety, crime prevention, health, and safety, etc.), NSR facilitates cooperation across sectors and industries and promotes openness and trust. According to the interviewees, "the Czech Security Council" would be an interesting and valuable instrument to enhance public-private cooperation at several levels (personal communication, 11 April 2022, and 13 April 2022). Firstly, the Council would promote the cooperation of public authorities with private businesses and between the private actors together. This serves to improve personal networks and trust and facilitates dialogue. Secondly, by participating in the workshops and

discussions, the private companies improve their position in the market as they can get various certifications and awards. Lastly, the existence of such a council where private association provides a platform for cooperation between ministries, NÚKIB, private businesses and academia would improve the state's image as a capable and reliable partner worth cooperating with.

So, to improve the domestic partnerships and voluntary cooperation through the economic motivation, the **policy recommendation** is following:

(i.) set up a new private body that would be funded by private funding but closely cooperate with public authorities, especially NÚKIB.

Conclusion

This thesis aimed to examine the public-private cooperation in Norway and the Czech Republic and answer the main research question—*What instruments from Norway's approach to public-private cooperation can the Czech Republic implement to enhance national resilience towards hybrid threats?* Throughout the thesis, the author presented the data from the eighteen interviews conducted in Norway and the Czech Republic between February and April 2022. The data from the interviews were accompanied by an open-source analysis of the Norwegian and Czech strategic documents.

The first chapter presented the methodology and sources used to complete the thesis. The second chapter provided the reader with a literature review and presented the current state of research. It also introduced a theoretical framework used to sort and analyse the data. The third chapter examined the current state of public-private cooperation in the Czech Republic. The emphasis was put on identifying the gaps in achieving resilience towards cyber threats. The fourth chapter presented the Norwegian approach to public-private cooperation, focusing on the "lessons learned" from Norway. This chapter attempted to identify the mechanisms of *why* exactly public-private cooperation works in Norway. The fifth chapter applied the findings from previous chapters and synthesised them into several policy recommendations on how to enhance Czech resilience. Based on the theoretical framework introduced in subchapter 2.4, the policy recommendations were sorted into three categories: (i.) raising awareness, (ii.) building resilience, and (iii.) improving partnerships.

The main contribution of the thesis is two-fold: firstly, it presents a comprehensive analysis of the Norwegian cyber security environment based

on ten interviews with the Norwegian stakeholders. The interviews provided the author with data on countering cyber threats and building resilience. A descriptive case study of this type is unique in academia—while several Norwegian researchers focused on cooperation between key actors within the Norwegian cybersecurity apparatus (e.g., Gjesvik 2019 or Muller 2016), none of them investigated the aspect of public-private cooperation and its application to countering hybrid threats. Secondly, the large contribution of the thesis represents the extrapolation of the data to the Czech environment. Academic research on the current situation in the Czech Republic is insufficient, and the thesis is the first of its kind in the Czech academia to identify the shortcomings in public-private cooperation in terms of cyber/hybrid threats.[21] The author's analysis revealed several gaps in the Czech Republic, and the author proposes possible solutions inspired by the Norwegian experience. Based on the interviews conducted in the Czech Republic, the author concludes that the tools of public-private cooperation presented are desirable and feasible. Of the utmost interest and benefit are the crisis scenarios, the system of POCs, and the forum for cooperation between the public and private sectors.

In the thesis, the author focused only on cybersecurity as one domain of hybrid warfare (to achieve a certain deepness of the analysis). But, as the purpose of the thesis was to present recommendations to improve public-private cooperation to enhance *resilience*, most of the instruments presented are applicable in other dimensions of hybrid warfare. Especially the system of

[21] In 2021, Bahenský and Ditrych published two policy papers: "Finnish Model of Countering Hybrid Threats: Inspiration for the Czech Republic", and "Netherland's Model of Countering Hybrid Threats: Inspiration for the Czech Republic". While the authors do not focus specifically on the public-private cooperation, they evaluate the applicability of their findings in Finland and Netherlands to the Czech security policy and they propose policy recommendations.

POCs, crisis scenarios, a forum for cooperation and sharing of know-how and information, and national exercises are easily transferable to other security sectors, for instance, disinformation, economic pressure, and political interference. To implement these tools effectively, they should become the goals of the 15-point *Action Plan* following the *National Strategy for Countering Hybrid Interference*.

To provide an example, let us look more into disinformation. The system of POCs would work similarly as in the domain of cyber threats—only the POCs would be the communication/PR managers. Disinformation should be one of the chapters in the introduced "Crisis Scenarios" booklet. Also, the Ministry of Interior (mainly CTHH), NÚKIB, and the newly established "Strategic Communication Office" should work together with private businesses to organise the "National Security Forum on Communication". There could also be exercises on disinformation (either as part of the cyber security exercises or stand-alone). There are also dimensions of hybrid warfare where the instruments introduced in the thesis are near to unapplicable. These dimensions include, for instance, diplomatic pressure, election interference, or international sanctions. However, once again, the utmost goal of the presented recommendations is to enhance overall societal resilience toward hybrid threats. Hence, despite the instruments are not universally applicable to all the threats, they should serve for creating a resilient society—primarily by improving trust, communication, personal networks and enhancing shared strategic thinking.

The table on the next page outlines and summarises the recommendations sorted according to the three-pillar structure introduced at the beginning of this chapter.

End Goal	Policy Recommendation
	• Secure sufficient finances and support to bring attention to the cyberculture to make cybersecurity an attractive topic. • Improve the image of NÚKIB by representatives giving lectures, and lessons, organizing discussions and cooperating with private businesses. • Bring more attention to the National Cyber Awareness Month and make it truly an event based on public-private cooperation that brings together various stakeholders. • Improve the strategic communication of the public sector by enhancing shared strategic thinking (e.g., through direct cooperation and personal contacts); make the communication easy and understandable.
Awareness	• The Office of the Government of the Czech Republic should establish Strategic Communication Office directly under its auspices; this Office should serve as a governing body of the public authorities' strategic communication. • Continuously enforce cyberculture to achieve shared strategic thinking in the society (use the recommendations above on cyberculture). • Use the already existing standard operating procedures by IZS to prepare real-life scenarios inspired by the DSB Crisis Scenarios publication; update the scenarios, the responsible subjects, and the processes every year; and use the scenarios for the state-organised exercises (not only in the field of cyber security but also for other (hybrid) threats).
Resilience	• Introduce a similar "system of POCs" as in Norway—set up a point of contact at every ministry that would be responsible for communication and cooperation with the private companies within the given sector. • Improve the cooperation and communication both *inside* and *outside* of the public sector by introducing a public catalogue of the public sector employees with their position, function, and contact details.

	• Improve the dialogue between public authorities and private businesses. Set up a new partnership forum ("Czech National Cyber Security Forum") where representatives from the private and public sector may meet and exchange information and know-how; promote openness, trust and cooperation between public and private actors through the established forum. • Start national cyber security exercises that are sector-specific and those where the companies across the industries may meet and cooperate; start with the exercises at the very top level—governmental and ministerial. • Allocate enough finances to organise the cross-sectoral exercises themselves, and to fill the security gaps revealed during the exercise.
Partnerships	• Deepen cooperation with the like-minded countries to exchange information. • Set up a new body independent from the government (i.e., privately funded) responsible for the cooperation between public authorities and private businesses; representing a hub for cooperation, networking, exchange of information, know-how and expertise.

Table 7: Policy Recommendations Summary
Source: Author's findings

It is important to note that several of the recommendations would not work separately (e.g., shared strategic thinking or the system of POCs cannot work without enhanced cyberculture or strategic communication). Rather, these instruments work the best when supported and complemented by each other. Building resilience in society is a long haul and requires joint efforts of all parts of society. It is also an intertwined process where it is difficult to determine a start point and an endpoint of the efforts. Yet, in the thesis, the author attempted to identify critical instruments that enhanced Norwegian resilience through public-private cooperation and might also work in the Czech environment.

The underlying difference between the Czech and Norwegian approach is that in Norway, public-private cooperation is based on the broader concepts of total defence and the whole-of-society approach that permeate all the strategic documents and every effort by the public sector. In the Czech Republic, the public and private sector relationship is more regulatory based—the state imposes obligations, and the private companies follow them. But it is not a partnership. In Norway, we can talk about a proper horizontal relationship between the public and private sectors, where both segments are partners.

It is also necessary to note that the Czech Republic has somehow functioning structures and mechanisms. On these, it is possible to build up in order to enhance its resilience (e.g., the crisis scenarios, the cyber exercises, the cyber security month). Yet there will be a need to start building some of the recommended instruments and mechanisms from scratch, especially the strategic communication, the system of POCs, or a public catalogue of the contacts of the public sector employees.

The initially ambitious goal of the thesis (i.e., to identify the overall strategy to counter hybrid threats) leaves generous space for future research. To further support the author's findings, a quantitative analysis based on a large-scale survey of the private companies in Norway and Czechia would be beneficial. Also, in the thesis, the author only focused only on one aspect of hybrid warfare. The results provoke questions about the feasibility of implementing the introduced recommendations—and the Norwegian model of public-private cooperation—into other dimensions of countering hybrid threats. Hence, in Czech academia, this thesis may serve as a first swallow in the efforts to present a coherent strategy to build resilience through public-private cooperation.

To conclude, Norwegian approach to the public-private cooperation incorporated in the concept of total defence is an inspiring example of building national resilience. While Norwegian cultural and historical experience is slightly different, all the good practices identified in the thesis are transmittable to the Czech environment—as the interviews with the public and private sector stakeholders proved. What's more, the good practices identified are not only feasible but also desirable from the side of the private companies to improve cooperation and trust. In the end, the whole-of-society approach based on trust, shared strategic thinking, cooperation, information flow and efficient institutional measures reveals the best approach to achieve societal resilience towards hybrid threats. While there is still a long way ahead, the Czech Republic has a vast potential to implement more public-private cooperation instruments at feasible costs. If doing so, the Czech Republic could get to the forefront of the countries successful in countering cyber threats in Europe.

Bibliography

Anon., 2015. *Security Strategy of the Czech Republic*, Prague: Ministry of Foreign Affairs of the Czech Republic. Available at: https://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf

Anon., 2021. National Strategy for Countering Hybrid Interference. Prague: Ministry of Defence of the Czech Republic. Available at: https://www.mocr.army.cz/assets/informacni-servis/zpravodajstvi/national-strategy---aj-final.pdf

Bahenský, V., O. Ditrych., 2021. Nizozemský model čelení hybridnímu působení: inspirace pro Českou republiku. Ústav mezinárodních vztahů [online]. Prague: 7.6.2021. [cit. 2021-10-02]. Available at: https://www.iir.cz/nizozemsky-model-celeni-hybridnimu-pusobeni-inspirace-pro-ceskou-republiku

Bezpečnostní informační služba, 2021. *Annual Report for 2020*, Security Information Service. Available at: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/ar2020en-2.pdf.

