Mikkel Amundsen
Fanny Chaba Sunde

Threat mitigation and national security

A mixed methods study of perceptions on cyber security information sharing among Norwegian organizations

Masteroppgave i MISEB
Veileder: Benjamin James Knox
Medveileder: Geir Olav Dyrkolbotn

Desember 2022

Masteroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

NTNU
Kunnskap for en bedre verden

Mikkel Amundsen
Fanny Chaba Sunde

Threat mitigation and national security

A mixed methods study of perceptions on cyber security information sharing among Norwegian organizations

Masteroppgave i MISEB
Veileder: Benjamin James Knox
Medveileder: Geir Olav Dyrkolbotn
Desember 2022

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

NTNU
Kunnskap for en bedre verden

Abstract

Norwegian organizations are increasingly targeted by cyber threat actors, reinforcing the need for a more holistic approach to national security. In the current Norwegian cyber landscape, the national security has to a large extent become the collective responsibility of individual undertakings due to increased interdependencies and complex supply chains. A descriptive mixed methods research design consisting of a dominant quantitative survey paired with qualitative in-depth interviews was used to examine perceptions of cyber security information sharing across Norwegian organizations, and its effect on individual organizations' and the overall national security posture.

This thesis found that private and public organizations had varied reasons for engaging in cyber security information sharing. Whereas public organizations participated due to superior requirements and regulations, and to develop relationships with government agencies, their private counterparts mainly participated to gain access to the information of similar undertakings. The underlying factors leading to cyber security information sharing were heavily influenced by a sense of mutual benefit toward increasing the individual undertakings' security posture, and a willingness to contribute to national security.

Even though undertakings were generally more willing to share information with the national services than any other organizations, the services were heavily criticized - mainly for disseminating low value information with insufficient timeliness. Despite this, information from national services was regarded as of high confidence, and was particularly used to address top management and non-technical personnel.

Although the study revealed general positive perceptions on the new Security Act and the Sector Response Entity model, findings also indicated that the current Norwegian information sharing framework contributes to increasing several challenges which restricts the overall national security posture. In the conclusion, the researchers propose four actions to counteract these challenges.

Sammendrag

Norske virksomheter blir i økende grad utsatt for målrettede cyberangrep som forsterker behovet for en helhetlig tilnærming til nasjonal sikkerhet. I dagens cyberlandskap har nasjonal sikkerhet i stor grad blitt enkeltvirksomheters kollektive ansvar på grunn av økt gjensidig avhengighet og komplekse leverandørkjeder. Denne studien har derfor undersøkt holdninger til informasjonsdeling på tvers av private og offentlige virksomheter i Norge, samt hvordan informasjonsdeling påvirker både enkeltvirksomheter og den nasjonale sikkerhetstilstanden. Både kvantitative og kvalitative undersøkelser ble benyttet for å gi en helhetlig og nyansert forståelse av holdningene innen det norske cybersikkerhetsmiljøet.

Studien avdekket at private og offentlige virksomheter deler cybersikkerhetsinformasjon av ulike grunner. I hovedsak deler offentlige virksomheter informasjon på bakgrunn av statlige krav og reguleringer, samt å utvikle samarbeidet med myndighetene. Private virksomheter anså imidlertid tilgangen til informasjon fra sidestilte virksomheter som den viktigste grunnen. De underliggende årsakene for at virksomheter velger å dele informasjon var forankret i troen på forbedret sikkerhetstilstand til enkeltvirksomheter, og et ønske om å bidra til nasjonal sikkerhet.

Selv om norske virksomheter generelt var mer villig til å dele informasjon med nasjonale tjenester enn øvrige norske virksomheter, ble de nasjonale tjenestene sterkt kritisert, i hovedsak for å dele informasjon av lav verdi med utilstrekkelig tidsriktighet. Til tross for dette var informasjonen ansett å ha høy konfidens, og ble benyttet særlig mot toppledere og ikke-teknisk personell i de respektive virksomhetene.

Studien avdekket også at cyberpersonell generelt var positive til den nye sikkerhetsloven og de sektorvise responsmiljøene. Allikevel indikerte funnene at det nåværende rammeverket for informasjonsdeling forsterket flere utfordringer som i sum svekker den samlede nasjonale sikkerhetstilstanden. For å motvirke disse utfordringene, er fire anbefalinger skissert i konklusjonen.

Preface

This thesis was written in the summer and fall of 2022 as part of IMT4905 Experience-based Master's Thesis - the final subject of *Experience-based Master in Information Security* (MISEB) at the Norwegian University of Science and Technology (NTNU) in Gjøvik, Norway. The project was supervised by Associate Professor Benjamin James Knox and conducted within the Department of Information Security and Communication Technology at NTNU.

We would like to give special thanks to our supervisor Benjamin James Knox and co-supervisor Geir Olav Dyrkolbotn for providing guidance and keeping our expectations realistic. Additionally, Adviser Hilde Bakke has been indispensable through our time at NTNU. Additionally, we would like to thank our partners Luigi and Camilla for supporting us through this journey which was made significantly more strenuous due to a pregnancy and the war in Ukraine. A heartfelt thank you is also in order to our respective co-assistants Timian and Koda for being present, very much available and adding some much needed real-life friction and stress. And, of course, love.

Mikkel Amundsen & Fanny Chaba Sunde
Oslo, December 2022

"Information sharing, however, is not an easy topic. It comes with many facets. For example, information sharing spans strategic, tactical, operational and technical levels; spans all phases of the cyber incident response cycle; is highly dynamic; crosses the boundary of public and private domains; and concerns sensitive information which can be potentially harmful for one organization on the one hand, while being very useful to others." [1]

LUIIJF & KLAVER

Contents

Figures

Tables

Acronyms

CDX Cyber Defense Exercise. 17–20

CERT Computer Emergency Response Team. 1, 17, 18, 33, 39–41, 83, 85, 108, 127, 129, 153

CIO Chief Information Officer. 14, 62

CISA Cybersecurity and Infrastructure Security Agency. 27

CNI Critical National Infrastructure. 26

CSaaS Cyber Security As A Service. 1, 61, 125, 153, 161

CSI Cyber Security Information. 2, 3, 5, 12, 21, 23, 86, 94, 108, 110–113, 120, 122, 123, 125, 129–133, 137–139, 141, 147–150, 152–157, 159, 163–167

CSIO Chief Information Security Officer. 14, 62, 131, 168

CSIRT Computer Security Incident Response Team. 35, 40, 41, 83, 85, 108

CSIS Cyber Security Information Sharing. 2–5, 7, 9, 11, 12, 18–23, 31, 40, 46, 48, 49, 53–60, 64, 76, 78, 83–85, 87, 88, 92, 94, 96–98, 103, 108–115, 120, 122, 123, 125–128, 130–133, 135, 136, 138, 140, 141, 143–145, 147–168

CSO Chief Security Officer. 62, 168

CTI Cyber Threat Intelligence. 5, 9–11, 14–17, 20–22, 31, 55, 88, 129, 154

ENISA European Network and Information Security Agency. 7, 11, 15, 16, 20, 21

EOS Committee Norwegian Parliamentary Oversight Committee on Intelligence and Security Services. 38

FIRST Forum of Incident Response and Security Teams. 35

FNF Fundamental National Functions. 1, 3, 25, 26, 28–30, 34, 41, 42, 61, 83, 87–89, 106, 116–118, 120, 129, 138, 147–149, 151, 163, 164

GCHQ Government Communications Headquarters. 27

GDPR General Data Protection Regulation. 136

ICT Information and Communications Technology. 39, 42, 43, 63, 65, 73, 106

IE Information Exchanges. 7–9, 16

IOC Indicators of Compromise. 15, 31, 32, 126

ISAC Information Sharing Analysis Center. 7, 40, 41, 83, 85, 108

JCCC Norwegian Joint Cyber Coordination Centre. 34, 38, 40, 85, 118, 119, 147, 148, 151

NC3 Norwegian National Cybercrime Centre. 85, 140

NCIS Norwegian National Criminal Investigation Service. 38, 40, 140, 153

NCSC Norwegian National Cyber Security Centre. 27, 32, 33, 38, 39, 41, 42, 85, 116–120, 126, 130, 135, 140, 147–149, 151, 153, 154, 164, 166, 167

NFC National Critical Functions. 26

NIS Norwegian Intelligence Service. 32, 38, 40, 64, 84, 85, 87, 134

NorCERT Norwegian Computer Emergency Response Team. 39, 42

NORDSA Norwegian Defence Security Agency. 38

NPSS Norwegian Police Security Service. 32, 38, 40, 64, 84, 85, 87

NRMC National Risk Management Center. 27

NRN National Restricted Net. 35, 134

NSA National Security Authority. 1, 27–29, 32, 35, 38–40, 42, 43, 64, 84, 85, 87, 117, 119, 120, 126, 130, 135, 147, 148, 153, 154, 164–167

PMESII Political, military, economic, social, infrastructure, information. 87–89, 92, 96, 99

SIC 2007 Standard Industrial Classification 2007. 61, 62, 71

SOC Security Operations Center. 40, 41, 85, 108

SRE Sector Response Entities. 2, 38, 41, 42, 115, 116, 118, 126, 129, 130, 140, 147–149, 152–154, 163–166

TLP Traffic Light Protocol. 17, 34–36, 116, 127, 135, 150, 155, 165, 166

TTP Tactics, Techniques, and Procedures. 31

WSDI National Warning System for Digital Infrastructure. 39, 118, 147

Introduction

1.1 Background

Over the last years, the threat landscape and how the Norwegian population and governance entities perceive it has changed drastically. There is an increasing risk for Norwegian entities being targeted by foreign cyber threat actors, reinforcing the need for a more holistic approach to national security. The extensive digitization has resulted in increasing interdependencies across traditional divisions in society - both between private and public undertakings, and between the civil society and the armed forces - while also leading to the same divisions becoming less distinct. Even though the development has enabled impressive new advancements, it has also lead to new vulnerabilities [2][3].

The risk of severe cyber-attacks are high and increasing, especially for organizations engaged in defense, foreign- and security politics, in addition to certain research and development entities [4][5]. From 2019 to 2021, the Norwegian National Security Authority (NSA) has registered a threefold increase in the number of severe cyber incidents toward both private and public entities in Norway, affecting several entities simultaneously across different sectors [6]. Prior to the extensive digitization and the actualization of hybrid threats in the west, national security was seen as a concern and responsibility for the public sector, and mainly delegated to the national intelligence and security services. In today's security landscape - where long and complex supply chains upholds the Fundamental National Functions (FNF) with in sum constitutes the national security interests - the responsibility to maintain national security has to a large extent become the collective responsibility of individual undertakings [7][8][9][10].

Thus, Norwegian national security depends on the security efforts and cooperation between public and private entities which support FNFs. This task is challenging, as FNFs span across different sectors, in which both Computer Emergency Response Team (CERT)s and security hubs are organized per sector, in addition to other private security organizations offering Cyber Security As A Service (CSaaS). The challenge is further complicated as most public and private entities have supply chains which spans across national borders [11].

Trust and mutual benefits are essential elements to ensure actionable Cyber Security Information Sharing (CSIS), but there is a lack of both national and international studies examining the efficacy and perceived quality of the Cyber Security Information (CSI) shared between different entities [12], and even less studies examining the efficiency of the current Norwegian cyber security landscape. A more nuanced and holistic understanding of how and why CSIS is performed in Norway may provide both private and public stakeholders incentives and guidance in enhancing their individual and collective security posture.

1.2 Scope and limitations

The thesis aims to examine attitudes and perceptions toward CSIS across private and public entities and their effect on the individual organizations' and overall national security posture. Naturally, the thesis focuses on Norwegian organizations from both the public and private sector. A descriptive mixed methods research design was used to enable development of a holistic and in-depth understanding on the perceptions of Norwegian cyber security professionals. Even though the study exclusively examines CSIS in the Norwegian context, the results could still be relevant for other cyber security communities.

The cyber threat landscape is quickly evolving and increasing, and to further limit the scope, this thesis will focus on Norwegian cyber security in the context of threats posed by adversaries or hostile actors, and information sharing in light of the Norwegian Security Act. The underlying documents leading to the current revision of the Security Act was used to form the current national cyber security architecture - the cooperation and information flow between national services, cyber security organizations, Sector Response Entities (SRE), and individual undertakings. These mechanisms serve as the focus areas for this study. Hence, the study does not cover foreign entities being part of supply chains or international cooperation.

To provide context and basis for comparison, relevant theoretical research and similar empirical studies in other countries were used to assess the current state of, and perceptions on the Norwegian cyber security landscape.

The thesis is descriptive and is not aimed at presenting normative recommendations. Thus, additional research addressing findings and converting them into recommendations and measures is necessary. However, findings may be used by different stakeholders within both private and public sector as a basis to develop or revisit its security measures such as procedures and future security investments, enhancing their individual and collective security posture.

1.3 Research questions

Based on the problem description outlined in this section, the overarching research question of the study is:

> *"Why do Norwegian organizations engage in cyber security information sharing?"*

To answer the research question, several subordinated questions were established to get a more profound insight in the problem described above. The subordinated research questions are:

RQ1: How is CSIS performed in Norway?
RQ2: How is CSIS perceived among cyber security professionals within the Norwegian cyber security community?

- **RQ2-1**: How is CSIS perceived in light of operational factors?
- **RQ2-2**: How is CSIS perceived in light of organizational factors?
- **RQ2-3**: How is CSIS perceived in light of economic factors?
- **RQ2-4**: How is CSIS perceived in light of policy factors?

RQ3: What is the perceived usefulness and willingness in sharing CSI within the Norwegian cyber security community?

- **RQ3-1**: Which factors affect the usefulness of CSI?
- **RQ3-2**: What factors affect the willingness to share CSI?

Throughout the thesis the research questions will be referred to by their numeric denomination (**RQ#**).

1.4 Thesis outline

The thesis has the following structure:

Chapter 2 Related Research presents the findings of the literature review with the main emphasis on empirical research of CSIS. In the end of the chapter, the relevance of the identified literature is assessed in relation to the different research questions.

Chapter 3 Theory includes theory and background information relevant to the thesis and is the foundation for the analysis, integration and and interpretation later in the thesis. Covered topics are: an introduction to the Norwegian Security Act and FNFs, definitions and categorizations related to information sharing, and lastly an overview of the Norwegian cyber security landscape.

Chapter 4 Methodology explains how the research was conducted in order to answer the research questions of the thesis. The chapter includes a description of the research process, research design, what research methods were used and how the data was collected, analyzed and interpreted. Lastly, considerations regarding validity and reliability of the thesis is discussed.

Chapter 5 Results presents the analysis of the collected data. Firstly, the sample is described through descriptive statistics. Then, the results following the questionnaire design is subsequently analyzed and integrated with the qualitative results. Lastly, the findings is compared with former empirical research on CSIS.

Chapter 6 Discussion discusses and integrates the findings of the results with that of the theoretical research of legislature and policy documents as stated in the theory. The section also provides a more detailed and nuanced understanding of how CSIS is practiced in Norway in contrast to how the theory intends it to be. The chapter also discusses several improvements of the research conducted.

Chapter 7 Conclusion and Future Research answers the overarching research question of the thesis, followed by proposed future research in the field of CSIS in Norway.

Related research

In this chapter, the findings of the literature review are presented. Related research regarding the scope of the thesis is structured into several subsections such as Theoretical research on CSIS and Empirical research on CSIS. Due to the scope of this thesis and its research questions, the exploration of empirical research related to CSIS was more thorough than the theoretical one. The relevance of the identified literature has been assessed in relation to the different research questions, and a summary can be seen at the end of the chapter.

2.1 Theoretical research on CSIS

2.1.1 Benefits and challenges with CSIS and CTI

This section comprises theoretical research regarding benefits and challenges with information sharing, i.e. CSIS or Cyber Threat Intelligence (CTI). Existing academic and grey literature presents numerous of reasons why CSIS or CTI are or could be beneficial, as well as challenging. Research regarding why organizations share Cyber Security Information (CSI) and what affects the usefulness of CSI were mainly addressed in the empirical literature. However, benefits and challenges affecting the willingness to share or influencing the usefulness of CSI are presented in the list of benefits and challenges.

The identified benefits and challenges associated with CSIS and CTI derived from the literature are presented in Table 2.1. The list of benefits and challenges is derived from Zibak & Simpson [13] and is supplied with additional benefits and challenges identified by this thesis' researchers, as well as references identified in the literature review. The benefits and challenges are divided into four different categories: *operational*, *organizational*, *economic* and *policy*. These categories are originally derived from [13] and were used to explore different perceptions within the individual categories, and analyze and interpret benefits and challenges of same category toward each other.

Category	Benefits	Challenges
Operational	• Reduces duplicate information handling [14][15] • Supports breach detection [16][17][18][19][20] • Reduces damage caused by breaches [16] • Supports incident response [21][1] [17][18][19][20] • Supports deterrence efforts [22]	• Lack of standardization [23][1][14] • Vaguely defined terminology [23][16] • Capacity limits [14] • Determining accuracy [14] • Validating quality [24][25] • Incomplete or false information shared [19] • Ensuring timeliness [14] • Achieving interoperability and automation [20][17] • Safeguarding sensitive information [20][1][26] • Handling unused or irrelevant data [20][16][15]
Organizational	• Expands professional networks [13] • Supports greater defensive agility and resilience [1][27][20] • Validates intelligence derived from other sources [20] • Improves overall security posture [20] [23][1][27][19] • Improves situational awareness [20][1][19] • Combats skills gap [27]	• Proliferation of redundant efforts [14] • Competition [14] • The risk of reputation damage [28][15][19][29] • Establishing trust among participants [30][1][19][29] • Lack of trained staff [14][17] • Lack of top management endorsement [1][17] • Cultural and ethical differences or barriers [1][29]
Economic	• Cost savings [30][31] • Allows subsidies provision by governments [30][22] • Lowers cyber insurance premiums [30] • Reduces uncertainty associated with cyber security investment decisions [32] • Support security changes and investments [20]	• Free riding [28][1][27][29] • Resource draining [1] • Loss of clients confidence and satisfaction [33][34][29]
Policy	• Reinforces relationship with government agencies [35] • Offers liability protection [16][19]	• The risk of violating privacy or antitrust laws [1][15][27] • Government over-classification [36] • Upholding public values [35] • Different legal frameworks across jurisdictions [14][29] • Mandated sharing and hierarchical differences [1] • Absence of mutually agreed clear mandate and rules [1][30] • Legal liability concerns [19]

Table 2.1: Benefits and challenges associated with CSIS and CTI derived from existing research literature.

2.2 Empirical research on CSIS

2.2.1 Perceived incentives and barriers to information sharing in EU

In 2010, European Network and Information Security Agency (ENISA) conducted an evidence-based research to identify which barriers and incentives were most important in daily practice in Information Exchanges (IE) and Information Sharing Analysis Center (ISAC)s within the European Union [30]. The report was part of ENISA's Resilience and Critical Information Infrastructure Protection Programme.

The researchers conducted interviews with nine network and information security experts from six EU countries, in addition to an online survey where the same respondents ranked a list of 23 incentives and 24 barriers to information sharing [30]. Even though the research did not directly comprise perceived benefits and challenges with CSIS, it addressed important incentives and drivers to increase the willingness of joining a IE or general willingness toward information sharing, and what barriers and challenges that might prevent or weaken information sharing. The study found that incentives and barriers affect the perceived usefulness of both information sharing in general and the shared information. The findings of the study can be compared to the results of this thesis if the proposed incentives and barriers are reflected in the perceived benefits and challenges within the Norwegian cyber security community. However, the research only included a limited number of experts from a handful of countries and the findings should therefore be seen as preliminary and general validity cannot be claimed to all kinds of IEs [30].

The findings of the research indicated that several of the incentives and barriers identified in the available literature were of relatively low importance to practitioners and security officials working in IEs. The incentives addressed in the report are listed in order of importance below of which incentives ranked as of low importance was excluded as a delimitation [30]:

1. Incentives of **high** importance
   - Cost savings and efficient allocation of information security resources, and
   - Quality, value and use of information shared.
2. Incentives of **medium** importance
   - Trust among IE participants,
   - Receiving privileged information from government or security services,
   - Processes and structures for sharing, and
   - Allowing IE participants' autonomy but ensuring company buy-in.

Barriers and challenges addressed in the report are listed below, ranked in order of importance by the participants in [30]. Similarly as the incentives, barriers ranked as of low importance are excluded:

1. Barriers of **high** importance
   - Poor quality information,
   - Risk to reputation, and
   - Poor management.
2. Barriers of **medium** importance
   - Type of participants,
   - Legal barriers related to fear of legal or regulatory action,
   - Fear of leaks,
   - Group size,
   - Group behavior externalities,
   - Social barriers from government,
   - Poor decision-making about investment in security, and
   - Norms of rivalry.

Cost savings and efficient allocation of information security resources were ranked as the most important incentives for participating in an IE. These incentives were followed by the importance of quality, value (e.g. usefulness) and further use of the shared information, which corresponded with the barrier *poor quality of shared information*, ranked as the most significant barrier to information sharing. Sufficient quality, value and usefulness of shared information were also reflected in one of the incentives assessed as of medium importance, such as receiving privileged information from the government or security services. According to the participants, restricted or classified information, or non-public information from governmental entities, law enforcement and security services represented high-quality information and were highly prized. Even though such information was rated as high quality information, the same participants stressed that the culture of secrecy within the government regarding the "need-to-know principle" was seen as a barrier to information sharing [30].

The quality information are within the literature described as a) data must be timely and specific, b) participants must share information which is of equal value (motivation to share information stemming from the expectation that they would receive information of equal value in the future), c) information shared must be relevant to participants' concerns and, d) sharing information at a suitable level [30].

Another interesting finding was that *poor management* was perceived as a more important barrier than *processes and structures for sharing*, which was perceived as an important incentive for participating in IE. Challenges related to poor management were comprised of how the IE was constituted and managed: such as leadership, rules, and structures for sharing information. Clear rules, which are understood and followed by the members of an IE were perceived as a medium important incentive to share information or enable information sharing, as well as building trust among the participants of an information sharing community. Information sharing communities with higher level of trust might, however, require less rules and procedures than newly-formed communities. Strong leadership was perceived as an important incentive as it could facilitate a good environment for sharing and prevent free-riders or lobbying. A clear mandate and goal of the information sharing community was also assessed as an important incentive to share information as it would ensure the relevance of information shared for all participants [30].

Trust among participants of an IE was ranked within the top three most important incentives for participating in information sharing. Strong management, participants of appropriate personnel categories, as well as limiting the number of participants were mentioned as important measures to develop trust among participants of an IE. If the entity was too big, it was assessed as less likely that the participants would have common interests, and less likely that trusting relationships would develop. Additionally, there was a strong preference among the respondents that the participants of an IE should be technical or security experts, rather than individuals working with sales, marketing or other commercial activities, in order to creating a trusted environment for information sharing [30].

Finally, risk to reputation, caused by e.g. leakage of sensitive or business confidential information, were of high concern among the respondents, and represented a significant barrier to information sharing. However, an interesting finding was that the possibility of achieving a good reputation due to participation in information sharing was not perceived as an important incentive, while the risk of getting a negative reputation by sharing information (e.g. disclosing information about an attack or vulnerability) was perceived as a significant problem [30].

2.2.2 Perceived benefits and barriers with CTI sharing in the UK

In 2019, Zibak & Simpson from the Department of Computer Science at the University of Oxford, examined the attitudes of cyber security personnel toward CTI within the UK cyber security community [13]. The researchers used empirical research to measure to what extent the benefits and barriers suggested by the CSIS literature were reflected in the attitudes of security professionals in the UK. The study aimed to get a deeper insight in which benefits and barriers influence organizations' decision to share CTI, and why. A questionnaire was used to examine the participants' experiences with CTI, in which a total of 67 cyber security professionals were asked to agree or disagree with 28 statements related to benefits and barriers with CTI. The findings are depicted in Table 2.2. The different benefits and barriers were divided into four categories: *operational*, *organizational*, *economic* and *policy* [13].

Statement	Category	Dimension	Median (IQR)
(St1) Threat actors are deterred by intelligence sharing among organizations	Operational	Benefit	3 (2.5)
(St2) Threat intelligence sharing supports incident response efforts	Operational	Benefit	4 (2.5)
(St3) Threat intelligence sharing contributes to breach detection and recovery	Operational	Benefit	5 (2)
(St4) Sharing of threat intelligence reduces duplicate information handling	Operational	Benefit	3 (3)
(St5) Threat intelligence sharing strengthens and expands professional networks	Organizational	Benefit	5 (2)
(St6) Threat intelligence sharing validates and complements other sources of intelligence	Organizational	Benefit	5 (3)
(St7) Threat intelligence sharing improves overall security posture and situational awareness	Organizational	Benefit	5 (3)
(St8) Threat intelligence sharing enhances defensive agility and resilience	Organizational	Benefit	5 (2)
(St9) Threat intelligence sharing helps in combating cyber security skills shortage	Organizational	Benefit	4 (4)
(St10) Threat intelligence sharing reduces overall cyber security costs	Economic	Benefit	3 (4)
(St11) Threat intelligence sharing lowers cyber insurance premiums	Economic	Benefit	2 (1.5)
(St12) Threat intelligence sharing reduces uncertainty surrounding security investment decisions	Economic	Benefit	4 (3)
(St13) Threat intelligence sharing strengthens relationship with government agencies	Policy	Benefit	5 (2)
(St14) Threat intelligence sharing offers organizations liability protection	Policy	Barrier	3 (3)
(St15) Standardization issues continue to hinder threat intelligence sharing	Operational	Barrier	4 (4)
(St16) Inconsistent definitions and terminology undermine efficient threat intelligence sharing	Operational	Barrier	5 (2)
(St17) It is difficult to determine the accuracy and quality of shared threat intelligence	Operational	Barrier	5 (2)
(St18) It is difficult to ensure the timeliness of shared threat intelligence	Operational	Barrier	5 (2)
(St19) The interoperability and automation of threat intelligence sharing are difficult to achieve	Operational	Barrier	4 (4)
(St20) Threat intelligence sharing results in redundant and irrelevant data	Operational	Barrier	5 (1)
(St21) There is a shortage of analysts with the skills required to handle shared threat intelligence	Organizational	Barrier	5 (2)
(St22) It is difficult to trust the other participants in threat intelligence sharing efforts	Organizational	Barrier	3 (3)
(St23) Free riding will impede threat intelligence sharing efforts	Organizational	Barrier	3 (3)
(St24) Setting up the threat intelligence sharing infrastructure is expensive and drains resources	Economic	Barrier	5 (2)
(St25) Threat intelligence sharing erodes clients' confidence	Economic	Barrier	5 (3)
(St26) Government over-classification undermine effective threat intelligence sharing	Policy	Barrier	4 (2.5)
(St27) Privacy and antitrust legal concerns impede threat intelligence sharing	Policy	Barrier	5 (3)
(St28) Inconsistent legal frameworks undermines cross-border threat intelligence sharing	Policy	Barrier	5 (3.5)

Table 2.2: Questionnaire items and their corresponding median and interquartile range (IQR) scores, where 7 = strongly agree; 1 = strongly disagree [13].

The survey revealed that neither job position nor the respondents' organization's sector accounted for any statistically significant differences in regards to perceived benefits and barriers with CTI sharing. Even though the majority of the participants agreed that threat intelligence sharing has a positive effect on their organizations' security posture, situational awareness and resilience, several barriers undermining the effectiveness of sharing efforts were highlighted [13].

Operational At the operational level, the participants agreed that CTI sharing improves organizations' defensive agility and resilience, and supports breach detection and recovery efforts. However they agreed less to that threat actors are deterred by intelligence sharing among organizations [13]. Additionally, the participants expressed strong agreement on the difficulty to determine the quality and accuracy of the shared data, to ensure timeliness of shared intelligence, and that inconsistent definitions and terminology undermines sharing efforts [13]. This findings correspond with the findings of [30], where *quality, value and usefulness of information shared* was ranked as the second most important incentive for participating in information sharing efforts. Accordingly, there might be a misalignment between the perceived importance of the quality, value and usefulness of shared threat intelligence and the actual quality, value and usefulness of the same information, resulting in that some organizations might refrain from participating in information sharing.

Organizational The respondents agreed upon the shortage of analysts with the skills required to handle shared CTI and that sharing threat intelligence results in redundant and irrelevant data. Accordingly, this might indicate absence of a clear mandate and goals of the information sharing efforts which prevents relevant information to be shared among the participants [13]. As reported in the ENISA report [30], the presence of a clear mandate and goals of information sharing communities was highlighted as an important incentive for joining information sharing initiatives.

The UK cyber security professionals agreed that CTI sharing develops and maintains strong professional relationships. In addition to this, they were not concerned about traditional information sharing challenges such as free-riding and establishing trust. Around 56% did not agree to that it is hard to trust other participants in threat intelligence sharing efforts, whereas 60% did not consider free-riding as a significant obstacle [13].

Economic Of the attitudes regarding economic barriers to CTI, there was an agreement among the respondents that CTI sharing causes expensive infrastructure costs that may divert or drain resources from other activities. As reported in the ENISA report [30], cost savings was the most important incentive to participate in information sharing efforts. Even though the majority of respondents agreed that establishing CTI infrastructure is expensive and drains resources, they agreed that threat intelligence sharing reduces the overall cyber security costs in the long run [13].

Policy Similarly to the findings in the study examining the incentives and barriers to information sharing within EU [30], the participants agreed that CTI sharing strengthens the relationship with government agencies, even though government over-classification was perceived to undermine effective sharing of CTI [13]. Various initiatives implemented by the UK's National Cyber Security Centre was mentioned as possible solutions to facilitate closer collaboration and information sharing between the public and private sector, however, this was not described any further as it was not within the scope of the thesis of [13].

2.2.3 Perceived attitudes toward information sharing in the UK

Zibak & Simpson also used empirical research to examine cyber security practitioners' understanding and attitudes toward CSIS within the UK cyber security community [37]. The study aimed to examine the respondents' awareness of CSIS efforts and the potential impact of CSIS. The research examined four thematic areas [37]:

a) the participant's understanding and definition of the term CSIS,
b) the participant's attitudes toward different types of information sharing,

c) the maturity levels of information sharing efforts in the participants' organization, and
d) evaluation of the efficacy of information sharing efforts within the participants' organization.

A questionnaire was used to examine the attitudes regarding CSIS. A total of 41 respondents, working as either cyber security managers or analysts with a minimum one year of working experience, were included in the study. The study disclosed that there existed differentiated opinions among cyber security personnel regarding the understanding and definition of CSIS. This includes both the nature of CSI, the content itself, and the process in which the content was exchanged. While the majority of the respondents provided a limited understanding of the term, some provided more detailed definitions. Despite this, almost all of the respondents used the terms *data*, *information* and *knowledge* interchangeably to describe *cyber security information*, even though the academic literature distinguished between these terms [37].

Considering the information sharing process, the survey revealed diversified opinions related to whom to share information with. Some respondents placed emphasis on sharing information "within the same sector or industry", while others mentioned "internally", "with relevant government agencies or "disclosed to the public". Further examination of the perceptions resulted in six different information sharing forms [37]:

1. a reciprocal exchange of information between two or more organizations,
2. one or more organizations providing information to a third party or parties,
3. several organizations pooling information and making it available to each other,
4. several organizations pooling information and making it available to a third party or parties,
5. exceptional, one-off disclosures of information in time-sensitive or emergency situations, and
6. different parts of the same organization making information available to each other.

In order to measure the usefulness, willingness, participation and effectiveness of CSIS, the researchers adopted the classification framework for traditional intelligence sharing, provided by the RAND Corporation [38], and adapted it to meet the requirements of the cyber security domain. Accordingly, Zibak & Simpson defined four different information sharing categories [37]:

1. Threat data sharing,
2. Triggers for action,
3. Knowledge sharing, and
4. Expertise sharing.

The categories used in this thesis are described further in Section 3.3.3Infor-

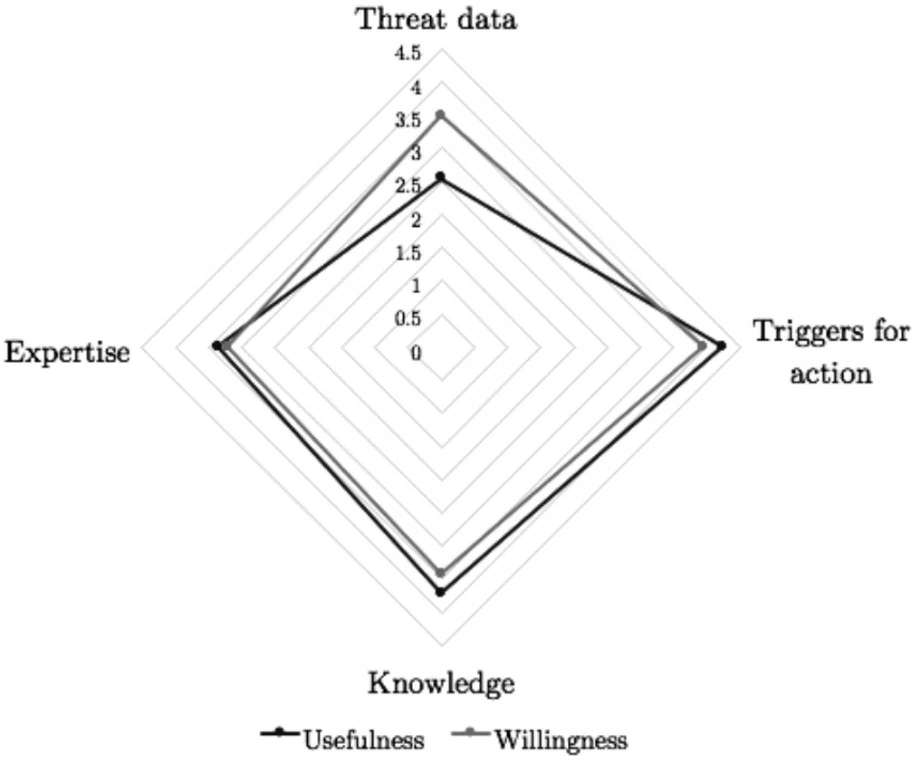

Figure 2.1: Difference between mean metric scores for the usefulness and willingness variables [13].

mation sharing categories.