Black, J., *et al*. 2020. Enhancing deterrence and defence on NATO's northern flank: Allied perspectives on strategic options for Norway. *RAND Corporation*. Available at: https://doi.org/10.7249/RR4381 [Accessed February 1, 2022].

Boin, A. & McConnell, A., 2007. Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. *Journal of Contingencies and Crisis Management*, 15(1), pp.50-59. Available at: https://onlinelibrary.wiley.com/doi/10.1111/j.1468-5973.2007.00504.x

Braw, E., 2021. Commentary: Everyone together now: Creating a resilient society in an age of cyber threats. Macdonald-Laurier Institute: Ottawa, Ontario, p. 1-18. Available at: https://macdonaldlaurier.ca/files/pdf/20210601_Everyone_together_now_Braw_COMMENTARY_FWeb.pdf

Breedlove, M., 2015. Foreword. In G. Lasconjarias & J. Larsen, eds. *NATO's Response to Hybrid Threats*. Rome: NATO Defense College, p. xxi-xxv.

Brown, J. et al., 2021. Building resilience through cooperation: Two case studies. *Learned Publishing*, 34(1), pp.25-29. Available at: https://doi.org/10.1002/leap.1354 [Accessed April 19, 2022].

Caliskan, M. & Liégeois, M., 2020. The concept of 'hybrid warfare' undermines NATO's strategic thinking: insights from interviews with NATO officials. *Small Wars & Insurgencies*, 32(2), pp.295-319. Available at: https://doi.org/10.1080/09592318.2020.1860374 [Accessed April 10, 2022].

Caliskan, M., 2019. Hybrid warfare through the lens of strategic theory. *Defense & Security Analysis*, 35(1), pp.40–58. Available at: https://doi.org/10.1080/14751798.2019.1565364 [Accessed February 1, 2022].

Carr, M., 2016. Public–private partnerships in national cyber-security strategies. *International Affairs*, 92(1), pp.43-62. Available at: https://doi.org/10.1111/1468-2346.12504 [Accessed April 19, 2022].

Cordesman, A.H. & Hwang, H., 2020. Chronology of Possible Russian Gray Area and Hybrid Warfare Operations, *Center for Strategic and International Studies (CSIS)*. Available at: https://www.jstor.org/stable/resrep24779 [Accessed February 1, 2022].

Cox, D.G., Bruscino, T. & Ryan, A., 2012. Why Hybrid Warfare is Tactics Not Strategy: A Rejoinder to "Future Threats and Strategic Thinking". *Infinity Journal,*, 2(2), pp.25-29. Available at: https://www.militarystrategymagazine.com/article/why-hybrid-warfare-is-tactics-not-strategy-a-rejoinder-to-future-threats-and-strategic-thinking/ [Accessed April 7, 2022].

Crisis Management Act N. 240/2000 Coll. (Crisis Act), 2000. Available at: https://www.hzscr.cz/hasicien/file/crisis-management-act-n-240-2000-coll-pdf.aspx.

Daniel, J. & Eberle, J., 2018. Hybrid Warriors: Transforming Czech Security through the 'Russian Hybrid Warfare' Assemblage. *Czech Sociological Review*, 54(6), pp.907–931. Available at: https://doi.org/10.13060/00380288.2018.54.6.435 [Accessed February 1, 2022].

Danish Ministry of Defence, 2020. *NORDEFCO Annual Report 2020*, Copenhagen: Danish Ministry of Defence. Available at:

https://www.nordefco.org/files/NORDEFCO-annual-report-2020.pdf.

Danyk, Y., Briggs, C. & Maliarchuk, T., 2017. Hybrid War: High-tech, Information and Cyber Conflicts. *Connections: The Quarterly Journal*, 16(2), pp.5-24. Available at: http://connections-qj.org/article/hybrid-war-high-tech-information-and-cyber-conflicts [Accessed February 1, 2022].

Daskalov, K., 2018. Hybrid Warfare and the Challenge It Poses to the Psychological Resilience Training in the Bulgarian Military. *Information & Security: An International Journal,* 39(3), pp.197-205. Available at: https://doi.org/10.11610/isij.3917

Dowse, A., S. Bachmann, 2019. Explainer: what is 'hybrid warfare' and what is meant by the 'grey zone'? The Conservation [online]. June 17, 2019. [cit. 2021-08-28]. Available at: https://theconversation.com/explainer-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone-118841

DSB, 2012. *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring*, Tønsberg: Direktoratet for samfunnssikkerhet og beredskap. Available at: https://www.dsb.no/globalassets/dokumenter/rapporter/sikkerhet-i-kritisk-infrastruktur.pdf.

DSB, 2016. *Samfunnets kritiske funksjoner: Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* Versjon 1.0., Tønsberg: Direktoratet for samfunnssikkerhet og beredskap. Available at: https://www.dsb.no/globalassets/dokumenter/rapporter/sikkerhet-i-kritisk-infrastruktur.pdf.

DSB, 2022. Om DSB: Direktoratet for samfunnssikkerhet og beredskap. Available at: https://www.dsb.no/menyartikler/om-dsb/ [Accessed March 1, 2022].

Edwards, R. & Holland, J., 2013. What is Qualitative Interviewing?. *Qualitative Research*, 15(4), pp.540-542. Available at: https://doi.org/10.1177%2F1468794114535040 [Accessed April 10, 2022].

European Commission, 2016. FAQ: Joint Framework on countering hybrid threats. *European Commission*. Available at:

https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250 [Accessed April 10, 2022].

European Commission, 2016. *Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats a European Union Response*, Brussels: European Commission. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

European Parliament, 2021. *Best Practices in the whole-of-society approach in countering hybrid threats*, Brussels: European Union. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf [Accessed April 7, 2022].

Fägersten, B., 2016. Forward Resilience in the Age of Hybrid Threats: The Role of European Intelligence. In *Forward Resilience: Protecting Society in an Interconnected World*. Washington, DC: Center for Transatlantic Relations, pp. 113-126.

Forsberg, T., 2013. The rise of Nordic defence cooperation: a return to regionalism?. *International Affairs*, 89(5), pp.1161–1181. Available at: https://doi.org/10.1111/1468-2346.12065 [Accessed February 1, 2022].

Giegerich, B., 2016. Hybrid Warfare and the Changing Character of Conflict. *Connections: The Quarterly Journal*, 15(2), pp.65-72. Available at: https://connections-qj.org/article/hybrid-warfare-and-changing-character-conflict [Accessed February 1, 2022].

Givens, A.D. & Busch, N.E., 2013. Realising the promise of public-private partnerships in U.S. critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, 6(1), pp.39-50. Available at: https://doi.org/10.1016/j.ijcip.2013.02.002 [Accessed February 6, 2022].

Gjesvik, L., 2021. Norwegian Cybersecurity: A small-state approach to building international cyber cooperation. In *Routledge Companion to Global Cyber-Security Strategy*. London: Routledge, pp. 143-152.

Haavik, T., 2020. Societal resilience – Clarifying the concept and upscaling the scope. *Safety Science*, 132, pp.2-7. Available at: https://doi.org/10.1016/j.ssci.2020.104964 [Accessed February 1, 2022].

Hagelstam, A., 2018. Cooperating to counter hybrid threats. *NATO Review*. Available at: https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html [Accessed February 1, 2022].

Hallahan, K. et. Al., 2007. Defining Strategic Communication. *International Journal of Strategic Communication*, 1(1), pp.3-35. Available at: https://doi.org/10.1080/15531180701285244 [Accessed April 29, 2022].

Halloran, R., 2007. Strategic Communication. *The US Army War College Quarterly: Parameters*, 37(3), pp.3-14. Available at: https://press.armywarcollege.edu/parameters/vol37/iss3/18/ [Accessed April 29, 2022].

Halvorsen, A., 2020. Statement at seminar on influence operations. *Government.no*. Available at: https://www.regjeringen.no/en/aktuelt/innlegg-pa-seminar-om-pavirkningsoperasjoner/id2690513/ [Accessed April 10, 2022].

Hammond-Errey, M., 2019. Understanding and Assessing Information Influence and Foreign Interference. *Journal of Information Warfare*, 18(1), pp.1–22. Available at: https://www.jstor.org/stable/26894654 [Accessed February 1, 2022].

Hanisch, M., 2016. What is Resilience? Ambiguities of a Key Term. *Bundesakademie für Sicherheitspolitik*, Security Policy Working Paper, no. 19, pp.1-4. Available at: https://www.baks.bund.de/sites/baks010/files/working_paper_2016_19.pdf [Accessed April 7, 2022].

Hartmann, U., 2017. The Evolution of the Hybrid Threat, and Resilience as a Countermeasure. *NATO Defense College*, 139, pp.1-8. Available at: https://www.ndc.nato.int/news/news.php?icode=1083 [Accessed April 10, 2022].

Havlík, M., 2020. Jak daleko má svět k dosažení světového míru a proč?. *Vojenské rozhledy*, 29(3), pp.2336-2995. Available at: https://www.vojenskerozhledy.cz/en/kategorie-clanku/bezpecnostni-prostredi/dosazeni-svetoveho-miru [Accessed April 10, 2022].

Hoffman, F., 2009. "Hybrid vs. compound war. The Janus choice: Defining today's multifaceted conflict," *Armed Forces Journal*, October 1, 2009. Available at: http://armedforcesjournal.com/hybrid-vs-compound-war/.

Hoffman, F., 2009. Hybrid Warfare and Challenges. *Small Wars Journal*. Vol. 51, No. 1, pp. 34-39. Available at: https://smallwarsjournal.com/documents/jfqhoffman.pdf.

Hoffman, F., 2018. Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges. *PRISM: National Defense University. The Journal of Complex Operations*, Vol. 7, No. 4, pp. 30-47. Available at: https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/

Hoffman, F.G. & Mattis, J.N., 2005. Future Warfare: The Rise of Hybrid Wars. *Proceedings Magazine*, 132(11). Available at: http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf [Accessed February 1, 2022].

Hsieh, H., 2005. Three Approaches to Qualitative Content Analysis. *Qualitative Health Research,* Vol. 15, No, 9, pp. 1277–1288. Available at: https://doi.org/10.1177/1049732305276687

Hybrid CoE, (no date). COI Hybrid Influence. *Hybrid CoE*. Available at: https://www.hybridcoe.fi/coi-hybrid-influencing/ [Accessed February 1, 2022].