The survey revealed that approximately 75% of the organizations were engaged in both *threat data sharing* and *triggers for action*, either always or often. The respondents reported that their organizations participated significantly less in *knowledge sharing*, followed by *expertise sharing* [37].

The empirical research revealed that the respondents regarded *triggers for actions* as the most useful form of information sharing, followed by *knowledge sharing*, *expertise sharing*, and *threat data sharing* as the least useful information sharing category. Regarding willingness to engage in information sharing, *triggers for action* also scored the highest among the respondents, followed by *threat data sharing*, *knowledge sharing* and finally *expertise sharing* [37].

Another interesting finding on the respondents' perceptions of the different information sharing categories, was that the respondents' willingness to participate in *threat data sharing* was reported significantly higher than the reported degree of usefulness of the same information sharing category (Figure 2.1). On the contrary, the level of perceived usefulness and willingness were rated more equally in the other information sharing categories. However, the perceived usefulness of knowledge, expertise and triggers for action sharing consistently scored higher than the perceived willingness to engage in the same categories [37].

In addition to measuring the attitudes toward the usefulness of- and the willingness to engage in the different information sharing categories, the researchers also measured the respondents attitudes toward the difficulty of evaluating both the quality of information shared in each category, as well as the effectiveness of the efforts. The survey revealed that evaluating the quality of the content was consistently perceived less difficult compared to assess the effectiveness of the information sharing efforts [37].

2.2.4 CTI sharing platforms and willingness to share CTI

In [39, p. 1409], Sillaber et al. at the University of Innsbruck used a combination of exploratory surveys, focus group discussions, and interviews to examine CTI sharing in practice. The aim of the study was to identify stakeholders' expectations to inter-organizational CTI sharing platforms and their willingness to share CTI. The participants also discussed what type of information and intelligence, including the security classification of it, they were willing to share with other participants of a CTI platform [39, p. 1410, 1412].

The study was conducted in 2016 and included 17 stakeholders representing both cyber security practitioners (e.g. cyber security analysts) and cyber security professionals at the managerial level (e.g. Chief Information Officer (CIO) or Chief Information Security Officer (CSIO)) in 17 different global organizations. The exploratory survey was conducted as a pre-study to reduce the possibilities of omitting important concepts and artifacts, and the focus group discussions and interviews were used to gain deeper insights in the stakeholders' perceptions about CTI platforms and willingness to share CTI [39, p. 1410, 1412].

Expectations of CTI sharing platforms

The study disclosed the following expectations of CTI sharing platforms [39, p. 1413-1415]:

1. CTI sharing platforms must reach critical mass,
2. Shared CTI should be more current than conventional information sources and reduce the time to detect threats,
3. CTI sharing platforms should offer social media and automated sharing functionalities,

4. CTI sharing platforms should implement functionalities to control what is shared with whom,
5. CTI sharing platforms should integrate external information sources, and
6. CTI sharing platforms should provide both qualitative and quantitative information.

The respondents stated that both the category and number of participating entities in CTI sharing were of importance. Nearly 80% of the stakeholders agreed that they expected national participants belonging to their branch of industry to join the same CTI sharing community. The remaining 20% of the respondents expected that large and medium-sized organizations participate, in addition to a mixture of businesses, academic and governmental institutions. Despite the clear expectation regarding the the type of participants, neither of the two groups managed to quantify a minimum number of respective participants [39, p. 1413]. Compared to the stated barrier related to *type of participants* and the incentive related to *processes and structures* in the ENISA report [30], inappropriate type of organizations represented within the same CTI sharing platform might act as a barrier to information sharing, especially if there is a lack of a clear mandate ensuring relevant information to be shared among the participants [30]. Accordingly, both the findings of the ENISA report, as well as the findings of Sillaber et al. [39, p. 1409] drew attention to the importance of the participants or members of a information sharing community.

The study further disclosed that all stakeholders expected that CTI sharing platforms should have automated sharing functionalities that facilitate timely sharing of actionable CTI between participating organizations in order to reduce the time to detect threats. This included, among other, CTI sharing platforms to have features like group chats, news streams, dashboards or forums, and notifications, where the participants could share timely Indicators of Compromise (IOC)s enriched with the collective knowledge and experiences of the participating experts [39, p. 1414]. The respondents in the ENISA report also highlighted timely information sharing as an important incentive for participating in information sharing efforts [30]. Despite this, Zibak & Simpson [13] reported that cyber security professionals agreed to difficulties in ensuring timely sharing of CTI. The same respondents did however not agree to that interoperability and automation of CTI sharing is difficult to achieve, indicating that timely sharing of CTI are not solely dependent on automated sharing functionalities and insufficient technology [37]. Considering the expectation of actionable CTI sharing, Zibak & Simpson [37] revealed that cyber security professionals in the UK perceived *triggers for actions* as the most useful form of information sharing, and that they were most willing to share this type of information. Accordingly, several studies supported that cyber security professionals perceive sharing of timely and actionable CTI as important, but difficult.

The fourth expectation, provided by the cyber security stakeholders, emphasized information exchange control mechanisms and filtering of received information. The stakeholders stressed the importance of control mechanisms to a) guarantee the exchange of information with trustworthy participants, b) guarantee for anonymization and c) specify whom to receive the information (e.g. one-to-one or one-to-many) depending on the sensitivity of the information [39, p. 1414]. The stakeholders argued that "unintentional disclosure of CTI to unknown third party organizations might damage the organization's reputation and put its business at risk" [39, p. 1415]. This was exemplified with scenarios like public disclosure of an encountered information leak might harm the trust relationships with customers, and that competitors can utilize information about an encountered attack to strengthen their market position, harming other competitors [39, p. 1415].

The reasons for expecting such control mechanisms corresponds with the findings in the ENISA report [30], as well as the examination of perceptions in the UK [13]. Within EU the respondents were concerned about reputational risk related to e.g leakage or sharing of sensitive or business confidential information, while the UK cyber security professionals agreed that CTI sharing could reduce a client's confidence in the organization that shares information with others. Consequently, information sharing control mechanisms are important to facilitate trustworthy information sharing that maintains the participants' reputations.

As mentioned above, the informants also emphasized the need for information filtering and subscription functionalities in order to control the information flow and prevent information overload [39, p. 1414]. The UK cyber security professionals in [13] agreed that CTI sharing lead to redundant and irrelevant data. Accordingly, in order to enable more efficient identification of relevant information and increase the value and usefulness of shared information for the participants in an information sharing community, information filtering and subscription functionalities must be integrated in CTI sharing platforms. Since the survey focused on technical measures such as expectations to functionalities in CTI platforms, social factors such as procedures and structures were not considered when discussing how to control the information flow or prevent information overload. This was however mentioned in the ENISA report, where the respondents agreed to that e.g. a clear mandate was necessary to ensure relevant information to be shared within an IE [30].

Lastly, in order to increase the value of CTI sharing platforms, the stakeholders expected that external information sources should be integrated, as well as include both qualitative and quantitative information [39, p. 1415]. The informants had varied opinions regarding what type of information to expect from a CTI sharing platform. Approximately 60% of the interviewees stated that they mainly expected quantitative information such as e.g. malicious URLs, IP addresses or email addresses, or file hashes and phishing emails. On the contrary, the remaining 40% expected qualitative threat intelligence such as contextualized quantitative information enriched by the knowledge of the other participating organizations [39, p. 1415].

Stakeholders' willingness to share CTI

The stakeholders' willingness to share CTI was examined in light of the Traffic Light Protocol (TLP). TLP is described in detail in Section 3.3.4 Information sharing controls.

The stakeholders reported that they were willing to share CTI of interest, but only within closed groups with known members. This was due to the fear of information leakage and the probability of reputational damage as described in relation to the fourth expectation in [39, p. 1415-1416].

On the other hand, the stakeholders showed more willingness to share quantitative or technical information, and reported that such information could be shared with all participating members on the CTI sharing platform. Accordingly, less sensitive information, not directly associated to a specific participant, was assessed to be more appropriate to be shared with a larger audience [39, p. 1416].

Lastly, the interviewees showed willingness to share sensitive information in an anonymized form, not traceable to the originating organization [39].

2.2.5 Cyber security practitioners' attitudes toward information sharing during cyber defense exercise

In [40], four researchers conducted a case study of two live international Cyber Defense Exercise (CDX)s to determine the attitudes of cyber security specialists toward information sharing. The study aimed to improve CTI sharing by among others examine and analyze the attitudes of cyber security practitioners during CDXs.

Since soft skills such as information sharing have a low priority during CDXs, the participants did not recognize the importance of information sharing outside the exercise [40]. Accordingly, investigating challenges and the perceived barriers of cyber security personnel to information sharing during CDXs can be used to foster the development of information sharing among cyber security personnel both during and outside CDXs.

Individual self-evaluation questionnaires before and after the exercises were used to examine among others the cyber security practitioners' soft skills (e.g. information sharing skills). In addition to this, qualitative assessments conducted by team observers from academia, industry and the national Computer Emergency

Response Team (CERT) disclosed several factors obstructing sufficient information sharing both within teams and across entities [40].

The majority of the participants in the study had either not previously participated in a CDX or only participated at one prior instance. In the first CDX nearly 60% of the participants rated their experience level as low. This indicated that the overall sample included less experienced cyber security personnel [40].

In summary, the study disclosed nine factors obstructing both proper reporting to relevant authorities and adequate communication among teams [40]:

1. A narrow focus on technical tasks,
2. Required divers technical skills,
3. No common vocabulary and taxonomy,
4. Fragmented knowledge of legal documents,
5. Missing knowledge of data exchange standards,
6. Unfamiliarity with information sharing platforms,
7. A variety/excess of communication channels,
8. Team size, and
9. Blurred benefits of skills outside the exercises.

The cyber security specialists assigned low priority to information sharing during the CDXs which emphasized on technical defense and tactics. The participants perceived technical skills more attractive and impressive than soft skills, and reporting and information sharing. According to the self-report questionnaire, only a few persons stated their desire to learn more about reporting, these persons also showed a distinctive attitude during the exercises [40].

In the study, the participants chose to assign the information sharing responsibility to either a novice cyber security specialist or to a person with a managerial background. Even though soft skills are assessed to be more important for personnel who report or share information on behalf of a technical team, technical skills of the reporter are required to excel in CSIS [40]. Accordingly, the absence of technical skills of the person assigned to report or share information demonstrates a possible challenge to information sharing.

Another factor assessed to hinder information sharing was the absence of a common vocabulary and taxonomy [40]. Similarly, in the UK study examining benefits and barriers to information sharing, the participants agreed that inconsistent definitions and terminology undermine efficient threat intelligence sharing [13].

Moreover, as Zibak & Simpson reported [13], cyber security professionals agreed that inconsistent legal frameworks undermines cross-border threat intelligence sharing. The same barrier to information sharing was also disclosed by the team observers during the CDXs. They reported that cyber security specialists need training on different reporting standards due to the wide existence of both national and international legal documents demanding different reporting procedures [40].

During the CDXs the team observers discovered a lack of knowledge about existing data exchange standards and protocols, and unfamiliarity with information sharing platforms among the cyber security specialists. Lack of such knowledge may lead to a delayed or missed utilization of threat intelligence data, as well as insufficient information sharing [40]. Accordingly, both of the discovered challenges might obstruct information sharing.

Similarly with the real world, a variety of communication channels were used during the CDXs. This lead to the information reporter being overloaded with manual tasks and multitasking. Too many communication channels prevented cyber security personnel from receiving timely, structured, relevant, correct and high-quality information in order to respond to cyber threats [40]. Almost all of the aforementioned studies [30][13][41][39] highlight timely and actionable information, as well as relevant and high-quality information, as important aspects of information sharing.

Lastly, the participants of the CDXs neither considered reporting and information sharing activities to be the primary goal of the exercise, nor to have value outside the exercise [40]. Accordingly, CDXs will not automatically lead to increased positive perceptions related to information sharing among cyber security personnel. To compensate for this, the researchers elaborated that the organizers of CDXs has the responsibility to elucidate the real value of reporting and information sharing skills [40].

2.3 Assessment of the literature review

2.3.1 Assessment of each research question

RQ1: How is CSIS performed in Norway?

Within Norway, the literature review identified one empirical study [42] that to some extent examined CSIS within the Norwegian cyber security community. However, as the study only considered the petroleum industry, it was assessed to be too limited to fully answer RQ1. Accordingly, the literature review revealed that it was a lack of empirical research considering how CSIS is performed in Norway.

In order to answer how CSIS is performed in Norway, grey literature were used to answer theoretically how it is and should be done, while empirical surveys were conducted to examine how CSIS is practiced in Norway. The literature used to answer RQ1 were based on formal documentation such as national strategies, the Security Act, and propositions to the Norwegian parliament (i.e. new legislation or amendments to legislation). This literature were used to give a brief introduction to the Security Act, different information sharing controls relevant for the Norwegian cyber security context and a brief depiction of the Norwegian cyber security landscape. This is elaborated in Chapter 3 Theory. The surveys were utilized to examine how CSIS is practically performed in Norway (e.g. whom share information with whom, how often is information shared, what type of information is shared, why does organizations share information, etc.). This is further elaborated on in Section 4.4.1 Questionnaire design and Section 4.5.1 In-depth interview design. The in-depth interviews answered this research question to a greater extent than the questionnaire, as the interviewees were able to provide detailed information and experiences of how CSIS is performed in Norway.

RQ2: How is CSIS perceived among cyber security professionals within the Norwegian cyber security community?

No former relevant empirical research on Norwegian cyber security professionals' attitudes toward CSIS were identified in the literature review. Despite this, several foreign empirical studies considering perceptions toward either CSIS or CTI were identified in [30], [13], [39, p. 1409-1420] and [40]. As none of the studies examined perceptions and attitudes toward CSIS within the Norwegian cyber security community, the relevance and applicability to the Norwegian cyber security community of each study were evaluated to determine whether the RQ2 and its sub-questions could be answered by already existing literature.

Due to the extensive development of technology since the ENISA study was performed in 2010 [30], it was uncertain whether the findings of the study were still valid, and whether the findings were valid within the Norwegian context. An additional reason for being cautious with generalizing the findings to a Norwegian context is due to the limited number of respondents and interviewees. The study is however partially relevant for RQ2 as it includes perceived incentives and barriers to information sharing. Accordingly, some of the findings still might be representative in the Norwegian cyber security community.

As the study in [39, p. 1409-1420] was limited to information sharing by CTI sharing platforms, and perceptions among international cyber security professionals, the findings did not adequately answer RQ2.

In [40] both incentives and benefits, in addition to challenges with information sharing during CDXs were examined. Due to the low experience level among the participants, unknown nationality of the participants, and that the observations were done during exercises in stead of a real life settings, the findings did not adequately answer RQ2.

The research in Zibak & Simpson [13] was assessed to be the most relevant empirical study contributing to answer RQ2 as the findings might be valid for the Norwegian cyber security community. However, a number of factors made it difficult to assess the applicability to the Norwegian cyber security community: 1) the sample size is relatively small considering the size of the UK cyber security community, reporting on the response rate is absent, difficulty of verifying self-reported data, and not every sector were represented in the sample. Zibak & Simpson [13] also stressed that CTI sharing might be very specific to both countries and industries and, therefore, attitudes toward information sharing might vary in different communities. Additionally, since the study only examined attitudes toward information sharing by using quantitative data, there is a lack of depth, possible explanations and nuances in the reported attitudes among the participants.

As non of the identified empirical studies were assessed by the researchers to be generalizable to the Norwegian cyber security community, no former research fully answered RQ2. Accordingly, in order to answer RQ2, a survey was conducted to examine perceptions and attitudes toward CSIS of Norwegian cyber security professionals. The questionnaire in [13] was assessed to provide relevant data and was therefore replicated in this thesis to examine perceptions with regards to operational, organizational, economic and policy factors within the Norwegian cyber security community. The list of recognized benefits and challenges in Table 2.1 were used as a baseline for the empirical research aiming to answer RQ2.

RQ3: What is the perceived usefulness and willingness in sharing CSI within the Norwegian cyber security community?

Similarly with RQ2, no former empirical research on Norwegian cyber security professionals' willingness and perceived usefulness of CSIS were identified in the literature review. Only two empirical studies examining willingness to share either CSIS or CTI were identified in the literature review.

The identified incentives and barriers to sharing information identified in both the ENISA report [30] and the research of Zibak & Simpson [13] might represent factors that affect the usefulness of- (RQ3-1) and willingness to share (RQ3-2) CSIS. However, the studies did not examine perceptions within the Norwegian cyber security community, and were therefore assessed to not adequately answer RQ3.

Existing literature regarding willingness to share information was covered in several empirical studies using different survey methods such as a questionnaire in [37] and focus group discussions in [39, p. 1409-1420]. Due to the limitation of this thesis where willingness of information sharing initiatives within the Norwegian cyber security community was examined, neither of the studies directly answered RQ3-2, as the study in [37] examined attitudes in the UK and the nationality of the personnel participated in [39] were unknown. Additionally, the study in [39] did not primarily seek to examine willingness to share CTI, and therefore the findings related to willingness were few and limited to sharing information on CTI platforms. The study in [37] however, was more specified in examining the attitudes toward willingness to share CSIS.

The empirical study in [37] also examined attitudes toward usefulness of CSIS within the UK cyber security community. Therefore, the study in [37] was assessed as partially relevant for RQ3 as the findings might be valid for the Norwegian cyber security community. However, due to a small sample size dominated by large organizations, and absent from some sectors, as well as the difficulty of verifying self-reported data, it was challenging to determine whether the findings were applicable to the Norwegian context. Despite this, the questionnaire used in the study was assessed to provide relevant data for answering parts of RQ3, and were therefore utilized as a template for the survey conducted in this thesis. Accordingly, the CSIS categories used in [37] were also used in the survey of this thesis to make the findings comparable to the UK study.

2.3.2 Overall assessment of the literature review

The analysis of existing literature revealed few existing empirical studies regarding CSIS. Most of the existing literature regarding information sharing or information exchange comprise theoretical literature on cyber security and threat information sharing such as theoretical research, white papers, standards, and guidelines. The literature review has shown that almost every identified empirical research related to CSIS were conducted outside Norway, and had not representative samples based on the target population: small sample sizes, low experience with cyber security among the respondents, absence of either industries, sectors or organizations size, etc. Accordingly, the individual evaluation of each study revealed that none of the empirical studies in Section 2.2 Empirical research on CSIS fully answered any of the RQs.

To the best of the researchers' knowledge, no prior extensive empirical research that examine perception and attitudes toward CSIS has been conducted in Norway. Accordingly, in order to answer the research question of this thesis two surveys were conducted to examine perceptions and attitudes toward CSIS within the Norwegian cyber security community.

In order to answer the research question, the surveys conducted by Zibak & Simpson in both [13] and [37] were used as a template for the surveys in this thesis. To answer RQ2, the researchers wanted to get a deeper understanding of which benefits and challenges are affecting individual's and organizations' decisions to share CSI, and why. Accordingly, the questionnaire in [13] were replicated with minor adjustments to fit into the Norwegian context. Furthermore, as [37] examined attitudes toward CSIS and different types of information sharing, parts of this study were also replicated in order to answer RQ3.

Theory

This chapter includes theory and background information relevant to the thesis and is the foundation for the analysis, integration and interpretation later in the thesis. Covered topics are: an introduction to the Norwegian Security Act and Fundamental National Functions (FNF), definitions and categorizations related to information sharing, and lastly an overview of the Norwegian cyber security landscape.

3.1 Definitions

3.2 National security

Norwegian legislation has a strong separation of national security and public security. The purpose of the Security Act is to ensure national security interests. Thus it is mainly other sectoral regulations that ensure public security. While the main instruction relevant to public security[1] is aimed at securing the continuity of critical societal functions like the public's access to food, water etc. and has an "all-hazards" perspective, the purpose of the Security Act is to protect national security interests against *intentional acts* by adversaries or hostile actors [44].

3.2.1 Introduction to the Norwegian Security Act

The Act relating to national security, abbreviated to the Security Act, has a three part purpose [45]:

a) protect Norway's sovereignty, territorial integrity and democratic system of government, and other national security interests,
b) prevent, detect and counter activities which present a threat to security,
c) ensure that security measures are implemented in accordance with the fundamental legal principles and values of a democratic society.

The societal development has actualized and reinforced the need for a more holistic approach to national security. An increasing degree of digitization has resulted in increased interdependencies across traditional societal divisions: between private and public organizations, and between civilian sectors and the Nor-

[1] Instructions for the Ministries' work with civil protection and emergency preparedness [43].

wegian Armed Forces and defence sector. At the same time, the emergence of a network-based society has led to the same divisions becoming less distinct. This development has been positive and given rise to an advanced society, but also new vulnerabilities. In order to meet both old and new challenges, the Security Act was revised in 2019. The revised act is intended to ensure both individual sectors' peculiarities and the need for a cross-sectoral and holistic management of national security [2].

The new Act acknowledges the role private undertakings play in ensuring national security to a greater extent. This resulted in an extended scope including both private and public organizations in its application. Thus, the Security Act applies to both governmental, county and municipal bodies, but also suppliers of goods and services related to classified procurements. Within their respecting area of responsibilities, a ministry may decide that the act shall apply wholly or partly to otherwise excempted undertakings if said undertakings either handle classified information; control information, information systems, objects or infrastructure which are of vital importance to FNFs; or engage in activities which are of vital importance to FNFs [45].

3.2.2 Fundamental national functions

This subsection is intended to describe the nature, need and purpose of Fundamental National Functions (FNF). In the Norwegian Security Act, FNFs are defined as [7]:

> "*services, production and other types of activity which are of such importance that a complete or partial loss of the function would have consequences for the State's ability to protect national security interests*"

This definition is intended to be broad in order to provide flexibility to a legislation which is aimed to be dynamic [44]. Several other nation states have also initiated similar frameworks to that of the Norwegian FNF initiative, of which the United States initiative of National Critical Functions (NFC) [46] and the United Kingdom's Critical National Infrastructure (CNI) [47] are notable examples.

Even though other nations' national risk management systems are outside the scope of this thesis, both the Norwegian, UK and US initiatives are all the result of an emergent need of considering risks and ensuring resiliency by avoiding traditional compartmentalization and division of responsibility. As shown in Table 3.1, the definitions of what the different risk management initiatives are intended to ensure highly resembles each other. But there are some apparent differences in how the different initiatives are presented: Whereas the Norwegian and US initiatives focuses on functions as a broader categorizing term and subsequently analyzing these to identify vital undertakings and objects, the UK initiative is to a larger extent focused on physical and logical entities within respective sectors,

Country	Designation	Definition
Norway	Fundamental National Functions	Services, production and other types of activity which are of such importance that a complete or partial loss of the function would have consequences for the State's ability to protect national security interests [45].
United States	National Critical Functions	The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof [46].
United Kingdom	Critical National Infrastructure	Those critical elements of Infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life [50].

Table 3.1: Comparison of Norwegian, U.S., and U.K. national cross-sectoral risk management initiatives.

which in sum constitutes the vital entities of a functioning society.

All presented frameworks are heavily linked to cyber security, but also incorporates physical security to ensure a holistic approach. In Norway, the Norwegian National Cyber Security Centre (NCSC) provides cyber expertise in national assessments and by advising private and public undertakings and organizations in how to best maintain their cyber security posture. The assessments and situational understanding of NCSC is then implemented in the overall security picture in their subordinated body National Security Authority (NSA) [48]. The U.K. and U.S. have similar approaches. The U.K. National Cyber Security Centre (NCSC) is responsible for the same responsibilities as its Norwegian counterpart, but is subordinated to the intelligence, security and cyber agency Government Communications Headquarters (GCHQ) [49]. In the U.S., the framework itself is enforced by National Risk Management Center (NRMC), which in turn is subordinated to the Cybersecurity and Infrastructure Security Agency (CISA) - clearly addressing the importance and societal dependency on the cyber domain.

In Norway, the need for developing a national framework based of FNFs was identified in the Norwegian Official Report 2016:19 (*Norges offentlige utredninger - NOU*) [2]. According to the committee of NOU 2016:19, the most vital task of a nation state is protecting the citizens and the society they are part of - a state which is unable to ensure its own and its citizens' survival is in breach of the social contract between the state and its citizens. In order to carry out this task and comply with said social contract, it is vital that the state is able to maintain society's fundamental functions regardless of what external influence they are subject to. In the report, the committee presented a number of key findings and recommendations to address the emergent risk landscape [2]:

- The purpose of the revised law should be to protect FNFs, as it are these functions that a threat actor will seek to target in an attack to neutralize Norway's most fundamental interests,
- undertakings of vital importance to FNFs should be subject to the act, regardless of ownership or organization. Additionally, all information systems vital to FNFs should be subject to the Security Act,
- the general principles for crisis management and readiness should be maintained, while the need for a holistic and cross-sectoral approach to security is addressed,
- the Norwegian authorities should be required by law to advise undertakings subjected to the law, and a duty to facilitate the sharing of security information to relevant parties.

3.2.3 Classification of critical national assets

To assess importance and ensure correct and proper priority by the Norwegian government when implementing protective measures and defensive activities [51], the Security Act defines a categorization of criticality as "Fundamental National Functions may be harmed if their function is reduced or they are subjected to vandalism, damage or unlawful seizure" [45]. The entities that fall under the term "critical national objects, infrastructure or information systems" (hereby commonly denominated under the term "critical national assets") are classified based on the following categorization [45]:

a) HIGHLY CRITICAL if critical adverse consequences could result,
b) CRITICAL if serious adverse consequences could result,
c) IMPORTANT if adverse consequences could result.

The classification is based on a damage potential assessment, in which the FNF being supported or ensured by the object or infrastructure in addition to the consequences of reduced functionality is specified. The entities are listed and maintained in an overview of FNFs and undertakings of material importance to the FNFs at both the ministerial level. NSA has the overall responsibility for controlling the state of security in all sectors, including ensuring that the undertakings comply with their duties under the act [45]. A depiction of the hierarchical

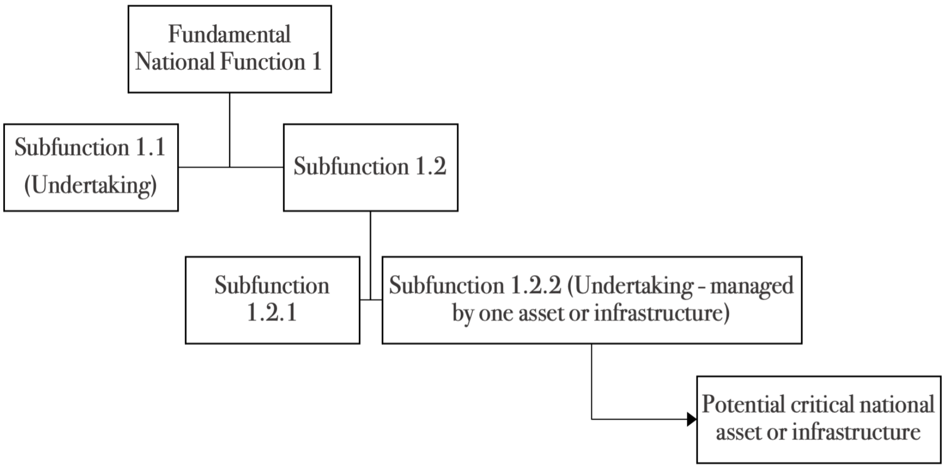
Fundamental National Function 1
Subfunction 1.1 (Undertaking)
Subfunction 1.2
Subfunction 1.2.1
Subfunction 1.2.2 (Undertaking - managed by one asset or infrastructure)
Potential critical national asset or infrastructure

Figure 3.1: Hierarchical example on how undertakings and governmental organizations in conjunction constitute Fundamental National Functions [52]. Note that each function is divided into subfunctions until relevant individual undertakings and their critical national assets are identified.

structure of FNFs is shown in figure 3.1, and a simplified flowchart depicting the ministries' process for identifying, subjecting and classifying undertakings is depicted in figure 3.2.

However, NSA also states that there must be a high threshold for designating critical assets, and that the ministries must not classify larger components of assets or give a higher classification than necessary [53].

3.2.4 The interdependencies of value and supply chains

Value chains are growing ever more relevant, especially within the cyber domain. Often, suppliers rely on contractors, which in turn rely on their own subcontractors. This creates challenges when mapping dependencies both in the physical and digital domain, in addition to collating and assessing whether apparent unrelated security threatening events may in fact be linked to an intentional campaign by a hostile actor. Additionally, an undertaking may have impenetrable security measures in all domains within their organization, but may be vulnerable due to an exploitation of a vulnerability in their supply chain which they do not control and may not be aware of [54]. Some notable examples of these supply chain attacks are the Stuxnet virus and the 2016 attack against the Ukrainian power grid.

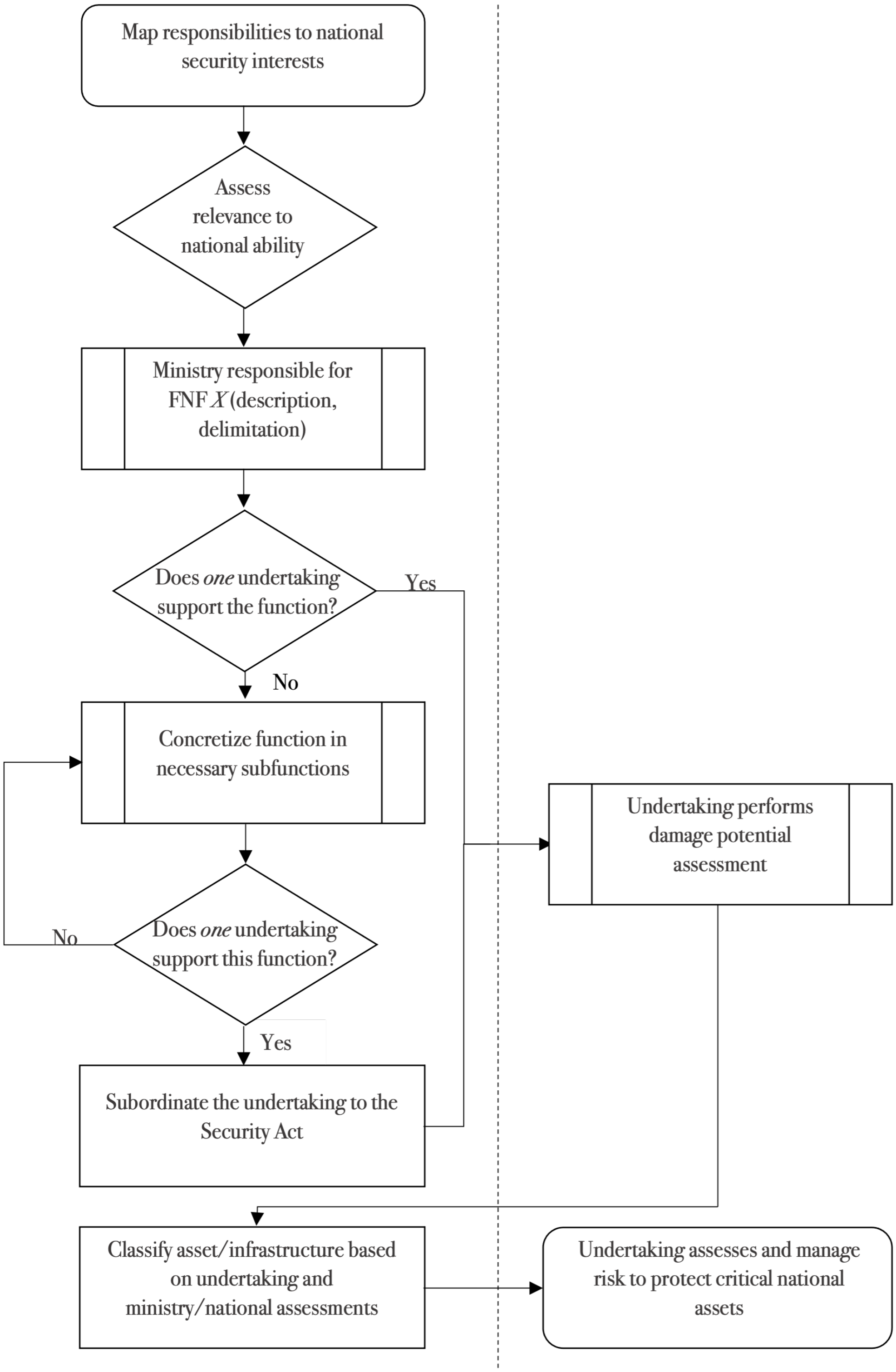
Map responsibilities to national security interests
Assess relevance to national ability
Ministry responsible for FNF *X* (description, delimitation)
Does *one* undertaking support the function?
Yes
No
Concretize function in necessary subfunctions
Undertaking performs damage potential assessment
No
Does *one* undertaking support this function?
Yes
Subordinate the undertaking to the Security Act
Classify asset/infrastructure based on undertaking and ministry/national assessments
Undertaking assesses and manage risk to protect critical national assets

Figure 3.2: Simplified flow chart depicting how Fundamental National Functions are determined [52]. The flow chart is divided between processes from a ministerial point of view on the left and from the undertakings' point of view on the right.