Hybrid CoE, 2022. What is Hybrid CoE?. *Hybrid CoE: European Centre of Excellence for Countering Hybrid Threats*. Available at: https://www.hybridcoe.fi/who-what-and-how/ [Accessed April 10, 2022].

Chivvis, C., 2017. *Understanding Russian "Hybrid Warfare" And What Can Be Done About It: Testimony presented before the House Armed Services Committee on March 22, 2017.* California: RAND Corporation. Available at: https://doi.org/10.7249/CT468.

Ilbiz, E. & Kaunert, C., 2021. Cyber-attacks: what is hybrid warfare and why is it such a threat?. Available at: https://theconversation.com/cyber-attacks-what-is-hybrid-warfare-and-why-is-it-such-a-threat-164091 [Accessed February 1, 2022].

ITU, 2021. Global Cybersecurity Index 2020 1st ed., Geneva: International Telecommunication Union. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf [Accessed April 7, 2022].

IZS ČR, 2022. Dokumentace IZS. *Hasičský záchranný sbor České republiky*. Available at: https://www.hzscr.cz/clanek/dokumentace-izs-587832.aspx [Accessed April 7, 2022].

J. Garriaud-Maylam, 2021. *Enhancing the Resilience of Allied Societies Through Civil Preparedness: Preliminary Draft General Report*, Brussels: NATO. Available at: https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-04/011%20CDS%2021%20E-%20RESILIENCE%20THROUGH%20CIVIL%20PREPAREDNESS_0.pdf.

Kallio H. et al., 2016. Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*. Vol. 72, No. 12, pp. 2954-2965. Available at: https://doi.org/10.1111/jan.13031.

Keck, M. & Sakdapolrak, P., 2013. What is Social Resilience? Lessons Learned and Ways Forward. *Erdkunde*, 67(1), pp.5-19. Available at: http://www.jstor.org/stable/23595352 [Accessed April 10, 2022].

Kobzeva, M. & Konyshev, V., 2017. China's policy in the Arctic: tradition and modernity. *Comparative Politics Russia*, 8(1), pp.77-92. Available at: https://doi.org/10.18611/2221-3279-2017-8-1-77-92 [Accessed February 1, 2022].

Lenton, T.M., Boulton, C.A. & Scheffer, M., 2022. Resilience of countries to COVID-19 correlated with trust. *Scientific Reports*, 12(75), pp.1-12. Available at: https://doi.org/10.1038/s41598-021-03358-w [Accessed March 24, 2022].

Liégeois, M., 2021. The concept of 'hybrid warfare' undermines NATO's strategic thinking: insights from interviews with NATO officials. *Small Wars & Insurgencies*, 32(2), pp.295-319. Available at: https://doi.org/10.1080/09592318.2020.1860374 [Accessed February 1, 2022].

Linder, S.H., 1999. Coming to terms with the public–private partnership: a grammar of multiple meanings. *American Behavioral Scientist*, 43(1), pp.35-51. Available at: https://doi.org/10.1177%2F00027649921955146 [Accessed April 19, 2022].

Lothar, M., 1974. Reflections on the Soviet Secret Police and Intelligence Services. *Orbis: A Quarterly Journal of World Affairs*, 18(3), p.921.

Mansoor, P.R., 2012. Hybrid War in History, in Hyb*rid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, ed. Williamson Murray and Peter R. Mansoor. Cambridge: Cambridge University Press.

Marginson, D. 2004. *The Case Study, The Interview and The Issues: A Personal Reflection* in Humphrey, Lee (eds.), *The Real Life Guide To Accounting Research.* United Kingdom: Elsevier, pp. 325-338. Available at:

Masters, J., 2018. NATO's Trident Juncture Exercises: What to Know. *Council on Foreign Relations.* Available at: https://www.cfr.org/in-brief/natos-trident-juncture-exercises-what-know [Accessed February 4, 2022].

Mayring, P., 2007. *Qualitative Content Analysis* in Flick, Uwe, Kardorff, Ernst von, Steinke (eds.), *A Companion to Qualitative Research*. Reinbek: SAGE Publications, pp. 266-269.

Metzl, L., 1974. Reflections on the Soviet Secret Police and Intelligence Services. *Orbis*, 18(3), p.921.

Ministry of Defence of the Russian Federation, 2019. *Russian Federation Armed Forces' Information Space Activities Concept*, Ministry of Defence of the Russian Federation. Available at: https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle.

Ministry of Defence, 2021a. *National Strategy for Countering Hybrid Interference*, Prague: Ministry of Defence. Available at:

https://www.army.cz/assets/en/ministry-of-defence/basic-documents/national-strategy---aj-final.pdf.

Ministry of Defence, 2021b. *Action Plan for National Strategy for Countering Hybrid Interference*, Prague: Ministry of Defence. Available at: https://mocr.army.cz/images/id_40001_50000/46088/app_2022.pdf

Ministry of Interior, 2018. *National Security Audit*, Praha: Ministerstvo vnitra České republiky. Available at: https://www.mvcr.cz/cthh/clanek/audit-narodni-bezpecnosti.aspx.

Ministry of Interior, 2021. Centre Against Terrorism and Hybrid Threats. *Ministerstvo vnitra České republiky*. Available at: https://www.mvcr.cz/cthh/clanek/centre-against-terrorism-and-hybrid-threats.aspx [Accessed February 1, 2022].

Møller, J.E., 2019. Trilateral defence cooperation in the North: an assessment of interoperability between Norway, Sweden and Finland. *Defence Studies*, 19(3), pp.235-256. Available at: https://doi.org/10.1080/14702436.2019.1634473 [Accessed February 1, 2022].

Monaghan, S., 2019. Countering Hybrid Warfare So What for the Future Joint Force?. Prism, 8(2), pp.83-95. Available at: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM%208-2.pdf?ver=2019-10-28-122747-047 [Accessed April 7, 2022].

Muller, L. P., 2016. Makt og avmakt i cyberspace: hvordan styre det digitale rom?. *Internasjonal Politikk*, *74*(4), pp.1-23. https://doi.org/10.17585/ip.v74.428

Murray, W. & Mansoor, P.R., 2012. *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge: Cambridge University Press.

Næringslivets sikkerhetsråd, 2021. Nasjonalt cybersikkerhetssenter (NCSC). *Næringslivets sikkerhetsråd*. Available at: https://www.nsr-org.no/om-nsr/nasjonalt-cybersikkerhetssenter-ncsc [Accessed February 28, 2022].

Næringslivets sikkerhetsråd, 2022a. Om NSR. *Næringslivets sikkerhetsråd*. Available at: https://www.nsr-org.no/om-nsr [Accessed February 28, 2022].

Næringslivets sikkerhetsråd, 2022b. Medlemmer. *Næringslivets sikkerhetsråd*. Available at: https://www.nsr-org.no/om-nsr/medlemmer [Accessed February 28, 2022].

NATO, 2020. *Science & Technology Trends 2020-2040: Exploring the S&T Edge*, Brussels: NATO Science & Technology Organization. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

NATO, 2021. NATO's response to hybrid threats. *North Atlantic Treaty Organization*. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm [Accessed April 10, 2022].

NATO, Resilience and Article 3. *North Atlantic Treaty Organization*. Available at: https://www.nato.int/cps/en/natohq/topics_132722.htm [Accessed February 1, 2022].

NATO's response to hybrid threats, 2021. *North Atlantic Treaty Organization* [online]. March 16, 2021. [cit. 2021-08-28]. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm

NBÚ, 2015a. *Národní strategie kybernetické bezpečnosti ČR 2015-2020*, Národní centrum kybernetické bezpečnosti. Available at: https://www.databaze-strategie.cz/cz/cr/strategie/narodni-strategie-kyberneticke-bezpecnosti-cr-na-obdobi-let-2015-az-2020?typ=o.

NBÚ, 2015b. *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020*, Národní centrum kybernetické bezpečnosti. Available at: https://www.databaze-strategie.cz/cz/cr/strategie/akcni-plan-narodni-strategie-kyberneticke-bezpecnosti-cr-2015-2020?typ=download.

NBÚ, 2019. *Typový plán: Typ krizové situace: Narušení bezpečnosti informací kritické informační infrastruktury*, Praha: Národní bezpečnostní úřad. Available at: https://www.hzscr.cz/soubor/635-priloha-c4-pdf.aspx.

Nilsen, H.T., 2018a. Felles og helt, ikke stykkevis og delt. *Telenor Norge*. Available at: https://www.telenor.no/om/digital-sikkerhet/forord.jsp [Accessed March 7, 2022].

Nilsen, H.T., 2018b. Økt kapasitet og beredskap under Nato-øvelsen: Pressemelding. *Telenor Norge*. Available at: https://www.mynewsdesk.com/no/telenor/pressreleases/oekt-kapasitet-og-beredskap-under-nato-oevelsen-2692513 [Accessed March 7, 2022].

NIS, 2021. *Focus 2021*, Norwegian Intelligence Service. Available at: https://www.forsvaret.no/en/organisation/norwegian-intelligence-service/focus/Focus2021-english.pdf/_/attachment/inline/a437a870-375e-4b4b-a007-b8c4492e4f9a:21c5241a06c489fa1608472c3c8ab855c0ac3511/Focus2021-english.pdf.

NKÚ, 2020. *Kontrolní závěr z kontrolní akce 19/26: Budování kybernetické bezpečnosti České republiky: Tisková zpráva ke KA č. 19/26 – 2. 11. 2020*, Nejvyšší kontrolní úřad. Available at: https://www.nku.cz/cz/pro-media/tiskove-zpravy/kyberneticka-bezpecnost-v-cr:-stat-ma-pred-sebou-radu-vyzev--jejich-podcenovani-muze-mit-v-budoucnu-vazne-dopady-id11523/.

Noble, H., R. Heale. 2019. Triangulation in research, with examples. *Evidence-Based Nursing*, Vol. 22, No. 3, pp. 67-68. Available at: https://ebn.bmj.com/content/ebnurs/22/3/67.full.pdf

NorSIS, 2021a. Om NorSIS. *Norsk senter for informasjonssikring (NorSIS)*. Available at: https://norsis.no/om-norsis/ [Accessed February 8, 2022].

NorSIS, 2021b. Øk bevisstheten om cybertrusler: European Cybersecurity Month 2021. *Norsk senter for informasjonssikring (NorSIS)*. Available at: https://norsis.no/ok-bevisstheten-om-cybertrusler-european-cybersecurity-month-2021/

Norwegian Ministeries, 2007. *National Guidelines on Information Security 2007 – 2010*, Oslo: Norwegian Ministry of Government Administration and Reform. Available at: https://www.oecd.org/norway/41671072.pdf [Accessed April 7, 2022].