3.3 Information sharing

In this thesis, *information sharing* is understood as the act when people or entities pass information from one to another. Even though the literature differentiate between *data*, *information* and *intelligence*, *information* in relation to *information sharing* is used as a general term for both data, information, intelligence and knowledge in this thesis.

3.3.1 Cyber security information sharing

Cyber Security Information Sharing (CSIS) is understood as sharing of any information that can help an organization identify, assess, monitor, and respond to cyber threats. CSIS includes information sharing on vulnerabilities as well as Cyber Threat Intelligence (CTI), such as Indicators of Compromise (IOC), Tactics, Techniques, and Procedures (TTP) used by threat actors, suggested actions to detect, contain, or prevent attacks - and the findings from incident analysis [20].

3.3.2 Horizontal and vertical information sharing

Security personnel within an organization may participate in several external coordination arrangements and information sharing fora routinely or in relation to cyber security incidents. Within the thesis, *horizontal* and *vertical information sharing* are used to describe the two lines of communication when an entity shares information with another entity.

NIST SP 800-61 Computer Security Incident Handling Guide proposes three different coordination relationships when an entity collaborates with external entities. The following relationships are: *team-to-team*, *team-to-coordinating team* and *coordinating team-to-coordinating team* [55]. These relationships and their associated properties are used to describe horizontal and vertical information sharing in more detail.

Some sharing relationships are mandatory, while others are voluntary. Mandatory sharing are often defined by a regulatory body within a specific domain [55]. Within Norway, mandatory CSIS is primarily regulated by the Security Act if the undertaking is subjected to the act (this process was depicted in Figure 3.2), or contractual requirements from one organizations to another. Voluntary sharing are often considered mutually beneficial by the participating entities [55].

Horizontal information sharing is when information is shared between two entities at the same hierarchical level. Such sharing relationships could be:

1. Team-to-team,
2. Coordinating team-to-coordinating team (on same hierarchical level).

Some examples of horizontal sharing relationships are between KraftCERT and HelseCERT, between Norwegian Police Security Service, Norwegian Intelligence Service and National Security Authority, or between two independent undertakings.

Vertical information sharing, on the other hand, is when information is shared between two entities at different hierarchical levels. Examples of vertical sharing relationships are when an undertaking shares information with the NSA or vice a versa, or when a sectoral response unit shares information downward (*top-down sharing*) with its members or upward (*bottom-up sharing*) to NCSC. Vertical sharing relationships could be:

1. Team to coordinating team,
2. Coordinating team to coordinating team (on different hierarchical levels).

3.3.3 Information sharing categories

As discussed in the introduction to this section, there are several possible categorizations and definitions of information sharing categories. In this thesis, the number of categorizations is limited to four exclusive types to limit the complexity during the survey and discussion later in Chapter 6 Discussion. The different categories of information sharing used in this thesis are based on what is being shared and the outcome it is designed to achieve [38]. To achieve applicability in comparing the results to that of other existing studies, the categories highly resembles that of Zibak & Simpson [37] and Jackson [38].

Data sharing

The first category - *data sharing* - aims to give a receiving organization a more complete picture of the nature of a cyber security threat, incident or vulnerability. The main goal of this type of sharing is "to inform a decision or assessment or to increase the chance of a successful detection of, triage of, and response to, cyber threats" [37]. Such information can be shared in e.g. intelligence reports or similar products. An example of threat data sharing is when an organization within e.g. the health sector experiences a cyber attack: In order to help similar organizations to detect the threat in question, the victim organization shares among others IOCs such as the IP address of the attacker. Accordingly, the receiving organization can investigate whether their systems are targeted by the same attacker.

Alerts & triggers for action

The next category is called *alerts & triggers for action*. This type of information sharing includes the sharing of information relevant to another organization that are in a position to act upon it. Such information often seek to direct the receiving organization to an unknown threat or vulnerability, and often bring to attention the need for decisions of the receiving organizations did not know prior to the alert [38][37]. In this type of information sharing, timeliness is more important than the degree of data processing and confidence in assessments.

Triggers for action are often communicated through warnings from national services [37]. An example is the warning disseminated by the Norwegian NCSC during April 2022 regarding the increased cyber threat related to the Ukrainian war. The warning informed about the threat from Russian state-sponsored threat actors and criminal organizations against critical national infrastructure, especially against the petroleum and energy industry [5]. The warning also provided guidance for cyber security enhancement, incident response and security reporting of possible malicious activity.

Knowledge sharing

Knowledge sharing differs from the above-mentioned categories as this type is not intended to share immediate or time-sensitive information, but aims to build a common pool of knowledge, advisories and lessons learned across different organizations [37][38].

Knowledge sharing focuses on education and to raise general awareness about cyber security. Examples of such efforts are sharing of post-breach reports, case studies, analytical products such as intelligence and security bulletins provided by security vendors, etc. [37]. As exemplified above, knowledge sharing can vary in both formality, format and dissemination method.

Expertise sharing

The goal of *expertise sharing* is to bring together individuals from separate organizations to exchange and apply multidisciplinary expertise to tackle common security issues or challenges [37][38].

Although similar, expertise sharing is more than knowledge sharing as it brings people and their expertise together either physically or digitally. Expertise sharing may be a necessity for an organization to be able to apply and achieve the full advantage of received security information. Accordingly, expertise sharing may provide the needed security skills or capabilities for an organization without requiring specific security investments [37].

This type of information sharing effort could be a fusion center that collocates security personnel from multiple organizations, or Computer Emergency Response Team (CERT)s where a diverse group of researchers, software engineers and security- and intelligence analysts from various sectors including government, industry and academia works together with cyber security, developing methods and tools to counter cyber threats. In Norway, Norwegian Joint Cyber Coordination Centre (JCCC)[2] is a prime example of an cyber security fusion center established to strengthen Norway's ability to effective defense against - and response to severe incidents and crime in the digital domain [3].

3.3.4 Information sharing controls

There are several methods to a) protect information and b) restrict sharing of information within the Norwegian context, referred to as *information sharing controls*. Such mechanisms are often related to legislation, or less formal sharing restrictions such as standards, agreements, customs, etc. The main difference between security classification controls (a) and dissemination controls (b), is that security classification controls focus on the potential harm of disclosure, while dissemination controls focus on how far and to whom information can be disseminated [1]. Within the scope of this thesis, relevant information sharing controls are information protection and restrictions related to the Security Act, as well as the Traffic Light Protocol (TLP) and Chatham House Rule.

Protection and restrictions related to the Security Act

As the thesis aimed to examine aspects of information sharing between the private and public sector while focusing on entities ensuring or participating in FNFs, several of the sample entities were subject to the Security Act. Accordingly, information sharing restrictions and protection related to the Security Act represent an important role in light of information sharing within the Norwegian cyber security community.

According to the Security Act, *critical national information* is any information where national security interests could be harmed if the information becomes known to unauthorized persons, is lost, is altered or becomes inaccessible [7]. Critical national information is not the same as *classified information*. Classified information is critical national information where the confidentiality must be protected with respect to national security interests. Classified information shall only be released to persons who have an official *need-to-know* and are authorized to have access to such information. Unclassified critical national information, on the other hand, is information assessed to be nationally critical where the availability and integrity must be protected with respect to national security interests [56].

Undertakings which produce information must assess if the information is nationally critical, and whether it is classified or unclassified. Classified information must be assessed with respect to the consequences of national security interests. The Security Act §5-3 defines the different security classification levels as [7]:

[2] JCCC is a translation of the Norwegian entity Felles cyberkoordingeringssenter (FCKS).

a) TOP SECRET (STRENGT HEMMELIG) if critical adverse consequences could result
b) SECRET (HEMMELIG) if serious adverse consequences could result
c) CONFIDENTIAL (KONFIDENSIELT) if adverse consequences could result
d) RESTRICTED (BEGRENSET) if adverse consequences could result to some extent.

For a person to get access to information with a classification of CONFIDENTIAL or higher must hold a valid security clearance [57]. According to NSA [57], one of two prerequisites must be in place in order to obtain a security clearance: 1) If the person is employed in an enterprise subject to the Security Act, or 2) employment in an enterprise which performs classified assignments for a public enterprise.

In Norway, National Restricted Net (NRN) facilitates exchange of low-level classified information within the civil service[3] to ensure more effective preparedness and crisis management. NRN is an important measure to improve effective exchange of information between governmental entities, ministries and relevant public and private entities [58]. The NRN is intended for both public and private undertakings subject to the Security Act.

Protection and restrictions related to the Information Protection Instruction

Instructions for the handling of records that need to be protected for reasons other than those set out in the Security Act and associated regulations, abbreviated to Information Protection Instructions, is applied in cases when content of a record could harm public interests, a business enterprise, an institution or an individual if it becomes known to unauthorized persons [43].

Traffic Light Protocol

Traffic Light Protocol (TLP) is defined by Forum of Incident Response and Security Teams (FIRST) and was created to facilitate both greater sharing of potentially sensitive information and more effective collaboration within the Computer Security Incident Response Team (CSIRT) community and its operational partners worldwide. TLP does not provide a formal classification scheme, however it provides a simple and intuitive schema indicating with whom potentially sensitive information can be shared. TLP is widely applied within the Norwegian cyber security community. TLP defines four different labels to indicate the sharing restrictions of the information shared to one or several recipients [59]. The labels are:

a) TLP:RED
b) TLP:AMBER
c) TLP:GREEN

[3] The civil service is an English translation of the Norwegian body Statsforvaltningen.

d) TLP:CLEAR

A more detailed description of the TLP labels are shown in Table 3.2.

When using TLP to control sharing of potentially sensitive information, the source is responsible to ensure that the recipients understand and adhere to both the TLP sharing guidance and additional specific sharing restrictions given by the source. A recipient can ask for and obtain permission from the source of the information to share the information more widely than the original TLP label indicated [59].

In order to understand the different TLP labels, the standard has defined three entity groups related to the recipient of any shared information. A *community* is "a group who share common goals, practices, and informal trust relationships" [59], such as all cyber security practitioners in a country, a sector or a specific region. An example of such a community is the Norwegian cyber security community. An *organization* is "a group who share a common affiliation by formal membership and are bound by common policies set by the organization" [59]. An organization could be all members of an information sharing organization. Within the Norwegian context, an organization could be HelseCERT. The last category is *clients* which are "those people or entities that receive cybersecurity services from an organization" [59]. An example is one of the members of HelseCERT which is defined as a client. Clients are by default included in TLP:AMBER in order for clients to take action to protect themselves [59].

Since the TLP standard does not explicitly describe how to use TLP in meetings or other types of oral information exchange, the Chatham house rule might be an alternative method to restrict the sharing of potentially sensitive information.

Chatham House Rule

The *Chatham House Rule* aims to create trusted environments to understand and resolve complex problems. The Rule is defined as [60]:

> *"when a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."*

Meetings to be held under the Rule does not have to take place at the Chatham House or be organized by Chatham House. Any group can use the Rule as a pre-agreed guide when having a meeting or event [60].

TLP label	Description
TLP:RED	For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.
TLP:AMBER	Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TLP:AMBER+STRICT restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.
TLP:GREEN	Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.
TLP:CLEAR	Previously known as TLP:WHITE in TLP version 1.0. Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

Table 3.2: Table of TLP labels according to TLP version 2.0 [59].

3.4 The Norwegian cyber security landscape

This section is intended to give a brief description of the current Norwegian cyber security landscape based on operational, political and strategic documents from the Norwegian authorities. National Services, cyber security organizations and Sector Response Entities (SRE) (later described in Section 3.4.2 Cyber security organizations and SRE) and the role and responsibility of individual undertakings are covered in turn.

3.4.1 National services

According to the Norwegian Parliamentary Oversight Committee on Intelligence and Security Services, the Norwegian national or so-called "secret" services are the Norwegian Police Security Service (NPSS), Norwegian Intelligence Service (NIS), Norwegian Defence Security Agency (NORDSA) and National Security Authority (NSA) [61].

This differs from the entities represented in the Norwegian Joint Cyber Coordination Centre (JCCC): NSA, NIS, NPSS and the Norwegian National Criminal Investigation Service (NCIS). The JCCC is tasked with strengthening the national ability to efficient defense against, and response to serious cyber attacks and crime in the cyber domain [3]. Additionally, the center provides strategic analysis and maintains a comprehensive threat and risk assessment of cyberspace [62]. The JCCC is a permanent and co-located body, consisting of permanent representative from each of the entities. However, the Center is not an independent body with independent decision-making authority [3].

The JCCC is limited to serious incidents in the cyber domain through coordinating the represented entities' efforts, contributing to more efficient use of national resources, strengthening information sharing as well as ensuring coordinated warning and production of comprehensive assessments for superior authorities. The center is not a resource that undertaking can turn to for assistance with handling cyber attacks [3].

Thus, the entities represented in NCSC is used when discussing *national services* in this thesis. Each national service and their respective area of responsibility is briefly explained below.

Norwegian National Security Authority

With each ministry being responsible for protective security work in their areas of responsibility (ergo also deciding which undertakings and bodies are subjected to the Security Act), the NSA is affirmed as having the cross-sectoral responsibility for ensuring that undertakings are in accordance with the act [45]. This includes compliance supervisions, inspections, maintaining an overview of functions and undertakings, and assist in the development of security measures related to protective security work. However, the NSA is also responsible for facilitating the exchange of threat assessments and other security information, as stated in the Security Act §2-3 [45].

As detailed in Section 3.2.1 Introduction to the Norwegian Security Act, the NSA is responsible for facilitating that all undertakings covered in the act have access to threat assessments and other relevant information to the undertakings' protective security work. This also includes the establishment of necessary forums for exchanging information and experience [45], which is further covered in sections Section 3.3 Information sharing and Section 3.4 The Norwegian cyber security landscape.

NCSC, NorCERT and WSDI The Norwegian National Cyber Security Centre (NCSC) is a national and international arena for cooperation in detection, response, analysis and counseling in the field of cyber security. The centre includes partners from businesses, academia, military and the public sector who actively contribute to mutual cooperation to ensure a more robust digital Norway. NCSC is also responsible for operating the Norwegian Computer Emergency Response Team (NorCERT) - a national response function for serious cyber attacks and a National Warning System for Digital Infrastructure (WSDI) [45].

The WSDI is intended to detect and give warning on malicious cyber operations inflicting Norwegian critical infrastructure or critical functions. To ensure the effectiveness and operation of NorCERT, the CERT bases its collection and subsequent verification, analysis and dissemination on information on vulnerabilities, risks, attack vectors and malicious code, on information gained through WSDI. The WSDI consists of a sensor network in selected governmental and private organizations which controls critical infrastructure in their ICT networks. The WSDI only fulfill a complimentary role to that of the organizations' own security measures, and all affiliated undertakings thus are obligated to ensure security of their own systems, regardless of participation in WSDI [63].

The NorCERT also exchanges information with other national and international partner organizations, which according to [63] is vital for the coordination and support of both domestic and foreign partners. According to the same source, the national ability of respond to serious cyber attacks depends on an effective cooperation between the Norwegian intelligence, surveillance and security services. NorCERT as part of NSA also cooperates with a number of other governmental and private partners. NSA has responsibility as the coordinating entity to the national sectoral CERTs and individual undertakings, as previously described in Section 3.2.2 Fundamental national functions.

Norwegian Intelligence Service

The Norwegian Intelligence Service (NIS) is the Norwegian national foreign intelligence service. NIS is responsible for assisting the Norwegian government and supporting decision-makers in foreign, security and defence matters. Within the cyber security community, NIS has a cross-sectoral national responsibility in times of peace, crisis and armed conflict to, among others, detecting foreign threats and provide intelligence on foreign threat actors in cyberspace. Additionally, NIS is responsible for other offensive cyber operations (including active defensive cyber operations against foreign targets within the confines of international and Norwegian law) [3].

Norwegian Police Security Service

The Norwegian Police Security Service (NPSS) is a police agency in addition to Norway's domestic security and intelligence service, reporting directly to the Ministry of Justice and Public Security. NPSS is tasked to protect democracy, its citizens and vital societal interests through detecting, preventing and investigating espionage, terrorism, the proliferation of weapons of mass destruction and threats to government officials. NPSS is also tasked to produce analyses and threat assessments for decision-making within the NPSS's own preventative activities, superior bodies and others in need of this type of information. As with NSA and NIS, NPSS is a permanent member of JCCC [3].

Norwegian National Criminal Investigation Service

Norwegian National Criminal Investigation Service (NCIS) is the national entity for combating organized and other serious crime, including computer crime. NCIS is subordinated the Norwegian Police Directorate, and has specialist expertise in criminal intelligence and technical & tactical computer crime investigations. NCIS has a designated computer crime unit which conducts intelligence, preventative efforts and investigations, as well as assisting the police and superior prosecuting authorities. The unit for internet-related investigative support assists with securing electronic traces and evidence [3].

3.4.2 Cyber security organizations and SRE

Cyber security organizations In this thesis, the term *cyber security organization* is used to categorize all incident management and cyber security structures, e.g. CERT, CSIRT, SOC and ISAC. Even though the different organizational types have different scopes and focuses, they all engage in the processing and dissemination of CSIS to some extent. A brief description of each main cyber security organizational type is given below.

Computer Emergency Response Team (CERT) - A CERT is, although many companies use the term generically, a registered trademark and is intended to operate as a partner with government, industry, law enforcement and academia to improve the security and resilience of computer systems and networks [64]. A CERT is intended to study problems that have widespread cyber security implications and develop advanced methods and tools [64].

Computer Security Incident Response Team (CSIRT) - A CSIRT is defined as: "... A concrete organizational entity (i.e. one or more staff) that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident" [65]. A CSIRT may vary in purpose based on sector and the intended purpose. For instance, government CSIRTs may focus on security awareness training and incident handling, whereas law enforcement CSIRTs may focus on prosecuting cybercrime incidents by collecting and analyzing computer forensics data from affected or involved systems [65].

Security Operations Center (SOC) - A SOC generally encompasses multiple aspects of security operations, while CSIRTs, CERTs etc. generally focuses specifically on incident response [66]. A SOC's area of responsibility may include the incident response function as well as other tasks, including [66]:

- Monitoring operations and controls, as intrusion detection, system/intrusion prevention system, security information management,
- Evaluate operational and security telemetry and information gathering,
- Manage identity management and authorization, firewall and filtering ruleset maintenance, forensics and investigation support etc.

Information Sharing Analysis Center (ISAC) - ISACs provide a central resource for gathering and processing information on cyber threats, in addition to allowing information sharing between the public and private sector about root causes, threats and incidents, as well as sharing experience, knowledge and analysis [67]. The formation and use of ISACs are wide-spread in the European Union.

Sector response entities Norwegian national security is dependent on cooperation and security efforts of both public and private entities which in sum support FNFs. These FNFs span across different sectors, whereas CERTs and other cyber security organizations are mainly organized per sector or government ministries. The challenge is further complicated as most public and private entities have long, complex supply chains, spanning across national borders.

Security reporting and incidents from each value chain supporting a FNF must be reported to the respective ministry, whereof most ministries have their own appointed cyber security organization, called Sector Response Entities (SRE). Eventually, security reporting from every security organization will terminate at the Norwegian National Cyber Security Centre (NCSC), which maintains the national

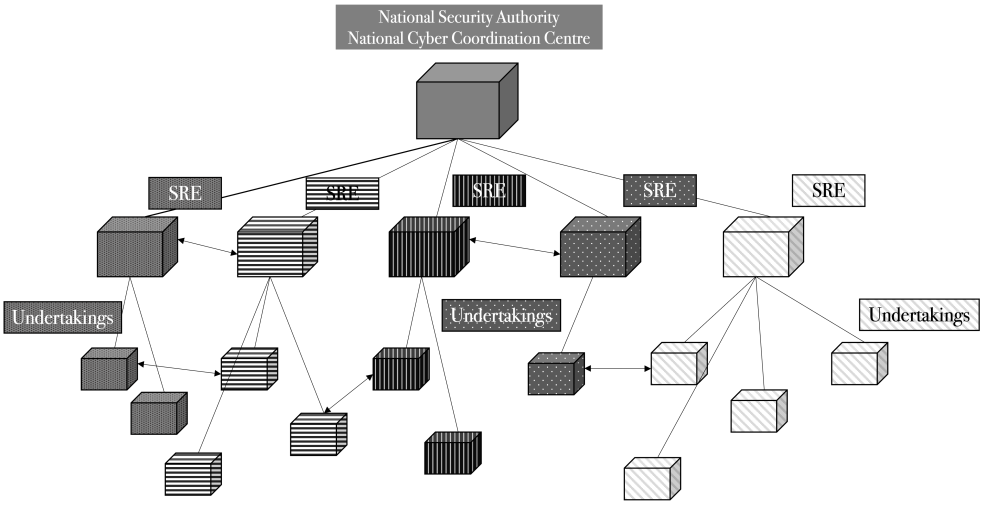
National Security Authority
National Cyber Coordination Centre
SRE
SRE
SRE
SRE
SRE
Undertakings
Undertakings
Undertakings

Figure 3.3: Depiction on the hierarchical structure from NSA/NCSC, through SRE and to each undertaking [3] .

cyber security situational understanding in Norway.

Accordingly, there are partly competing, partly complementing public and private security hubs within the different sectors in Norway [68], resulting in a complex cyber security landscape. Private security hubs are not obligated to report to NCSC, making it even more challenging to maintain a comprehensive situational understanding of the national cyber security landscape in Norway.

The establishment of Norwegian SRE were first discussed in a parliamentary notice in 2012 [69]. The notice states that "as a minimum solution, a contact point must be established in each sector for serious ICT incidents and procedures for internal notifications and toward NorCERT. In addition, the sectors themselves must assess their need to manage ICT crises and how they in turn will scale up their response entities" [69].

More recent governmental strategies outline the ambition for SRE, in which they should be capable to assist their sector with expertise and be a hub for sharing information between inter-sectoral undertakings, between sectors and between the sector and the national level [70]. As with the FNF identification process (previously described in Section 3.2.3 Classification of critical national assets and depicted in Figure 3.2), each ministry is responsible for appointing a SRE and ensure that their sector's SRE at any given time meet the requirements and expectations for this function [3]. The individual ministry may decide if it is appropriate to have one or more SREs in its own sector, or whether to establish cross-sectoral SREs where necessary. Pending SRE appointment, the given ministry is itself responsible to perform all related tasks [3].

3.4.3 Individual undertakings

NSA states that ICT security first and foremost is the responsibility of each individual undertaking. By this, the undertaking is responsible for responding to cyber attacks, regardless of whether the undertaking is part of the public or private sector [3]. The Security Act states general security requirements for both physical and digital assets in undertakings subjected to it. For all undertakings not subjected to the Act, there are no regulations or legislature stating minimal security levels in the digital domain other than secure management of employee and customer personal data.

Methodology

This chapter explains how the research was conducted in order to answer the research questions of the thesis. The chapter includes a description of the research process, research design, what research methods were used in addition to detailing how the data was collected, analyzed and interpreted. Lastly, considerations regarding validity and reliability of the thesis is discussed.

4.1 Research process

This section presents the overall structural research process used in the thesis. An introduction to the sampling criteria, data collection and analysis will be described.

According to Thomas [71, p. 29], a research process starts with identifying a research problem and ends with a publication of the results in a report. A list of important steps in the research process is shown below [71, p. 30]:

1. Identify the research problem
2. Review of literature
3. Develop the objectives
4. Decide the research design
5. Formulate the research protocol
6. Get approval from competent authorities
7. Conduct the research work and collect data
8. Analysis of data
9. Interpretation of data
10. Preparation of the thesis/report
11. Presentation of the results
12. Publication of reports

The researchers divided the research process into four phases which included the steps of the research process proposed by Thomas.

1. Direction and planning (May - June 2022)
2. Collection (June - August 2022)
3. Processing (September - November 2022)
4. Dissemination (December 2022)

The project started in May 2022 and ended in December 2022.

Phase 1: Direction and planning

The first phase was conducted as an independent course prior to the master thesis. This phase included an initial literature review to identify an area of interest, deciding what research design and methods to use and creating a progress plan.

Initially, the researchers decided to explore the concept of "information sharing" in light of national security. Due to the nature of the masters program, the researchers delimited the scope to information sharing in the context of information security or cyber security. During the initial literature review, several relevant studies regarding Cyber Security Information Sharing (CSIS) were identified, and gave inspiration to the research problem and it's sub-problems within this thesis. After defining the objectives, contributions and limitations of the thesis, the researchers created an appropriate research design in order to answer the research problem and achieve the objectives of the research. The chosen research design is covered below in Section 4.2 Research design.

As a part of the research project plan, both a risk and feasibility assessment were conducted, as well as an assessment of legal and ethical considerations regarding the study. A progress plan including milestones, deliverables and required resources was created to ensure structure and progress during the research period [72].

Phase 2: Collection

The data collection period lasted for two months and was conducted between the end of June and the end of August 2022. In this phase a total of 13 in-depth interviews were conducted, as well as an extensive recruitment of respondents to the questionnaire.

Phase 3: Processing

The processing of the collected data was conducted from early October to late November 2022. The processing phase was divided into five sub-processes, explained in detail in Section 4.5.3 Processing:

a) Collation
b) Evaluation
c) Analysis
d) Integration
e) Interpretation

The processing phase included individual processing of the quantitative data and the qualitative data, in addition to integration and interpretation of the two data sets as the final stage of the processing phase.

Phase 4: Dissemination

The fourth phase included production of the written product - *the thesis*, and a presentation to be disseminated to those of interest as several of the interview objects and respondents asked for the key findings of the project during the data collection. If possible, one or several scientific papers will also be produced in order to contribute with our findings to the research within the field, and to cyber security decision-making within Norwegian organizations.

4.2 Research design

A *descriptive mixed methods research design* combining both quantitative and qualitative research methods was used to examine the research problem and it's subproblems of the thesis. This section includes an introduction to descriptive research, mixed methods designs and the reason for choosing the approach to address the research questions of the thesis.

4.2.1 Descriptive research

Descriptive research examines either a situation, a phenomenon or a population *as it is*, and does naturally not include any researcher-imposed treatments or interventions. Nor is descriptive studies intended to determine cause-and-effect relationships [73, p. 154]. In other words, descriptive research can answer questions such as *what*, *where*, *when* and *how*, but not *why* questions. In order to answer the above-mentioned questions, a wide variety of research methods within the category of descriptive studies can be applied to investigate the scope of the research. *Survey research* is one form of descriptive research methods. While some sources defines *survey research* as almost any type of descriptive, quantitative research, Leedy et al. [73, p. 159] defines the term more restricted. Survey research "*involves acquiring information about one or more groups of people — perhaps about their characteristics, opinions, attitudes, or previous experiences - by asking them questions and tabulating their answers*" [73, p. 159]. Typical data collection techniques utilized in survey research are interviews and questionnaires [73, p. 159]. Within survey research, questionnaires are used to understand general characteristics of a specific population, while interviews are used to gain more in-depth understanding of a topic.

Descriptive research is used to measure one or more variables in some way. Measuring *substantial phenomena* - phenomena that have physical substance - can be done by using existing and clearly valid measurements instruments. *Insubstantial phenomena* such as concepts, ideas, opinions, feelings or other intangible entities, are more challenging to measure. There exist some well known measurements within certain subject areas, although no ready-made measurement instruments exist to measure complex variables such as e.g. peoples attitudes toward a specific topic [73, p. 107, 161]. Accordingly, when complex variables are measured in descriptive studies, the measurement instrument must be carefully planned and designed in order to ensure the study's validity.

Non acknowledged measurement instruments exist for measuring peoples attitudes and perceptions toward CSIS. Consequently, the researchers had to design an appropriate measurement instrument to be able to address the research problem. The next subsection includes the chosen research design and why it was chosen.

4.2.2 Mixed methods research design

mixed methods research combines quantitative and qualitative research methods and often provides a more complete picture of a specific phenomenon than either approach could obtain alone [73, p. 100]. Researchers using mixed methods designs are required to comprehend a more advanced skill set as the researcher must be familiar with both qualitative and quantitative research skills. Mixed methods research is also often more time-consuming and resource demanding [73, p. 329].

In addition to mixed methods generally being more challenging, each collection method entail several possible sources of errors. A qualitative approach to data collection and especially data collection through questionnaires is subject to a number of bias and errors which may affect the results. This includes: sampling errors, a flawed or biased questionnaire design, leading or ambiguous wording, sampling bias and errors in the analysis and interpretation of results, and may lead to an artificial sense of accuracy [74][75][76].

Interviews are also prone to errors in the data collection. As data is based on personal interactions, the results are negotiated and contextually based [76][77][78][79]. The interviewer is subject to a number of bias, including leading questions, satisficing from both interviewers and interviewees and the collected data is always contrived and an incomplete understanding of the interviewees point of view [76].

However, a combination of qualitative and quantitative approaches provides certain benefits that neither approach could provide alone. Some of the benefits include the method's ability to address complex research question in a more complete and profound manner when combining qualitative and quantitative data. Another benefit of combining two approaches is if weaknesses occur in one of the methods. Then the opposite approach could compensate for emerging flaws. Sometimes one of the research methods may provide inconsistent or contradictory results, often the quantitative data. In those cases, the opposite approach, the qualitative, may contribute to reveal underlying nuances and meanings of the data collected by the quantitative approach [73, p. 330].

As shown, there are certain drawbacks as well as several benefits with mixed methods research. The reason for choosing either a qualitative, a quantitative or a mixed methods research design should, however, depend on the research question and it's sub-questions that shall be addressed, the researcher's skills [73, p. 330], as well as available time and resources.

mixed methods can be conducted in numerous different designs. Creswell [80, p. 42][73, p. 331] proposes five different designs such as *convergent designs*, *embedded designs*, *exploratory designs*, *explanatory designs* and *multiphase iterative designs*. Within this thesis, *embedded design* were chosen as the research design.

4.2.3 Descriptive mixed methods research design

The initial literature review disclosed that the majority of the identified empirical studies examining people's attitudes toward CSIS only used one research method, most often a quantitative. Despite this, one of the empirical studies [30] had used questionnaires as the primary data collection method and utilized supplementary interviews to get deeper insight and other perspectives of the problem investigated. An additional empirical study [24] used both exploratory survey, focus group discussions and interviews to examine the research problem. The exploratory survey was conducted as a pre-study to reduce the possibilities of omitting important concepts and artifacts, while the focus group discussions and interviews were used to gain deeper insights in the stakeholders' perceptions about the research problem [24, p. 1412].

Since the thesis aimed to examine a larger group's attitudes and opinions about a specific topic, a quantitative approach was chosen as the primary data collection method while the qualitative approach was applied as a supplementary one to gain a deeper insight and enable a more nuanced understanding on the research problem. The researchers also decided to use the same combination as other previous empirical studies, including a questionnaire as the quantitative data collection and in-depth interviews as the qualitative data collection.

Due to the lack of empirical studies regarding attitudes toward CSIS within the Norwegian cyber security community, the researchers assessed that some weaknesses potentially would appear in the questionnaire. In addition to complementing and enhancing the depth of the statistical analysis, in-depth interviews also functioned as a mitigating measure for potential flaws in the collected and analyzed statistical data.

As mentioned above, a combination of quantitative and qualitative is also beneficial because quantitative data collection may provide inconsistent or contradictory results that requires qualitative data to either explain or reveal underlying nuances or meanings [73, p. 330].

The qualitative and quantitative approaches were conducted in parallel as two independent data collection methods. However, since the qualitative data collection aimed to explain and enrich the quantitative data, the measurement instruments were synchronized and tuned to answer the same research questions.

Despite that mixed methods research designs are known to be used by more experienced researchers, requires a broader skill set of the researcher and often span over a larger time period, the researchers decided to use mix-methods research design as both individuals have several years of work experience within structured data collection, analysis and production of reports.

Details related to the quantitative research method will be outlined in Section 4.4 Quantitative research method - Questionnaire and in Section 4.5 Qualitative research method - In-depth interviews for the qualitative research method.

4.3 Multivocal literature review

In mixed methods research designs, most of the literature review should be conducted at the very beginning of the project. A profound literature review may serve as an inspiration and help the researcher to identify appropriate research questions and/or hypotheses, different research designs and potential measurement instruments [73, p. 335]. As previously mentioned, the literature review helped the researchers to chose a suitable research design and measurement instruments.

A *Multivocal Literature Review* was used to get a deeper insight in the scope of the thesis and to find relevant literature and previous research related to the topic of the thesis. Both theoretical and empirical studies were taken into account.

Multivocal Literature Reviews is a type of a *Systematic Literature Review* which includes grey literature (e.g. white papers, blog posts, technical reports, preprints, etc) in addition to white literature such as published journals papers, conference proceedings and books [81]. Due to the speed of the technological and cultural progress within cyber security, the researchers assessed it as necessary to include more current knowledge provided by grey literature. The validity of the included grey literature was rigorously assessed and compared to other published and peer-reviewed literature in addition to the assessed expertise of the researchers [72].

4.3.1 Search process

To find relevant literature, a systematic search process was conducted. Among the different digital databases and libraries accessible for NTNU students, the following academic search engines were used: IEEE DL, ACM DL, Elsevier and JSTOR. Additional secondary search engines were Research Gate and Google. Research Gate were not used as a primary search engine as access to papers in this database often required interactions with the authors, resulting in a time-consuming process, often with negative results [72]. Systematic searching in the mentioned databases were used to find white literature relevant to the thesis.

Defining relevant search strings is an iterative process, where the initial exploratory searches reveal more relevant search strings [81]. The search process started with one defined search string: "cyber security information sharing" (SQ1). This search string provided few, but highly relevant results, such as e.g. the research of Zibak & Simpson [13]. This paper provided a new search string (SQ2) relevant for the scope of this thesis. Four additional, more wide search strings were used in the literature review (SQ3-6) due to the narrowness of SQ1 and SQ2.