Norwegian Ministeries, 2019a. *National Cyber Security Strategy for Norway*, Available at: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf [Accessed 7 February, 2022].

Norwegian Ministeries, 2019b. *List of measures – National Cyber Security Strategy for Norway*, Available at: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/list-of-measures--national-cyber-security-strategy-for-norway.pdf [Accessed 7 February, 2022].

Norwegian Ministry of Defence Norwegian and Ministry of Justice and Public Security, 2018. *Support and Cooperation: A description of Norway's total defence*, Norwegian Ministry of Defence Norwegian and Ministry of Justice and Public Security. Available at: https://www.regjeringen.no/contentassets/5a9bd774183b4d548e33da101e7f7d43/support-and-cooperation.pdf.

Norwegian Ministry of Defence, 2020. *The Defence of Norway: Long Term Defence Plan 2020*, Norwegian Ministry of Defence. Available at: https://www.regjeringen.no/contentassets/7d48f0e5213d48b9a0b8e100c608bfce/long-term-defence-plan-norway-2020---english-summary.pdf.

Norwegian Ministry of Justice and Public Security, 2017. *Risk in a Safe and Secure Society On Public Security: Meld. St. 10 (2016–2017) Report to the Storting (white paper)*, Norwegian Ministry of Justice and Public Security. Available at: https://www.regjeringen.no/contentassets/00765f92310a433b8a7fc0d49187476f/en-gb/sved/stm201620170010000engpdfs.pdf.

Norwegian National Security Authority, 2021. Norwegian National Cyber Security Centre (NCSC) and NorCERT. Nasjonal sikkerhetsmyndighet (NSM). Available at: https://nsm.no/areas-of-expertise/cyber-security/norwegian-national-cyber-security-centre-ncsc/ [Accessed February 8, 2022].

NÚKIB, 2020a. Národní strategie kybernetické bezpečnosti ČR 2021-2025, Brno: Národní úřad pro kybernetickou a informační bezpečnost. Available at: https://www.databaze-strategie.cz/cz/cr/strategie/narodni-strategie-kyberneticke-bezpecnosti-cr-2021-2025?typ=download.

NÚKIB, 2020b. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019*, Brno: Národní úřad pro kybernetickou bezpečnost. Available at:

https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019_verze-pro-tisk.pdf.

NÚKIB, 2020c. *Bezpečnostní role a jejich začlenění v organizaci*, Brno: Národní úřad pro informační a kybernetickou bezpečnost. Available at: https://nukib.cz/download/publikace/podpurne_materialy/bezpečnostn%C3%AD-role_v3.pdf.

NÚKIB, 2021a. About NÚKIB. *National Cyber and Information Security Agency*. Available at: https://www.nukib.cz/en/about-nukib/ [Accessed March 8, 2022].

NÚKIB, 2021b. *Akční plán Národní strategie kybernetické bezpečnosti ČR 2021-2025*, Národní úřad pro kybernetickou a informační bezpečnost. Available at: https://www.databaze-strategie.cz/cz/cr/strategie/akcni-plan-narodni-strategie-kyberneticke-bezpecnosti-cr-2021-2025?typ=download.

NÚKIB, 2021c. Jsme součástí Evropského měsíce kybernetické bezpečnosti 2021. *Národní úřad pro kybernetickou a informační bezpečnost*. Available at: https://www.nukib.cz/cs/infoservis/aktuality/1753-jsme-soucasti-evropskeho-mesice-kyberneticke-bezpecnosti-2021 [Accessed April 7, 2022].

NÚKIB, 2022. Exercises Types. *National Cyber and Information Security Agency*. Available at: https://nukib.cz/en/cyber-security/exercises/exercise-types/ [Accessed May 3, 2022].

OECD, 2012. Recommendation of the Council on Principles for Public Governance of Public-Private Partnerships, https://www.oecd.org/governance/budgeting/PPP-Recommendation.pdf.

Olsen, O.E., Kruke, B.I. & Hovden, J., 2007. Societal Safety: Concept, Borders and Dilemmas. *Journal of Contingencies and Crisis Management*, 15(2), pp.69-79. Available at: https://doi.org/10.1111/j.1468-5973.2007.00509.x [Accessed April 10, 2022].

Ovelse.no, 2021. Om ovelse.no. *Ovelse.no*. Available at: https://ovelse.no/about [Accessed March 15, 2022].

Oxfam, 2017. *The Future is Choice: Absorb, Adapt, Transform*, Oxford: Oxfam International. Available at:

https://oxfamilibrary.openrepository.com/bitstream/handle/10546/620178/gd-resilience-capacities-absorb-adapt-transform-250117-en.pdf;jsessionid=660932421B9CCCFF3039BF5C12D6EE4C?sequence=4.

Paul, C., 2016. Confessions of a Hybrid Warfare Skeptic: What Might Really Be Interesting but Hidden Within the Various Conceptions of Gray Zone Conflict, Ambiguous Warfare, Political Warfare, and Their Ilk. *Small Wars Journal*. Available at: https://smallwarsjournal.com/jrnl/art/confessions-of-a-hybrid-warfare-skeptic [Accessed April 10, 2022].

Permanent Delegation of Norway to NATO, 2017. *Government launches international cyber strategy*, Press Release. Available at: https://www.norway.no/en/missions/nato/norway-nato/news-events-statements/government-launches-international-cyber-strategy/.

Pronk, D., 2019. The case of Norway. In *Witnesses to Change: Defence Transformation in Comparative Perspective*. Clingendael Institute, pp. 11-14. Available at: https://www.jstor.org/stable/resrep21417.7 [Accessed February 7, 2022].

Pursiainen, C., 2018. Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction*. Vol. 27, pp. 632-641. Available at: http://dx.doi.org/10.1016/j.ijdrr.2017.08.006

Puyvelde, D.V., 2015. Hybrid war – does it even exist?. *NATO Review*. Available at: https://www.nato.int/docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/index.html [Accessed April 10, 2022].

Qureshi, W., The Rise of Hybrid Warfare. *Notre Dame Journal of International & Comparative Law*, 10(2), pp. 174-205. Available at: https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1124&context=ndjicl [Accessed February 1, 2022].

Reichborn-Kjennerud E. & P. Cullen, 2016. What is Hybrid Warfare? *Norwegian Institute for International Affairs (NUPI)*. Policy Brief 1/2016, part of the Multinational Capabilities

Development Campaign (MCDC) project Countering Hybrid Warfare (CHW) funded by the Norwegian Ministry of Defence. Available at: http://www.jstor.com/stable/resrep07978.

Riste, O., 2005. *Norway's Foreign Relations – A History*. Oslo: Universitetsforlaget.

Rühle, M., 2019. Deterring hybrid threats: the need for a more rational debate. *NATO Defense College*, 15, pp. 2-4. Available at: https://www.jstor.org/stable/resrep19846 [Accessed April 10, 2022].

Schmidt, C., 2007. *The Analysis of Semi-structured Interviews* in Flick, Uwe, Kardorff, Ernst von, Steinke (eds.), *A Companion to Qualitative Research*. Reinbek: SAGE Publications, pp. 253-258.

Schmidt, N., 2014. Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War. *Obrana a strategie*, 14(2), pp. 73-86. Available at: https://www.obranaastrategie.cz/cs/archiv/rocnik-2014/2-2014/clanky/neither-conventional-war-nor-a-cyber-war-but-a-long-lasting-and-silent-hybrid-war.html [Accessed April 10, 2022].

Smith, M., 2016. *Collaboration for Resilience: How Collaboration among Business, Government and NGOs could be the Key to Living with Turbulence and Change in the 21st Century.* 1st ed., Gland, Switzerland: International Union for Conservation of Nature and Natural Resources. Available at: http://dx.doi.org/10.2305/IUCN.CH.2016.09.en.

Speranza, L., 2020. *A Strategic Concept for Countering Russian and Chinese Hybrid Threats*, Washington DC: Atlantic Council. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Strategic-Concept-for-Countering-Russian-and-Chinese-Hybrid-Threats-Web.pdf [Accessed February 1, 2022].

Stoilova, V., 2018. The Art of Achieving Political Goals without Use of Force: War by Non-Military Means. *Information & Security: An International Journal,* 39(2). pp. 136-142. Available at: https://doi.org/10.11610/isij.3911

Stoker, D. & Whiteside, C., 2020. Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking. *Naval War College Review*, 73(1), pp. 13-40. Available at: https://digital-commons.usnwc.edu/nwc-review/vol73/iss1/4 [Accessed February 1, 2022].

Szymański, P., 2020. New Ideas for Total Defence Comprehensive Security In Finland And Estonia. *Centre for Eastern Studies*, pp. 9-51. Available at: https://www.osw.waw.pl/sites/default/files/OSW-Report_New-ideas-for-total-defence_net_0.pdf [Accessed February 1, 2022].

Šedivý, J., 2018. Národní resilience České republiky versus fragmentovaná společnost. pp. 1-16. Available at: http://www.lipa.cz/doc/43/Jiri%20Sedivy%20-%20Resilience%20CR%20versus%20fragmentovana%20spolecnost.pdf [Accessed April 7, 2022].

Šindlerová, B. & Koleňák, I., 2017. Metodika ke zpracování typových plánů. *Časopis 112*, XVI(2). Available at: https://www.hzscr.cz/clanek/casopis-112-rocnik-xvi-cislo-2-2017.aspx?q=Y2hudW09Ng%3D%3D [Accessed April 28, 2022].

The Global Risks Report 2021: 16th Edition, 2021. World Economic Forum, p. 53. Available at: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

Thiele, R.D. & Schmid, J., 2020. Hybrid Warfare – Orchestrating the Technology Revolution. *ISPSW Strategy Series: Focus on Defense and International Security*, (663). Available at: https://www.ispsw.com/wp-content/uploads/2020/01/663_Thiele_Schmid.pdf [Accessed February 1, 2022].

UCDP, 2018. *Definitions, sources, and methods for Uppsala Conflict Data Program Battle-Death estimates*, Department of Peace and Conflict Research, Uppsala University: Uppsala Conflict Data Program (UCDP). Available at: https://ucdp.uu.se/downloads/old/brd/ucdp-brd-conf-41-2006.pdf.

UiT, 2021. Sikkerhetsmåned 2021. *UiT Noregs arktiske universitet*. Available at: https://uit.no/om/informasjonssikkerhet#innhold_699027 [Accessed February 8, 2022].