In addition to academic search engines, supplementary literature was identified in either related work or the bibliography/references of the identified relevant literature provided by the search strings [72]. This search method is called *snowballing*. Snowballing is a search technique "where one follows citations either backward or forward from a set of seed papers" [81] to find other sources of information relevant to a topic. This search method contributed to identifying both white and grey literature relevant to the scope of the thesis. Both of the studies conducted by Zibak & Simpson [13][37] were good sources for additional relevant literature.

The different search strings used in the search process are listed below [72]:

SQ1: “cyber security information sharing”
SQ2: (“cyber security” OR “threat”) AND (“intelligence” OR “information” OR “data”) AND (“sharing” OR “exchange”)
SQ3: (“norway”) AND (“cert” OR “isac” OR “csirt”)
SQ4: ((“state” OR “national”) AND “security”) AND (“information” AND (“exchange” OR “sharing”))
SQ5: (“information sharing”) AND (“empirical”)
SQ6: ("information" AND ("sharing" OR "exchange")) AND ("security" OR "threat") AND ("empirical")

4.3.2 Results of the search process

To delimit the results of the search strings, the time-span was set to 2010-2022 due to the rapid development of the cyber domain in the last years, as well as the development of acknowledged cyber security standards and guidelines. The results were further sorted by relevance. Only the top 50 results were examined. The result of the different search strings is shown in Section 2.1.1 Benefits and challenges with CSIS and CTI. The table includes information about [72]:

a) search query number (SQ#),
b) academic search engine,
c) number of results and number of relevant literature identified,
d) reference to the relevant literature mapped to RQ#,
e) whether the search query gave theoretical or empirical results, and
f) the date of the search.

Search query	Database	# results / # relevance	Source mapped to RQ#	Theoretical / empirical	Date of search
SQ1	JSTOR	19 / 2	[34] : RQ2 [82]: RQ2	Theoretical Theoretical	25.05.22
	IEEE	1080 / 5	[37] : RQ3 [83]* : N/A [84]: RQ2/RQ3 [85]: RQ2 [19] : RQ2	Empirical N/A Empirical Theoretical Theoretical	25.05.22
	Elsevier	25 / 2	[86] : RQ2 [29] : RQ2	Theoretical Theoretical	25.05.22
	ACM DL	8 / 2	[13] : RQ2 [87] : RQ2	Empirical Theoretical	25.05.22
SQ2	JSTOR	49473 / 2	[88]: RQ2	Both	25.05.22
	IEEE	3697 / 4	[83]* : N/A [84] : RQ2, RQ3 [85] : RQ2 [19] : RQ2	N/A Empirical Theoretical Theoretical	25.05.22
	Elsevier	188213 / 1	[29] : RQ2	Theoretical	25.05.22
	ACM DL	9646 / 1	[87] : RQ2	Theoretical	25.05.22
SQ3	JSTOR	2526 / 0	[83]* : N/A	N/A	25.05.22
	IEEE	4 / 1	[42] : RQ1	Empirical	25.05.22
	Elsevier	453 / 1	[86] : RQ2	Theoretical	25.05.22
	ACM DL	27 / 0	N/A	N/A	25.05.22
SQ4	JSTOR	54275 / 2	[88] : RQ2 [38] : RQ2, RQ3	Both Both	25.05.22
	IEEE	4284 / 1	[83]* : N/A	N/A	25.05.22
	Elsevier	176531 / 2	[86] : RQ2 [89] : RQ2	Theoretical Theoretical	25.05.22

Table 4.1 continued from previous page

Search query	Database	# results / # relevance	Source mapped to RQ#	Theoretical / empirical	Date of search
	ACM DL	22659 / 5	[87] : RQ2 [90] : RQ3 [13] : RQ2 [91]* : N/A [92]* : N/A	Both Theoretical Empirical N/A Both	25.05.22
SQ5	JSTOR	2768 / 1	[88] : RQ2	Both	25.05.22
	IEEE	778 / 1	[84] : RQ2, RQ3	Empirical	25.05.22
	Elsevier	13643 / 0	N/A	N/A	25.05.22
	ACM DL	1536 / 3	[13] : RQ2 [92]* : N/A [24] : RQ2	Empirical Both Empirical	25.05.22
SQ6	JSTOR	25848 / 1	[88] : RQ2	Both	25.05.22
	IEEE	95 / 2	[84] : RQ2, RQ3 [42] : RQ1	Empirical Empirical	25.05.22
	Elsevier	113615 / 1	[89] : RQ2	Theoretial	25.05.22
	ACM DL	6875 / 3	[84]: RQ2 [24] : RQ2 [92]* : N/A	Empirical Empirical Both	25.05.22

Table 4.1: Results of search in digital databases and libraries (SQ1-6). References marked with (*) were not able to access.

Some of the literature (marked with a (*) in Table 4.1) either provided by the search strings or the snowball technique were not directly accessible due to the requirement of direct contact with the author of the paper. A few identified, likely relevant studies were not accessed as the researchers were not able to come in contact with the authors. Another emergent hinder to utilize relevant literature was that some of the papers were written in a foreign language outside the researchers' knowledge [72].

The result of the literature review is outlined in Chapter 2 Related research and is structured into separate sections such as theoretical and empirical research on CSIS. Due to the scope of the thesis and its research questions, the exploration of empirical research related to CSIS was more thorough than the theoretical one. Finally, the relevance of the identified literature was assessed in relation the different research questions [72].

4.4 Quantitative research method - Questionnaire

Quantitative research is aimed at among others test theory or confirm and validate existing theories or practices across a representative, large sample. The method is often focused, pre-planned and seeks to examine known variables. Contrary to qualitative research methods, quantitative data analysis is statistical and aims to be objective [73, p. 99]. Quantitative data "are often collected from a large sample that is presumed to represent a particular population so that generalizations can be made about the population" [73, p. 99].

The quantitative method is described by dividing the research process into four parts, mirroring the sectionalization of the research process as a whole: *1) Direction and planning*, *2) Collection*, *3) Processing* and *4) Dissemination*.

4.4.1 Direction and planning

In this subsection, all factors related to planning and preparing the quantitative data collection are described, including the selection of quantitative method, and planning the questionnaire.

Questionnaire

A questionnaire is neither an official form, nor a set of random questions. Questionnaires should be designed carefully in order to measure a specific issue under investigation and provide useful data [75, p. 100][73, p. 160]. The structure and design of a questionnaire depends on e.g. the aim of the research, characteristics of and access to the targeted population, the promise of anonymity, etc. [75, p. 100-101].

Even though questionnaires can serve different goals and appear in different fashions, Oppenheim proposes five common matters that should be addressed in order to create an useful questionnaire [75, p. 101]:

1. The main type of data collection instrument (in this case, a questionnaire),
2. the method of approach to respondents,
3. the build-up of question sequences,
4. the order of questions, and
5. the type of question to be used.

Each of these matters will be described in the following subsections: 2) is covered in *Collection* and 3-5 is covered in *Questionnaire design*.

The researchers decided to use a web-based self-administered questionnaire to provide a comprehensive understanding of a significant number of different cyber security personnel's perceptions and attitudes toward CSIS within the Norwegian cyber security community (RQ2 and RQ3), as well as examining how CSIS is practically permormed in Norway (RQ1).

Postal questionnaires are written questionnaires distributed to respondents via either mail or e-mail, and returned back filled out to the researcher [75, p. 102][73, p. 160]. Postal questionnaires are the precursor of web-based questionnaires, in which web-based questionnaires utilize more modern and digitized methods such as digital format, and distribution via e-mail or other social media platforms.

Pros and cons considering the fashion of the questionnaire were weighted during the design phase. Some of the main arguments for choosing a web-based self-administered questionnaire was due to common benefits related to: a) broad and effective distribution unconstrained by geographical location, b) cost-effective data processing and analysis afterwards, and c) safeguarding the respondents anonymity [73, p. 160, 175][75, p. 102-103]. The protection of the respondents anonymity was highly important as several of the targeted respondents worked in national security and intelligence services.

Additional important benefits of self-administered questionnaires are that it facilitates for more honest answers by respondents than e.g. personal interviews and the avoidance of interview bias [73, p. 160][75, p. 102].

However, a common drawback with web-based questionnaires distributed by either e-mail or other social media is low *return rate*, meaning that the majority of people who receive questionnaires do not return them. Additionally, web-based self-administered questionnaires do not provide an opportunity to correct misunderstandings or to offer explanations or help when it is conducted by the respondents [73, p. 160][75, p. 102].

Questionnaire design

Relevant questionnaires identified in the literature study were used as a baseline and inspiration for the qualitative data collection. When designing the questionnaire, Table 4.6 comprising a profound list of possible sources of bias or errors related to survey design was used to increase the quality of the measurement tool.

Previous studies examining either information sharing or CSIS [13][37][93][39][94][40] have used questionnaires as a quantitative data collection method. The questionnaire in this thesis was primarily based on the questionnaires in the research of Zibak & Simpson [13][37], which examined CSIS or CTI in the UK cyber security community.

Minor adjustments, improvements and additions were applied to the questionnaire to address the research questions given in Section 1.3 Research questions. The questionnaires in [94] and [93] were used as an inspiration for designing and adjusting the questionnaire of [13] and [37].

As mentioned above, the quantitative data collection method was performed as an web-based self-administered questionnaire. The questionnaire included five parts:

1. Classifying questions about the respondent,
2. A mix between close-ended and multiple-choice questions regarding CSIS in Norway (RQ1),
3. Likert scale measuring perceived benefits and challenges regarding CSIS at different levels: operational, organizational, economic and policy (RQ2),
4. A mix between closed-ended multiple choice questions and semantic differential scale measuring the attitudes (usefulness and willingness) toward information sharing efforts (RQ3) and,
5. Two open-ended questions giving the respondents the possibility of giving feedback and comment it's answers.

The complete questionnaire is presented in Appendix A.3 Questionnaire.

Every question of the questionnaire was mandatory except for the questions in part 5, which avoided the respondent to deliver without answering the whole questionnaire.

Part 1 included several close-ended classification questions about:

a) the participant's sector (public/private and its organization's primary activity),
b) whether it works in a cyber security organization,
c) size of organization given in number of employees,
d) work experience and,
e) organizational role.

The purpose of part 1 was to collect classifying information about the respondents in order to make group comparisons. Accordingly, part 1 was not aimed at answering any of the RQs. Questions given in part 1 were based on questions in the research of Zibak & Simpson [13][37], with some additional questions from [93], as well as self-composed questions. Since close-ended questions are easy and quick to answer, as well as easily quantifiable and facilitate for group comparisons [75, p. 114-115], part 1 included only close-ended single select multiple choice questions with either "yes/no" answers or a list of few answer options.

One of the questions measured whether the respondent fulfilled the sampling criteria of the questionnaire or not. If the respondent had less than one year of working experience in cyber security, its answers were discarded and not included in the analysis and results.

Part 2 included six close-ended questions regarding the respondent's organization's engagement in CSIS and therefore partially answered RQ1. The questionnaire in [93] was used as a baseline for designing the questions in part 2.

Similarly to part 1, part 2 included only close-ended questions to make it possible to compare one group of respondents with another. The majority of the questions were single select multiple-choice questions enabling both comparison and easier statistical data analysis afterwards. However, a familiar disadvantage with close-ended questions aiming to measure less classifying concepts, is the loss of expressiveness. This might lead to bias as the respondent is forced to choose between an incomplete list of choices making the respondent focus on alternatives that might not had occurred to them naturally [75, p. 114]. Oppenheim suggests that all closed-ended questions initially should be open-ended questions included in a pilot questionnaire in order to derive pertinent answer options that actually reflect the variety of answers from the population under investigation [75, p. 129]. However, as described in Section 4.6 Considerations on validity, reliability and research ethics, this possible source of error was not sufficiently taken into account when the questionnaire was designed and tested due to time restrictions.

Furthermore, open-ended questions were neither included in part 2 nor generally in the questionnaire, except from part 5, due to time restriction preventing the researchers from conducting a more profound pilot questionnaire. Open-ended questions were not included in order to avoid collecting information not relevant to the inquiry and the possibility of limiting statistical analysis of the data collected.

See Section 4.6 Considerations on validity, reliability and research ethics for several identified sources of errors related to the questionnaire.

Part 3 This part of the questionnaire aimed at answering RQ2 and included a total of 26 statements about benefits and challenges regarding CSIS within the four categories included in the RQ2: operational (RQ2-1), organizational (RQ2-2), economic (RQ2-3) and policy (RQ2-4). The statements were based on Table 2.1, originally derived from a profound analysis of existing grey and academic literature conducted by Zibak & Simpson [13] about benefits and challenges regarding CSIS. The distribution of benefits and challenges was 50/50, as proposed by [95, p. 70]. Some minor adjustments mainly related to the phrasing of the statements, as well as removing or adding a few statements were conducted to both adjust it to the Norwegian context and make it easier for Norwegians to understand the statements (phrasing).

The statements in part 3 measured cyber security personnel's attitudes by using seven-point Likert scale ranging from 1 = "strongly disagree" to 7 = "strongly agree". Accordingly, high scores indicated agreement with the statement. Likert scale was used due to two main reasons: a) an appropriate instrument for measuring specific statements and b) the possibility to compare the results with the findings in [13]. Since the benefits and challenges with CSIS were formulated as statements, not concepts, Likert scale were the most appropriate *attitude scale* compared to both *semantic differential scales*, *rating scales*, *Thurstone scales* and *Guttman scales* [96, p. 156-157]. Each statement represented a Likert item and was assigned to one of the given categories in Table 2.1: *operational*, *organizational*, *economic* and *policy*.

Part 4 included a mix of both close-ended questions and five-point semantic differential scale to measure cyber security personnel's attitudes toward CSIS. This part aimed at answer RQ1 and RQ3:

a) organization's engagement in CSIS (RQ1),
b) perceived usefulness of CSIS efforts (RQ3-1), and
c) perceived willingness to engage in CSIS efforts (RQ3-2).

The questions within this part were mainly based on the research of Zibak & Simpson [37], with a few additional questions derived from [93]. Part 4 was the most complex part of the questionnaire since it included a variety of question types and aimed at measuring both the respondent's attitudes and more objective information about the organization the respondent represented.

Within this part, the respondents were presented four different categories of CSIS, also known as efforts, based on the categories defined by [38][37] as outlined in Section 3.3.3 Information sharing categories. The categories were described in the questionnaire to prevent misunderstandings related to the terms.

Engagement in CSIS efforts were questioned using close-ended single select multiple choice questions. Compared to Zibak & Simpson [37], which used semantic differential containing more diffuse answer options, the questionnaire in this thesis provided more specific answer options such as *daily, weekly, monthly, quarterly, semi-annually* and *yearly* to measure the frequency of engagement.

The respondent's perceived usefulness of information sharing efforts and the respondent's willingness to engage in different information sharing efforts were measured by using both attitude scales and close-ended questions.

A *semantic differential scale* is an instrument used to measure an individual's attitude about a specific concept by selecting a position on a continuum that ranges from one bipolar adjective to another [96, p. 631]. The scale is defined by choosing two opposite descriptors at the extremes, such as e.g. "useful" and "useless" [75, p. 239]. Semantic differential scales, compared to Likert scales, are more suitable when measuring attitudes toward a specific domain e.g. CSIS, while Likert scales are more suitable when measuring the degree of agreement when a more detailed statement is provided, such as a benefit with information sharing. Accordingly, semantic differential scale was more suitable then Likert scale to measure the variables in part 4.

Even though research has shown that semantic differential scales are most optimal when using seven-point scales, five-point scales were used in part 4 [75, p. 237]. The main reason for using five-point scales was due to the possibility to compare the attitudes within the Norwegian cyber security community with the British one as presented in [37].

The semantic differential scale aimed to assess respondents' attitudes toward the *domain* CSIS, represented by four categories: *data sharing*, *alerts & triggers for action*, *knowledge sharing* and *expertise sharing*, on a five-point scale ranging from "not useful" to "very useful", and "least willing" to "most willing".

Part 5 included two open-ended questions which gave the respondents the possibility to give feedback or comment any of their answers. The questions within this part was the only two optional given in the questionnaire. The purpose of this part was to identify possible flaws within the questionnaire, suggested improvements, as well as relevant information supporting the statistical analysis.

Pilot test

A pilot version of the questionnaire was tested on five acquaintances of the researchers to identify weaknesses or flaws in the questionnaire design. The acquaintances gave feedback on specific possible sources of bias of errors stated in Table 4.6. This included among others wording and phrasing of the questions, identifying leading questions, measuring response fatigue and questionnaire length, and if sufficient answer options on the close-ended single select multiple choice question were provided.

4.4.2 Collection

This section describes the distribution strategy including the sampling criteria, aimed sample size and the distribution method of the questionnaire.