UN, 2012. Disaster Risk and Resilience. *UN System Task Team on the Post-2015 UN Development Agenda*. Available at: https://www.un.org/en/development/desa/policy/untaskteam_undf/thinkpieces/3_disaster_risk_resilience.pdf [Accessed April 10, 2022].

WEF, 2021. *The Global Risks Report 2021* 16th Edition., Switzerland: World Economic Forum. Available at: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf [Accessed February 1, 2022].

Weissmann, M., 2019. Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework. *Journal on Baltic Security*, 5(1), pp. 17-26. Available at: https://doi.org/10.2478/jobs-2019-0002 [Accessed April 10, 2022].

Wigell, M., 2019. Democratic Deterrence: How to Dissuade Hybrid Interference. *Finnish Institute of International Affairs*, (110), pp. 4-15. Available at: https://www.fiia.fi/wp-content/uploads/2019/09/wp110_democratic-deterrence.pdf [Accessed February 1, 2022].

Wither, J.K., 2016. Making Sense of Hybrid Warfare. *Connections: The Quarterly Journal*, 15(2), pp. 73-87. Available at: https://www.jstor.org/stable/26326441 [Accessed February 1, 2022].

Wither, J.K., 2020. Back to the future? Nordic total defence concepts. *Defence Studies*, 20(1), pp. 61-81. Available at: https://doi.org/10.1080/14702436.2020.1718498 [Accessed February 1, 2022].

World Bank, 2014. Public-Private Partnerships: Reference Guide. Available at: https://documents1.worldbank.org/curated/en/600511468336720455/pdf/903840PPP0Refe0Box385311B000PUBLIC0.pdf

World Bank, 2017. *Resilient Infrastructure Public-Private Partnerships : Contracts and Procurement – The Case of Japan*, Washington

DC: World Bank. Available at: http://hdl.handle.net/10986/29208.

Zachmeisterová, J. & Táborský, J., 2021. Unikátní cvičení kybernetické bezpečnosti pro strategické firmy obranného průmyslu. *Ministerstvo obrany České republiky*. Available at: https://mocr.army.cz/informacni-servis/zpravodajstvi/unikatni-cviceni-kyberneticke-bezpecnosti-pro-strategicke-firmy-obranneho-prumyslu-227788/ [Accessed March 28, 2022].

Zerfass, A. et. al., 2008. Strategic Communication: Defining the Field and its Contribution to Research and Practice. *International Journal of Strategic Communication*, 12(4), pp.487-505. Available at: https://doi.org/10.1080/1553118X.2018.1493485 [Accessed April 29, 2022].

Appendices

Appendix 1: List of Questions: Norwegian Ministry of Public Security and Justice

1) How does the cooperation between the cybersecurity apparatus work? Is the communication between responsible ministries (UD, JD, and FD), POCs at other ministries, and NCSC working well?

2) Your colleague from the UD mentioned something like a "Security Council for Cooperation" that allows for sharing classified information between the public sector and private companies. How exactly does this work? Could you explain to me the selection process of the companies involved in the Council? How does the process of security clearance for private subjects work?

3) How were the private companies involved during the Exercise Trident Juncture 2018? Are there any plans on the exact role of private companies during a crisis?

4) How would you evaluate the "National Cyber Security Forum"? How does it work? And does it work? Do you have any evaluation of Forum's achievements?

5) How does the "NC3" work? Are the police successful in combating cybercrimes? Do police cooperate with private companies?

6) Are you satisfied with the "Cyber Security Committee"? Did the Committee bring any interesting/valuable results?

7) Have you finished working on the framework for assessing digital value chains?

8) How does the "National Cyber Security Exercise" work? Are the private companies interested in cooperation? Could you shed a light on the scenarios?

9) Is National Cyber Security Month popular? Is it useful in bringing attention to the issue of cybersecurity? Do you think that this event also enhances the level of trust in society?

10) What are the conditions for public-private cooperation to be successful? Do you think that personal networks play important role in the high level of public-private cooperation in Norway?

11) Considering cybersecurity and countering other hybrid threats – what are the obstacles to be overcome in Norway? What are the current issues you are dealing with?

Appendix 2: List of Questions: Czech Private Companies

1) How do you generally evaluate cooperation with the state in the field of information sharing, exchange of know-how and share of experience?

2) How do you evaluate the cooperation with the state in the field of ensuring cyber security, especially the cooperation with NÚKIB? Do NÚKIB's efforts seem sufficient to you? Where do you see room for improvement?

3) In the event of a cyber-attack, would the representatives of the *company name* know whom to turn to within the state administration? Would you contact NÚKIB or other institutions?

4) In your opinion, does the obligation to appoint a security manager ("liaison security employee") according to Act No. 240/2000 Coll. On Crisis Management work well?

5) Did the *company name* participate in any of the cyber security exercises organised by the state?

6a) Do you think that the exchange of information between the public and private sectors works well? If there was a tool to improve collaboration (for better networking, exchange of information and experience), would you be interested in participating in such a platform?

6b) Can you imagine the functioning of such a forum in the Czech environment?

7) In Norway, there is a so-called sector-specific responsibility. Each ministry has one person responsible for cybersecurity and communicates with the communication / IT managers within private companies in certain sector (i.e., energy, transport). Together, they communicate potential threats, risks, etc. This “link” simplifies the exchange of information in Norway and improves trust between the private and public sectors. Can you imagine the functioning of the POC within the state administration and in the Czech Republic? Would the existence of such a person within the Ministry of Industry and Trade facilitate your cooperation with the state?

8) If state authorities organized more training, workshops, discussions, working breakfasts, etc. with the participation of critical infrastructure

companies and representatives from ministries, NÚKIB, CTHH, etc. to improve the resilience of Czech companies, would you be interested in a greater degree of cooperation with the state?

9) If the Czech state prepared a brochure / book with scenarios of various crisis situations (apart from the currently existing standard operating procedure of the IZS ČR), would the existence of such a brochure be beneficial for you?

10) Has the *company name* ever been part of any of the events organized as part of the European Cyber Security Month? Are you aware of this event?

Appendix 3: Thesis Project

Department of International Relations
Faculty of Social Sciences
Charles University

Diploma Thesis Project:

Countering Hybrid Threats: The Nordic Model of the Whole-of-Society Approach

Name: Bc. Kristýna Musilová
Academic advisor: Mgr. Vojtěch Bahenský
Study programme: International Relations
Year of project submission: 2021
September 2022

Introduction to the topic

In the field of security studies, 'hybrid warfare' is an emerging, but also ill-defined concept. This introductory part briefly presents the topic addressed in the thesis, i.e., why, and how can enhanced public-private cooperation contribute to national security, and the political as well as scholarly relevance of the research on the issue of whole-of-society approach to security.

Cyberattacks, the spread of disinformation, and political interference are on the rise. The coronavirus outbreak has revealed how governments can exert conspiracy theories as geopolitical weapons—and in the next decades, more recurrent and impactful use of disinformation on issues of geopolitical importance should be anticipated (WEF 2021). From its inherent nature, hybrid threats are cross-sectoral, and any attempt to build resilience requires action from all parts of the society—and especially their cooperation. However, the recent coronavirus crisis revealed how low is the trust of Czech citizens and industries in the state and the solutions provided by the Government. In 2021, the Ministry of Defence (MoD) of the Czech Republic issued a document "*National Strategy for Countering Hybrid Interference*". According to the Strategy, the main strategic objectives are resilient society, resilient state, and resilient critical infrastructure. The Government of the Czech Republic will seek to enhance cooperation with the commercial, media, non-profit, and education sectors, however, it does not specify *how*. Until the present day, the Czech Republic does not possess any instrument through which it would effectively, systematically, and measurably build the resilience of the state and society.

According to the North Atlantic Treaty Organization (NATO) (2021), hybrid methods of warfare such as propaganda, deception, sabotage, and other non-military tactics have long been used to destabilise adversaries. However, what is new is the speed, scope, and intensity in which are the attacks carried out, partially facilitated by the new technology development. Hybrid warfare targets all elements of national power—critical infrastructure (CI), businesses, and individuals (Dowse and Bachmann, 2019). Hence, for the state, it is essential to develop a toolkit of instruments to protect *not only* its national capacities but also businesses and individuals.

Throughout the years, Nordic countries have been the standard-bearers of the whole-of-society approach (Braw 2021, p. 11). Concerning the critical infrastructure, recently, there has been a significant shift in Norway, Sweden, Denmark, and Finland from the protection of the CI to its resilience. This development is given primarily by the acknowledgement that full protection cannot be guaranteed, and thus, it is not cost-effective. According to the 'Nordic model', it is impossible to safeguard the country against all threats posed by hybrid interference. As a result, Nordic countries adopt a more holistic approach, focusing on vital societal functions rather than mere sector-based infrastructures (Pursiainen 2018). Hence, regarding countering hybrid threats and the whole-of-society approach, Nordic countries represent a security model worth following.

Research target, research question

The purpose of the thesis is to answer the following research question:

How can the Czech Republic employ the instruments of public-private cooperation to enhance its national resilience towards hybrid threats?

According to the research question, the main objective of the thesis is to investigate *how* the Czech Republic can amend its security policy to enhance societal resilience when countering hybrid threats from Russia and China. The thesis aims to propose/design a working custom-made model for the political environment of the Czech Republic. To achieve so, study wants to determine a so-called Nordic comprehensive security model stemming from the policy of total defence. Thus, the study will be conducted in the Czech Republic as well as in Norway and Sweden.

In the thesis, several sub-questions are to be defined. To provide solution for the RQ presented, thesis will firstly answer following sub-question:

Why does the Nordic model of 'total defence' work in countering hybrid threats?

This sub-question aims to holistically explain the Nordic approach towards security, societal resilience, and the roots of the success of the whole-of-society approach in the Scandinavia. Hence, while the RQ is interpretative, the sub-question is explanatory.

To sum up the research target of this thesis, its aim is to i.) clarify and define the Nordic model of countering hybrid threats, and ii.) bring a custom-made model of enhanced societal resilience for the Czech Republic. Overall, the thesis seeks to understand and explore the conditions under which the resilience of the Czech Republic towards hybrid threats may be enhanced.

Literature review

1 Hybrid Warfare: Clarifies or Clouds the Meaning?

Shortly after the Russian annexation of Crimea in 2014, the term *hybrid warfare* rose to prominence among defence and policy circles, media, and wide public. However, despite an increased interest in that buzzword, there is no agreed definition. The absence of one universal term led to many debates over how to define terms like 'Gray Zone Aggression', 'Hybrid Warfare', 'Multi-Domain Warfare', and 'Irregular Warfare'. According to some scholars (e.g., Stoker and Whiteside, 2020; Puyvelde, 2015; Paul, 2016; Cox, Bruscino and Ryan, 2012; Caliskan and Liégeois, 2020) these debates are counterproductive, they attempt to separate the military and civil dimensions of the warfare, and label "hybrid warfare" is merely "old wine in a new bottle". Also interesting is Cordesman's (2020, p. 7) statement that efforts to precisely define "hybrid warfare" completely ignores the fact that the history of war has often begun after decades of competition at a civil level. Thus, according to the critics, the term "hybrid warfare" does not make sense as it is mainly tactically focused—and wars obviously do not consist of just tactical systems (Cox, Bruscino and Ryan, 2012). Stoker and Whiteside (2020) argue that adoption of term hybrid war[22] is "an example of an American failure to think clearly about political, military, and strategic issues". According to Stoker and Whiteside, "hybrid war" causes more harm than good, contributes to the distortion of the concepts of war, peace, and geopolitical competition, and "should be eliminated from the strategic lexicon." In their words, term hybrid warfare is being "used to describe nearly every form of interstate competition and conflict from the

22 Stoker and Whiteside also mention term 'grayzone' or 'gray zone conflict' defined as the "space between peace and war".

tactical to the political, thus, it becomes more confusing than clarifying our understanding of a conflict."

Despite the difficulties with the definition and acquired criticism, these terms deserve attention. Irregular warfare operations garnered significant attention when Frank G. Hoffman labelled them as "hybrid war" in his 2007 book 'Conflict in the 21st Century'. Since then, he has revised his definition in 2009 to describe "hybrid warfare" as follows: "*Any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior in the battle space to obtain their political objectives*." (Hoffman, 2009). "Hybrid warfare" is often used interchangeably with the term "grey zone aggression" defined by Hoffman as "*covert or illegal activities of non-traditional statecraft that are below the threshold of armed organized violence; including disruption of order, political subversion of government or non-governmental organizations, psychological operations, abuse of legal processes, and financial corruption as part of an integrated design to achieve strategic advantage*." (Hoffman, 2009, p. 36)

In their attempts to find a common definition and clarify what "hybrid warfare" is, scholars can be divided into two groups. While one group of scholars keep on with Hoffman's definition (e.g., Mansoor, 2016; Chivvis, 2017; Reichborn-Kjennerud and Cullen, 2016; Giegerich, 2016; Weissmann, 2019, Schmidt, 2014), the others do not consider the term "hybrid warfare" neither useful nor helpful. Scholars following Hoffman agree that hybrid warfare is a combination of conventional military forces and irregulars (insurgents, guerrillas, and terrorists) to achieve control over the population, that is conducted by either state or non-state actors (Chivvis, 2017; Monsoor, 2016, Giegerich, 2016). Authors also agree—rather broadly, though—on a "tool-box" of hybrid warfare consisting of both unconventional and conventional instruments; hence, "blurring" of traditional concepts of warfare (Reichborn-Kjennerud and Cullen, 2016; Chivvis, 2017, Giegerich, 2016). Generally, the agreed characteristic may be population-centrism, use of wide toolbox of non-military and military instruments, and persistence.

NATO understands hybrid threat in the 2020 'NATO Glossary of Terms and Definitions' as "*[a] type of threat that combines conventional, irregular and asymmetric activities in time and space*" (NATO, 2020, p. 64). NATO definition

involves among hybrid threats military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use of regular forces. According to NATO, the hybrid actions aim to "*destabilise and undermine societies.*" (NATO, 2021, p. 64).

In 2016, The European Union adopted a Joint Framework to counter hybrid threats and foster the resilience of the EU, and in 2018, Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats. According to the definition by the European Commission, "*hybrid threats aim to capture the mixture of conventional and unconventional, military and non-military, overt and covert actions that can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare*" (European Commission, 2016), which is a definition very similar to the NATO's one. As for the tools applied as part of hybrid warfare, the EU's definition mentions, e.g., cyberattacks on critical information systems, disruption of critical services such as energy supplies or financial services, undermining public trust in government institutions or exploiting social vulnerabilities (European Commission, 2016).

To sum up, there are two main approaches to the term "hybrid warfare" among scholars—scholars from critical stream are sceptical towards the usefulness of "hybrid warfare" and find it as an ambiguous concept, while authors following Hoffman's definition consider the label to be a useful way how to think about past, today and future wars. Considering the definitions formulated by NATO, EU, and the Governments of Norway, Sweden, and the Czech Republic, they do not significantly differ from each other. Hence, both the international organizations[23] and governments of the examined countries understand "hybrid threats" in a very similar manner.

2 Countering Hybrid Threats: Resilience as a Countermeasure

Authors throughout the spectre all come to the same conclusion regarding countering hybrid threats—there is no one-size-fits-all solution. According to

23 While the EU is not considered to be an international organization, but organization *sui generis*, the author uses this term for a simplification.

Cilluffo and Clark (2012, p. 58), any defence against hybrid threats is inherently a complex operation. The point of entry should be the recognition that the critical tasks that must be accomplished to defend against hybrid threats are beyond the capability and operational capacities of any single actor. Currently, the Czech Republic does not possess many legal nor political instruments to counter hybrid threats. In 2021, Government adopted the Strategy that "*defines objectives and determines instruments essential for the protection of vital, strategic and other important interests of the Czech Republic […] against hostile hybrid interference*." (Ministry of Defence, p. 3). It compliments already existing system of security policy documents "by formulating a comprehensive nationwide policy to counter hybrid interference", e.g., *the Security Strategy of the Czech Republic* (Ministry of Defence, 2015). The Security Strategy, *inter alia*, focuses on the weakening of the political and international legal commitments in the area of security as *some* countries pursue their power-seeking goals through hybrid warfare methods (e.g., propaganda using traditional and new media, disinformation intelligence operations, cyber-attacks, political and economic pressures, etc.) (p. 13). However, according to the Strategy, the government pinpointed three strategic objectives: i.) resilient society, resilient state, resilient critical infrastructure, ii.) holistic approach, and iii.) capability of adequate and timely reaction. These goals are in line with objectives defined by General Philip M. Breedlove, former Supreme Allied Commander Europe of NATO Allied Command Operations, who in 2015 pointed out that resilience, readiness and quick decision-making are fundamental to NATO's success (Breedlove in Lasconjarias and Larsen, eds., 2015).

Jiří Šedivý, former Czech Minister of Defence and current CEO of the European Defence Agency (EDA) divides concept of 'resilience' into three domains: i.) technical-organizational, ii.) environmental, and iii.) societal (2018, p. 3). Norwegian scholar Christer Pursiainen introduced similar three-layer division, however, Pursiainen differs between societal, organizational, and technological domains of resilience. In societal resilience, important actors are national and local governments, communities, and households, and CI resilience often overlaps with normal civil protection. In organizational resilience, the actors are businesses, especially those responsible for CI and

supply chains. In technological resilience, the actors include CI and the respective facility operators (Pursiainen 2018, p. 41).

In the 'technical-organizational' or 'technological' domain, the basic framework for resilience is represented by the Integrated Rescue System (IRS) of the Czech Republic. IRS is in the gesture of the Ministry of Interior and within the EU and NATO, it is considered to be one of the best-working and most effective system. It was inspired by the Finnish model of crisis preparedness and during several past crises proved itself to be a well-working system. In the Czech environment, organizational resilience is—to some extent—specified in Act N. 240/2000 Coll. (hereinafter "the Act") on Crisis Management or so-called "Crisis Act".*24* For the first time, the Act was applied on a larger scale when dealing with emergencies that arose in connection with 1999 floods. For the second time, Crisis Act was applied on a larger scale during the 2020-2021 coronavirus pandemic. The Act regulates the competence and authority of state bodies, and it can limit the rights and freedoms of citizens guaranteed by the Charter of Fundamental Rights and Freedoms. Hence, while first and second domains*25* of the resilience seem to be rather clearly legally defined and regulated, concept of societal resilience remains problematic in the Czech environment.

Despite its importance, concept of "societal resilience" represents similar conceptual challenge as the "hybrid warfare". Hanisch (2016, p. 3) defines three different features of the resilience: i.) *coping capacities* (meaning overcoming disruptions reactively, rapidly, and flexibly), ii.) *adaptive capacities* (proactive and long-term adaptation of structures, processes, or modes of behaviour) and iii.) *transformative capacities* (societies do not adapt gradually but undergo radical change). This three-dimensional approach is shared among several scholars and organizations (e.g., Keck and Sakdapolrak 2013;

---

24 "*Act specifies domain and jurisdiction of state authorities and of authorities of territorial self-governing units and rights and obligations of legal and natural entities during preparedness for crisis situations, which are not related to provision of defence of the Czech Republic against an external attack and during their solution and protection of critical infrastructure and responsibility for the breach of these obligations*." (Chapter 1, paragraph 1, Act N. 240/2000 Coll.).

25 Environmental resilience is defined in the *Conception of Environmental security 2021-2030*.

Guerrero 2020; United Nations 2021; Oxfam 2017). According to Boin and McConnell, the unpredictability and variety of the current threats exposed that the traditional crisis management approach (meaning mainly *protection* of the critical infrastructure) is insufficient. A more holistic approach is required as the conventional prevention, and contingency planning approaches and traditional top-down crisis management solutions have significant limitations in the face of critical infrastructural breakdowns (2007, p. 51). This development reflects the realisation that complete protection can never be guaranteed and that achieving the desired level of protection is not cost-effective (Pursiainen 2018, p. 632). Opposite to the *protection*, adopting a *resilience* approach allows for developing prevention, preparedness, response, and recovery capacities to face predictable and unpredictable situations (Boin and McConnell 2007, p. 52).

In the early attempts in Norway to define societal safety, Olsen et al. (2007) operationalised societal safety to address critical infrastructures and critical societal institutions. Hence, social safety is "*the ability to maintain critical social functions, to protect the life and health of citizens and to meet the citizens' basic requirements in a variety of stress situations*" (Olsen et al., 2007). Christer Pursiainen came up with the similar shift in 2018 (p. 632), as he describes shift in emphasis from critical infrastructure protection to that of resilience in Nordic countries. The author identifies "Nordic model" of CI resilience as Norway, Sweden, Finland, and Denmark had "*based their policies on securing vital societal functions rather than the individual infrastructures that support these functions*." (Pursiainen 2018, p. 634). According to Haavik, societal resilience must build knowledge and methods for producing resilience through the networks where global risks are shaped—which implies a turn from robust infrastructures to the shaping of resilient societies through sustainable livelihood-, scientific- and political practices (Haavik 2020, p. 7). According to Elizabeth Braw (2021, p. 7), to be effective, resilience requires cooperation between government and private sector. However, societal resilience must involve all parts of society. Until recently, governments were reluctant to involve the population in resilience, and instead adopted a whole-of-government approach to all manner of national crises (Braw 2021, p. 11). Hence, when embracing the whole-of-society approach, individuals, businesses, and organisations all play a part in building resilience.

Within the Czech academia, there are several scholars focusing on the resilience as a measure to counter hybrid interference. In 2021, Bahenský and Ditrych proposed the "Netherlandic model" as an inspiration for the Czech model that should be adopted as a follow-up of the release of the Strategy. According to policy paper by Bahenský and Ditrych (2021 p. 7), state institutions should cooperate more, meet frequently and involve *secondment*—the interchange of the personnel within the ministries. Authors then propose joint exercises and deepening of the cooperation between executive power and academia. Thus, creation of the network of experts may contribute to the effectiveness of the future Czech model of countering hybrid threats. Havlík (2020) describes the formation and integration of cyber forces and information operations into the structure of the Army of the Czech Republic. Havlík's main argument is the reflection of the transition from the classical form of warfare to the new platform, represented mainly by cyberspace and hybrid operations. To ensure the operational capability and readiness of the Army of the Czech Republic, it is "*necessary to work on the protection of critical infrastructure and develop defensive and protective mechanisms and processes*" (Havlík, 2020). Nikola Schmidt in his article (2014, p. 74) claims that any future conflict will have a hybrid shape; and exerts "mental resilience" as a crucial defensive measure when facing hybrid threats (Schmidt, 2014, p. 85). The Czech Republic is also pioneering new forms of societal resilience—in 2021, Czech government introduced the new concept of joint military-industry grey-zone exercises that are purely defensive and involve armed forces and invited representatives from strategic industries. These exercises allow the government and private sector to train together to better handle forms of grey-zone aggression (Braw 2021, p. 11), set up new channels of communication, and build mutual trust.

Swedish defence strategy rests upon the concept of 'total defence'—which is in Swedish law defined as the preparations and planning required to prepare Sweden for war consisting of military defence and civil defence. The Parliament, the Government, government authorities, municipalities, private enterprises, voluntary defence organizations as well as individuals are all part of the total defence (Swedish Defence Commission 2021, p. 1). Swedish defence strategies and defence planning are well-researched topics within the academic circles, and the author will discuss them in larger depth later on in the thesis.

The Norwegian Directorate for Civil Protection (DSB) has recently also embraced similar concept of 'total defence' that is based on the collaboration between the military and civic resources to ensure societal safety, and through this added weight to the focus on protection and the national scope (Haavik 2020, p. 3). Norwegian countermeasure strategy then involves primarily three elements: awareness, resilience, and partnerships. As for awareness, it is crucial to increase knowledge and understanding of the tools and tactics, build situational awareness and ensure cross-sectoral communication between private businesses, organizations, and local actors. As for resilience, Norwegian state authorities work together to counter foreign interference, the government established 'National Cyber Security Center' to help protect basic national functions and private business from digital attacks; and works on countering disinformation. As the hybrid interference also crosses national borders, third step is partnerships. Norway takes part in the "Centre of Excellence for Countering Hybrid Threats" (Hybrid CoE) in Helsinki, and actively supports EU-NATO cooperation (Halvorsen 2020).

EU's approach to resilience basically stems from the 2017 "Joint Report to the European Parliament and the Council on the Implementation of the Joint Framework on Countering Hybrid Threats", in which European Commission proposes 22 actions that may be divided into three thematic topics: i.) improving awareness, sharing information among member states and coordination of strategic communication, ii.) building resilience in the fields such as critical infrastructure, energy security, transport, supply chain security, cyber security, public health or space security, and iii.) building resilience against radicalisation and violent extremism (European Commission 2017, p. 6-11). Since 2016, the EU and NATO have identified countering hybrid threats as a priority for cooperation. In Helsinki, the new Hybrid CoE was set up to facilitate and strengthen EU-NATO cooperation (Hagelstam 2018) and provide a forum for strategic discussions and joint training and exercises (Hybrid CoE 2021). Papers issued by The Research Division of the NATO Defense College also often refer to the concept of *resilience* as a key measure when discussing hybrid threats (e.g., Hartmann, 2017; Rühle, 2019). Michael Rühle, Head of Hybrid Challenges and Energy Security Section at NATO, proposes (2019, p. 1) two countermeasures—*deterrence by punishment* (e.g., attribution, sanctions) and *deterrence by denial*

(meaning, e.g., the enhanced resilience) to hybrid attacks. According to Hartmann (2017, p. 7), resilience should become the guiding principle for NATO's forthcoming strategic concept. By enhanced resilience, Hartmann understands putting the effort into improving interaction between politics, citizens, and the armed forces; or creating a new basis for dialogue and cooperation with international organizations, in particular with the European Union (p. 8).

Empirical data and analytical technique

The purpose of this part is to describe how the research will be conducted, how the data will be gathered and how are they going to be analysed. All three of the Nordic states, Norway, Sweden, and Finland, have adopted policy of so called "*total defence*" in their approach to security (Wither 2020, p. 61). However, due to the limited range of the paper and an attempt to achieve analytical depth, only Norwegian and Swedish security models are examined. Countries were selected based on their membership in political and military organizations (Norway is a NATO member country and not an EU member, while Sweden is not a NATO country, but it accessed to the EU). Both Norway and Sweden represent countries with a long tradition of whole-of-society approach. Currently, they are rebuilding their civil defence by drafting strategies, designating coordinating institutions, imposing additional responsibilities on central, regional, and local entities, and developing cooperation between the private and public sectors (European Parliament 2021, p. 2). Hence, as the Nordic countries stand at the forefront of the whole-of-society approach towards security, they serve as valuable case studies on the implementation of whole-of-society practices and how they can be utilised in building up societal resilience (European Parliament 2021, p. 2).

The empirical part of the thesis is divided into two major chapters—first one analysing the Nordic model of total defence, and the second designing a "Czech model" tailored to the Czech environment. In qualitative research as such, various methods may apply, e.g., interviews, focus groups or observations. In case of this thesis, semi-structured interviews represent a suitable method to gather data. Asking open-ended questions allows to explore individual experiences or opinions regarding the researched

phenomenon. Also, as the interviewer does not follow a formalized list of questions, there is broader space for a discussion with the interviewee (Edwards and Holland, 2013).

The first step to identify Nordic model of the whole-of-society approach towards countering hybrid threats is an open-source analysis and study of the existing literature. The sources to be used include academic resources, official documents issued by the governments (in English, Norwegian, and Swedish language), independent analyses conducted by the think-tanks and non-governmental organizations, and documents issued by international organizations (mainly NATO and the EU).

The gained insight is to be used to create a set of questions for the interview to understand how the 'Nordic model' of defence work. Interviewing is one means of collecting data in case study research. While the interviews will be the cornerstone of case study research, collection of data from other sources should be a strength of the case study as it allows for 'triangulation' (Marginson 2004, p. 329). Triangulation is a way of enhancing construct validity as each source of evidence may be 'tested' against each other (Marginson 2004, p. 329). By combining theories, methods or observers in a research study, triangulation "can help ensure that fundamental biases arising from the use of a single method, or a single observer are overcome" (Noble and Heale, 2019, p. 67).

Kallio et al. (2016) describes tool to prepare for interview—an "interview guide"—which is a list of questions that directs conversation towards the research topic. The aim of the guide is to inquire answers from the participants that are both spontaneous and in-depth (Kallio et al., 2016).

After developing the interview guide, the interviews will be conducted with the pre-selected group of the representatives profiled both from the government and private sector. To do so, author of the thesis will travel to Norway and Sweden to conduct the interviews on-site and in-person with the participants. Then, if there is a need of clarification or more information, further information will be retrieved by an online interview through video teleconferencing program. The interviews are important source of information as the respondents possess in-depth information about the topic which is not possible to obtain from the open source.

Based on the open-source analysis and the responses from the interview participants, the Nordic security model will be outlined and explained. A suitable method to analyse text data is a qualitative content analysis. Qualitative content analysis focuses on the characteristics of language as communication with attention to the content and contextual meaning of the text (Hsieh 2005, p. 1278). According to Downe-Wamboldt (1992), "*the goal of content analysis is to provide knowledge and understanding of the phenomenon under study*" (in Hsieh 2005, p. 1278). In this thesis, qualitative content analysis will be used "*as a research method for the subjective interpretation of context of text data through the systematic classification process of coding and identifying themes and patterns*" (Hsieh 2005, p. 1278). Based on the approach presented by Mayring (2007, p. 266) and Schmidt (2007, p. 253), interviews will be fully and literally transcribed to obtain 'material'. After an intensive and repeated reading of the material, author will determine analytical categories. Then the draft analytical categories will be assembled into a guide of analysis. Thanks to this guide, collected material will be coded. That means "*relating particular passages in the text of an interview to one category, in the version that best fits these textual passages*" (Schmidt 2007, p. 255). Then, every interview will be coded according to all the categories in the coding guide. The next stage of the analytical technique involves the compilation of quantifying surveys of the results of coding—i.e., presentation of results in the form of tables (Schmidt 2007, p. 257). In the last step, detailed case interpretation will be provided. The goal of this stage of analysis is to use the results from the codings and present an in-depth, detailed case-study of the Nordic approach to countering hybrid threats.

This case-study will then serve as a 'pattern' or an 'archetype' for the model tailored to the possibilities of the current Czech environment. After conducting an open-source analysis (current policies withing the field of countering hybrid threats, mobilization plans, etc.), a model for enhanced Czech resilience will be introduced. Then, after designing a custom model of the Czech whole-of-society approach to counter hybrid threats, author will conduct another set of interviews, this time with the Czech stakeholders within the government, private sector, and academia. Another set of the interviews will be carried out to ensure the feasibility of the model, and to get valuable feedback from the stakeholders involved in the mechanisms for countering hybrid interference.

The thesis utilizes policy-oriented methodology. Hence, the output of the thesis should consist of policy recommendations with the addressees within both public and private sphere in the Czech Republic.

Planned thesis outline

1. **Introduction**
2. **Research Design & Literature Review**
    i. Methodology
        - Semi-structured Interviews
        - Qualitative Content Analysis
    ii. Data analysis, coding of the data
    iii. Literature Review
        - Hybrid warfare
        - Resilience as a Countermeasure
        - Whole-of-society-approach to Security
3. **Norwegian Model of Public-Private Cooperation**
4. **Design of a Model for the Czech Republic**
5. **Conclusions**

References

The Global Risks Report 2021: 16th Edition, 2021. World Economic Forum, p. 53. Available at: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

NATO's response to hybrid threats, 2021. *North Atlantic Treaty Organization* [online]. March 16, 2021. [cit. 2021-08-28]. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm

Dowse, A., S. Bachmann, 2019. Explainer: what is 'hybrid warfare' and what is meant by the 'grey zone'? The Conservation [online]. June 17, 2019. [cit. 2021-08-28]. Available at: https://theconversation.com/explainer-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone-118841

Kallio H. et al., 2016. Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*. Vol. 72, No. 12, pp. 2954-2965. Available at: https://doi.org/10.1111/jan.13031.

Edwards R. and J. Holland, 2013. What is Qualitative Interviewing? *Qualitative Research*. Vol. 15, No. 4, pp- 540-542. Available at: https://doi.org/10.1177%2F1468794114535040.

Anon., National Strategy for Countering Hybrid Interference, 2021. Ministry of Defence of the Czech Republic [online]. VHÚ, Prague. Available at: https://www.mocr.army.cz/assets/informacni-servis/zpravodajstvi/national-strategy---aj-final.pdf

Pursiainen, C., 2017. Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction*. Vol. 27, pp. 632-641. Available at: http://dx.doi.org/10.1016/j.ijdrr.2017.08.006

Mansoor, P.R., 2012. Hybrid War in History, in Hyb*rid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, ed. Williamson Murray and Peter R. Mansoor. Cambridge: Cambridge University Press.

Chivvis, Ch., 2017. Understanding Russian "Hybrid Warfare" and What Can be Done About It. *The RAND Corporation*. Testimony presented before the House Armed Services Committee on March 22, 2017. Available at: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

Giegerich, B., 2016. Hybrid Warfare and the Changing Character of Conflict. *Connections*. Vol. 15, No. 2 (Spring 2016), pp. 65-72. Available at: https://www.jstor.org/stable/26326440.

Reichborn-Kjennerud E., P. Cullen, 2016. What is Hybrid Warfare? *Norwegian Institute for International Affairs (NUPI)*. Policy Brief 1/2016, part of the Multinational Capabilities Development Campaign (MCDC) project Countering Hybrid Warfare (CHW) funded by the Norwegian Ministry of Defence. Available at: http://www.jstor.com/stable/resrep07978.

Hoffman, F., 2009. Hybrid Warfare and Challenges. *Small Wars Journal*. Vol. 51, No. 1, pp. 34-39. Available at: https://smallwarsjournal.com/documents/jfqhoffman.pdf.

Stoker, D. and Whiteside, C., 2020. Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking. *Naval War College Review.* Vol. 73, No. 1, Article 4. Available at: https://digital-commons.usnwc.edu/nwc-review/vol73/iss1/4.

Mayring, P., 2007. *Qualitative Content Analysis* in Flick, Uwe, Kardorff, Ernst von, Steinke (eds.), *A Companion to Qualitative Research*. Reinbek: SAGE Publications, pp. 266-269.

Schmidt, C., 2007. *The Analysis of Semi-structured Interviews* in Flick, Uwe, Kardorff, Ernst von, Steinke (eds.), *A Companion to Qualitative Research*. Reinbek: SAGE Publications, pp. 253-258.

Marginson, D. 2004. *The Case Study, The Interview and The Issues: A Personal Reflection* in Humphrey, Lee (eds.), *The Real Life Guide To Accounting Research.* United Kingdom: Elsevier, pp. 325-338. Available at:

Wither, J. K., 2020. Back to the future? Nordic total defence concepts. *Defence Studies*, Vol. 20, No. 1, pp. 61-81. Available at: https://doi.org/10.1080/14702436.2020.1718498

Noble, H., R. Heale. 2019. Triangulation in research, with examples. *Evidence-Based Nursing*, Vol. 22, No. 3, pp. 67-68. Available at: https://ebn.bmj.com/content/ebnurs/22/3/67.full.pdf

Hsieh, H., 2005. Three Approaches to Qualitative Content Analysis. *Qualitative Health Research,* Vol. 15, No, 9, pp. 1277–1288. Available at: https://doi.org/10.1177/1049732305276687

Hoffman, F., 2009. "Hybrid vs. compound war. The Janus choice: Defining today's multifaceted conflict," *Armed Forces Journal*, October 1, 2009. Available at: http://armedforcesjournal.com/hybrid-vs-compound-war/.

Hoffman, F., 2018. Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges. *PRISM: National Defense University. The Journal of Complex Operations*, Vol. 7, No. 4, pp. 30-47. Available at: https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/

Bahenský, V., O. Ditrych., 2021. Nizozemský model čelení hybridnímu působení: inspirace pro Českou republiku. Ústav mezinárodních vztahů [online]. Prague: 7.6.2021. [cit. 2021-10-02]. Available at: https://www.iir.cz/nizozemsky-model-celeni-hybridnimu-pusobeni-inspirace-pro-ceskou-republiku

Braw, E., 2021. Commentary: Everyone together now: Creating a resilient society in an age of cyber threats. Macdonald-Laurier Institute: Ottawa, Ontario, p. 1-18. Available at: https://macdonaldlaurier.ca/files/pdf/20210601_Everyone_together_now_Braw_COMMENTARY_FWeb.pdf

Rühle, M., 2019. Deterring hybrid threats: the need for a more rational debate. *NATO Defense College*, 15, pp.2-4. Available at: https://www.jstor.org/stable/resrep19846 [Accessed April 10, 2022].

Hartmann, U., 2017. The Evolution of the Hybrid Threat, and Resilience as a Countermeasure. *NATO Defense College*, 139, pp.1-8. Available at: https://www.ndc.nato.int/news/news.php?icode=1083 [Accessed April 10, 2022].

Crisis Management Act N. 240/2000 Coll. (Crisis Act), 2000. Available at: https://www.hzscr.cz/hasicien/file/crisis-management-act-n-240-2000-coll-pdf.aspx.

Halvorsen, A., 2020. Statement at seminar on influence operations. *Government.no*. Available at: https://www.regjeringen.no/en/aktuelt/innlegg-pa-seminar-om-pavirkningsoperasjoner/id2690513/ [Accessed April 10, 2022].

NATO, 2021. NATO's response to hybrid threats. *North Atlantic Treaty Organization*. Available at:

https://www.nato.int/cps/en/natohq/topics_156338.htm [Accessed April 10, 2022].

Puyvelde, D.V., 2015. Hybrid war – does it even exist?. *NATO Review*. Available at: https://www.nato.int/docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/index.html [Accessed April 10, 2022].

Paul, C., 2016. Confessions of a Hybrid Warfare Skeptic: What Might Really Be Interesting but Hidden Within the Various Conceptions of Gray Zone Conflict, Ambiguous Warfare, Political Warfare, and Their Ilk. *Small Wars Journal*. Available at: https://smallwarsjournal.com/jrnl/art/confessions-of-a-hybrid-warfare-skeptic [Accessed April 10, 2022].

Caliskan, M. & Liégeois, M., 2020. The concept of 'hybrid warfare' undermines NATO's strategic thinking: insights from interviews with NATO officials. *Small Wars & Insurgencies*, 32(2), pp.295-319. Available at: https://doi.org/10.1080/09592318.2020.1860374 [Accessed April 10, 2022].

Breedlove, M. & eds., 2015. Foreword. In *NATO's Response to Hybrid Threats*. Rome: NATO Defense College, p. xxi-xxv.

Keck, M. & Sakdapolrak, P., 2013. WHAT IS SOCIAL RESILIENCE? LESSONS LEARNED AND WAYS FORWARD. *Erdkunde*, 67(1), pp.5-19. Available at: http://www.jstor.org/stable/23595352 [Accessed April 10, 2022].

European Commission, 2016. FAQ: Joint Framework on countering hybrid threats. *European Commission*. Available at: https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250 [Accessed April 10, 2022].

Weissmann, M., 2019. Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework. *Journal on Baltic Security*, 5(1), pp.17-26. Available at: https://doi.org/10.2478/jobs-2019-0002 [Accessed April 10, 2022].

Cox, Dan G., Bruscino, Thomas & Ryan, Alex, "Why Hybrid Warfare is Tactics Not Strategy: A Rejoinder to 'Future Threats and Strategic Thinking'", *Infinity Journal*, Volume 2, Issue No. 2, Spring 2012, pages 25-29.

Haavik, T., 2020. Societal resilience – Clarifying the concept and upscaling the scope. *Safety Science.* Vol. 132, pp. 1-8. Available at: https://doi.org/10.1016/j.ssci.2020.104964

Havlík, M., 2020. Jak daleko má svět k dosažení světového míru a proč?. *Vojenské rozhledy*, 29(3), pp.2336-2995. Available at: https://www.vojenskerozhledy.cz/en/kategorie-clanku/bezpecnostni-prostredi/dosazeni-svetoveho-miru [Accessed April 10, 2022].

Olsen, O.E., Kruke, B.I. & Hovden, J., 2007. Societal Safety: Concept, Borders and Dilemmas. *Journal of Contingencies and Crisis Management*, 15(2), pp.69-79. Available at: https://doi.org/10.1111/j.1468-5973.2007.00509.x [Accessed April 10, 2022].

Oxfam, 2017. *The Future is Choice: Absorb, Adapt, Transform*, Oxford: Oxfam International. Available at: https://oxfamilibrary.openrepository.com/bitstream/handle/10546/620178/gd-resilience-capacities-absorb-adapt-transform-250117-en.pdf;jsessionid=660932421B9CCCFF3039BF5C12D6EE4C?sequence=4.

UN, 2012. Disaster Risk and Resilience. *UN System Task Team on the Post-2015 UN Development Agenda*. Available at: https://www.un.org/en/development/desa/policy/untaskteam_undf/thinkpieces/3_disaster_risk_resilience.pdf [Accessed April 10, 2022].

Hybrid CoE, 2022. What is Hybrid CoE?. *Hybrid CoE: European Centre of Excellence for Countering Hybrid Threats*. Available at: https://www.hybridcoe.fi/who-what-and-how/ [Accessed April 10, 2022].

Anon., 2015. *Security Strategy of the Czech Republic*, Prague: Ministry of Foreign Affairs of the Czech Republic.

Schmidt, N., 2014. Neither Conventional War nor a Cyber War, but a Long-Lasting and Silent Hybrid War. *Obrana a strategie*, 14(2), pp.73-86. Available at: https://www.obranaastrategie.cz/cs/archiv/rocnik-2014/2-2014/clanky/neither-conventional-war-nor-a-cyber-war-but-a-long-lasting-and-silent-hybrid-war.html [Accessed April 10, 2022].