The data collection took place during June-August 2022.

Sample and population

A *sample* is defined as a group of individuals, items, or events that represents the characteristics of the larger group, a *population*, from which the sample is drawn. Sampling is known as the process of selecting a sample and begins with describing the population of interest with several structures and characteristics. The entire population of interest, called the *target population* is rarely available, forcing the researcher to select subjects from what is called the *accessible population*, also known as *available population* [96, p. 129-130]. According to Leedy et al., "*the sample should be so carefully chosen that, through it, the researcher is able to see characteristics of the total population in the same proportions and relationships that they would be seen if the researcher were, in fact, to examine the total population*" [73, p. 177].

To obtain an adequate representative sample of the target population Gay et al. proposes certain procedures to be followed [96, p. 129]:

a) defining a population with structures and characteristics,
b) selecting a suitable sampling method to select a sample,
c) determining a representative sample size, and
d) avoiding sampling error and bias.

As the thesis aimed to examine attitudes toward CSIS within the Norwegian cyber security community, "personnel working with cyber security in Norway" was the main delimiter of the target population. A secondary delimiter was working experience. Only personnel with at least one year of working experience in cyber security were of interest in order to increase the *external validity* of the study. Accordingly, the target population of the study was "personnel working with cyber security in Norway with more than one year of working experience in cyber security".

In order to be able to make generalizations about the population, the sample must be representative. However, representative samples of populations with unknown characteristics are challenging to estimate. Oppenheim suggests that if the target population has unknown characteristics or lacks accurate parameters, a *judgment sample* can be drawn by the researcher [75, p. 42-43]. Judgment sample is a sample drawn by using a judgmental sampling technique, also known as *purposive sampling* which is further elaborated in the next step of the procedure. There is, however, a risk that the judgment sample will represent only a particular sub-group of the target population and that the sub-group only will be roughly represented [75, p. 43].

Accordingly, additional sampling criteria reflecting the goal of the study were considered to increase the chances of obtaining a representative sample of the target population. The sampling criteria is summarized below, including the three additional criteria:

Sector	% of population	% of respondents
Private	67	61
Public	33	39

Table 4.2: Distribution of employees and respondents within the private and public sector

1. Personnel working with cyber security in Norway,
2. at least one year of working experience in cyber security,
3. cyber security personnel from both public and private sector,
4. cyber security personnel from different industries, and
5. cyber security personnel at several hierarchical levels.

The third criteria considered an approximate representative *distribution of cyber security personnel from both the private and public sector*. In this criteria public sector is understood as employees within the local and central government, while the private sector is understood as employees working in a private organization, public owned enterprises (e.g. Telenor, Equinor, etc.), or unspecified organizations. In the second quarter of 2022, the distribution of employees within the public and private sector was approximately 33% and 67% respectively, according to Statistics Norway [97]. Accordingly, the sample aimed to reflect the given distribution. Question 1.1 in part 1 of the questionnaire measured the distribution between the private and public sector among the respondents. As shown in table 4.2, the distribution of the respondents in the questionnaire was approximately the same as the distribution in the population.

The fourth criteria considered the *distribution of cyber security personnel in different industries*. This criterion was chosen to reflect attitudes of cyber security personnel across different sectors due to the fact that also the Fundamental National Functions (FNF) span across the different sectors.

Information about the distribution of cyber security personnel per industry in Norway was however challenging to acquire as no statistical information exists and the uncertainty related to whether organizations have own cyber security employees or are dependent on Cyber Security As A Service (CSaaS) were cyber security management is outsourced to a specialized provider of information security services who handle a specific part of your business operations [98].

However, to obtain information about the distribution between different industries, the statistical standard *Standard Industrial Classification 2007 (SIC 2007)*, used by *Statistics Norway* in economic statistics, was used in the questionnaire to classify the primary activity of the respondents organization [99]. The reason for including this in the questionnaire was to map the distribution of industries within the sample and within each sector, as well as to identify the convergence or diver-

Industry	% of employees
Agriculture, forestry and fishing	2.3
Mining and quarring	2.1
Manufacturing	7.6
Electricity, gas, steam and air conditioning supply	0.6
Water supply; sewage, waste management and remediation	0.6
Construction	8.6
Wholesale and retail trade	12.7
Transportation and storage	4.7
Accommodation and food services	3.4
Information and communication	3.9
Finance and insurance	1.7
Real estate	1.0
Professional (consultatory), scientific and technical activities	5.6
Administrative and support services	4.9
Defense and public administration; compulsory social security	6.3
Education	8.3
Human health and social work	20.8
Arts, entertainment and recreation	2.1
Other service activities	2.7

Table 4.3: Distribution of employees per industry in 2021, Norway [99]

gence between cyber security personnel's attitudes within a specific industry and between several industries. An ultimate reason for including industry as a parameter was due to the replication of the questionnaire in [13][37] which examined attitudes within the British cyber security community, and the possibility to compare results within Norway and the UK. However, due to a small sample within each industrial category, these correlations were assessed as not generalizable to the individual industries as a hole. Thus, correlation against industries was not further examined.

The researchers were, however, aware of the possible sources of error considering this parameter for the reason that a correct statistical estimate of this parameter does not exist, and uncertainties considering the respondents familiarity with the standard SIC 2007.

The fifth criteria considered the *distribution of cyber security personnel working at different hierarchical levels within an organization*. Three different hierarchical levels were included: top management, middle management and practitioners. Top management represented Chief Security Officer (CSO), Chief Information Security Officer (CSIO), Chief Information Officer (CIO), or similar positions at the same hierarchical level. Middle management represented e.g. security managers, while practitioners represented security analysts, incident responders, etc.

This parameter was included in the sampling criteria to ensure that both managers and practitioners within the Norwegian cyber security community were represented in the sample, and to examine the attitudes within a specific hierarchical level and between the different levels.

The researchers were not able to find exact statistical data related to the distribution of the hierarchical levels. Only one source of information was identified, however it was not sufficient for estimating the amount of Norwegian employees within each defined hierarchical level. *12542: Employed persons. 4th quarter, by occupation, contents and year* [100] from Statistics Norway provided only information related to the amount of ICT services managers in Norway, which does not differentiate between top managers and middle managers, and include other managers not specifically working with cyber security. The same challenge holds true for cyber security practitioners as well, as no exclusive occupation category exists for this personnel. Accordingly, an estimate could not be found.

Naturally, there will be several practitioners than managers, and several managers than top managers due to the nature of hierarchy. However, the criterion of minimum one year of working experience in cyber security might reduces the amount of practitioners within the population, resulting in uncertainties regarding the distribution of each hierarchical level category.

As demonstrated, information about the exact amount of personnel within each hierarchical level of the population does not exist. Despite this, a question regarding the role of the respondent was included in part 1 to both increase the external validity and make it possible to identify differences or similarities across the different hierarchical levels of cyber security personnel. This variable was however, analyzed with caution due to a possible inaccuracy caused by two factors: hierarchy variances in different sectors and industries, and subjective perceptions related to the hierarchical levels.

Sampling method

Master students, similar to doctoral students, often have limited resources and time due to completion deadlines to obtain their degree. Accordingly, the research design and sampling techniques should aim to optimize data collection and reduce the overall survey error within the available time and resources [101]. Researchers are thus often encouraged to find the most suitable sampling method in respect to the research problem and available time and resources. This "requires compromises between theoretical sampling requirements and practical limitations (...)" [75, p. 43].

Even though random sampling provides the best chance to acquire an unbiased sample in quantitative research, random sampling techniques are not always adequate when the target population is either hard to reach, or when it is not feasible due to practical constraints [96, p. 140]. In such cases, non-random sampling techniques might be more suitable.

Non-probability sampling is often used when the population is either difficult or almost impossible to describe or reach. Non-probability sampling, also called non-random sampling, is the process of selecting a sample that does not guarantees that each member or variation of the population will be represented in the sample [96, p. 140]. Accordingly, some individuals of the population will have little or no chance of being sampled [73, p. 182]. Since the population is either difficult or almost impossible to describe, it might also be challenging to know whom the results can be generalized [96, p. 140]. As demonstrated in the section above, the target population in this thesis was difficult to describe and estimate due to the lack of known characteristics and accurate parameters of the population. To address this challenge, a judgment sample was described in the previous section and needs to be drawn from the target population by *purposive sampling* which is a non-probability sampling technique.

Purposive sampling is the process of selecting a sample that is believed to be representative of a given population, allowing the researcher to select the sample based on own experience and knowledge of the target population. This sampling technique is based on identifying and describing specific criteria for selecting the sample [96, p. 141]. The five criteria listed in the previous section were used as the sample criteria and parameters for recruiting respondents to the questionnaire. Since purposive sampling allows the researcher to define specific criteria for the selected sample, findings of the study can be generalized to the population that contains the specific criteria.

The main weakness of purposive sampling, however, is the potential for inaccuracy in the defined criteria and the resulting sample selection [96, p. 141]. As demonstrated, the parameters considering both the distribution of cyber security personnel per industry and hierarchical level were prone to subjective interpretations or misinterpretations by the respondents, possibly causing inaccuracy in the collected data. Despite this, as the thesis aim to examine attitudes toward CSIS among Norwegian cyber security personnel with more than one year of working experience in cyber security, the above-mentioned characteristics are not decisive for the study, but included to increase the external validity of the research.

Non-probabilistic purposive sampling were used as the sampling technique within the qualitative data collection due to several factors: 1) to access cyber security personnel in general, 2) to include respondents from the so-called secret services (NSA, NPSS and NIS), 3) to ensure a dispersion in both industries and positions of the respondents, and 4) time and resource constraints.

Cyber security personnel, especially those working within the so-called secret services, are in general harder to reach than an average individual due to their focus on personal security and security policies provided by their organizations. Such personnel are therefore normally reluctant to use social media or to expose personal information on social media platforms. Cyber security personnel within the secret services were assessed to be a so called "hard-to-reach" population which are firstly, as the name indicates, hard to reach and secondly generally not open to researchers who do not have social entrées into the population. Surveys, e.g. a questionnaire, received from a unknown researcher on sensitive topics will not be welcomed if no relationship, particularly a trusting one, exists in advance [101]. Consequently, in order to represent the attitudes of this personnel category, *snowball sampling* were used.

Historically, snowball sampling was applied in qualitative research to recruit interview subjects outside the researcher's network. Snowball sampling is when a qualified participant either shares an invitation with other qualified subjects or gives a referral of subjects who fulfill the criteria defined for the target population [101]. This technique was particularly useful to both establish direct contact with possible participants or sharing the questionnaire within the secret service networks.

Sample size

The size of a sufficient and representative sample depends on the size of the population under investigation, as well as e.g. how homogeneous or heterogeneous the target population is [73, p. 184].

Neither "cyber security practitioners" nor "cyber security managers" exist as occupation categories within the employment statistics provided by Statistics Norway [99]. Even though several other occupation categories related to ICT exist, these categories do not provide a sufficiently accurate estimate of the population size. Additional possible sources of error related to the size of the population includes the possibility of cyber security personnel being employed in "wrong" positions/occupations, cyber security personnel being employed in unspecific positions/occupations and that the number of cyber security personnel working within the defense or justice department are not known. Consequently, it was impossible to estimate the size of the target population.

On the other side, Oppenheim suggests that a representative sample does not solely depend on the size of the sample, where he argues that the accuracy of the sample is more important than its size [75, p. 43]. He further proposes that a representative sample and its size can be determined by several theoretical factors [75, p. 44]:

a) the sampling error,
b) the cluster size,
c) the required accuracy of population estimates,
d) the precision of the sampling operation,
e) the number of subgroup comparisons the researcher aims to make,
f) the nature of the variable under investigation, and
g) constraints of time and resources.

The theoretical factors listed above consider both probability sampling and non-probability sampling, whereas some of the factors are less, or in some cases not valid for non-probability sampling. The last three factors are applicable in non-random sampling [75, p. 42-43], and were therefore considered when the appropriate sample size was estimated.

As demonstrated above, the size of the population was not possible to estimate. Accordingly, other factors were considered when the sample size was estimated. A benefit with mixed methods research design, as described in Section 4.2.2 Mixed methods research design, is that the qualitative approach may compensate for weaknesses in the quantitative approach. For that reason the qualitative data collected through in-depth interviews were assessed to compensate for a smaller sample size and thus increasing the overall representativity of the sample in the quantitative data collected.

To facilitate statistical analysis of the different subgroups such as public-private, industry and hierarchical level distribution, this were taken into account when deciding the minimum sample size.

Additionally, as the chosen sampling method was assessed to be resource-demanding due to a significant amount of person-to-person recruitment via digital communication platforms, and that the data collection period was limited to only two months, as well as during the summer vacation in Norway, the time and resource constraints were significant.

Factors such as unknown population size, benefits related to mixed-method research design, the number of subgroup comparisons, as well as time and resource constraints resulted in an assessed achievable and sufficient sample size of 100 respondents.

Response rate

In order to achieve the desired sample size for the questionnaire, common response rates for questionnaires, as well at response rate bias were taken into account.

Higher response rates provide larger data samples and lead to a higher probability of samples being representative of the target population [102]. Consequently, lower response rates lead to a heightened probability of statistical biases, and challenges valid and trustworthy conclusions to be drawn from the sampled data [102][96, p. 9]. A 100% response rate is however rarely achieved, unless the questionnaire is coercively administered to the target population [102].

Response rates in academic surveys have been decreasing for several decades [101]. According to Johnson & Owens, the decline in response rates is related to among others privacy issues, exploitation of personal information, confidentiality issues, and general cynicism [103]. Additional reasons for people not responding to surveys have been reported to be: too busy, not relevant, unavailable mail address to return the questionnaire and that organizational policies prohibit participation [102]. Also, survey saturation caused by the increasing popularity of opinion polls, as well as the interest in data-driven decision making based on surveys may be others reasons for decreasing response rates [102].

According to Rogelberg & Stanton, the average response rate for "studies conducted at the organizational level seeking responses from organizational representatives or top executives are likely to experience lower response rates" [101] than studies conducted at the individual level. The average response rate at the organizational level is approximately 35–40%, while 50% at the individual level [104]. Gay et al. [96, p. 193] and Leedy et al.[73, p. 172] also address that the typical response rate of questionnaires is approximately 50%. A response rate above 50% will increase the probability of the sample being generalizable to the population from which it was drawn [96, p. 193].

Since the questionnaire focused on individual perceptions, and mainly included personal questions with only a few non-controversial questions on behalf of the respondent's organization, the response rate was assumed to be approximately 50%. As the sample size of the questionnaire was estimated to be 100 respondents, and the average response rate for questionnaire is 50%, approximately 200 invitations were distributed to possible respondents via either email or LinkedIn messages. Additional details related to the distribution method is described in the next section.

To increase the validity of the study, a significant number of measures to maximize the response rate were considered and complied. How to maximize the response rate is however widely discussed among researchers and contradictory meanings exist within the literature [102]. A great variety of different measures to maximize the response rate are listed below:

- design the survey carefully: types of questions, length, structure, etc. [104],
- guarantee of anonymity [105][96, p. 192],

- provide sufficient and adequate response opportunities [104],
- provide a specific deadline date [96, p. 191],
- pre-paid or promised incentives [106],
- monetary and non-monetary rewards [106][105],
- make a good first impression [73, p. 172],
- personalization [106],
- motivate potential respondents [73, p. 172],
- establish survey importance [104],
- foster survey commitment [104],
- pre-notify participants [104],
- offer the results of your study [73, p. 172],
- consider the timing for distribution [73, p. 172],
- distribute questionnaires through a person of authority [96, p. 192],
- publicize the survey [104],
- monitor survey response [104],
- provide survey feedback [104], and
- reminders and follow-up activities [96, p. 192][73, p. 172].

Despite all efforts made to maximize the probability of responses, some individuals will still not respond to the questionnaire due to the fact that people that does not know each other will have little or nothing to gain by answering an unknown person [73, p. 170]. In such cases, the questionnaire can be distributed to a person of authority, rather than directly to a potential respondent. If persons of authority are invested in the research and encourage its colleagues to complete the questionnaire, this strategy could contribute to a increased response rate. However, this is only beneficial if the person of authority do not influence the respondent's response [96, p. 192], which is challenging to detect. In addition to distribute the questionnaire via either recognized persons within the target population of persons of authority, follow-up activities may motivate some of the initially reluctant persons to reconsider their though about not attending, making them to respond to the questionnaire.

A low response rate increases the number of non-respondents which introduces a potential response bias in the results [96, p. 140]. A lower response rate raises concern about the generalizability of the results because the researcher does not know to what extent the respondents represent the population from which the sample was originally selected, and if the respondents and non-respondents equally represent the target population [96, p. 193]. According to Gay et al., the usual approach to dealing with non-respondents is to determine if they are different from the respondents in some systematic way. This can be done by randomly selecting a small sample of non-respondents and compare their responses with a random selection of the respondents responses. If the responses are approximately equal for the two groups, it can be assumed that the response group is representative for the original sample and that the results are generalizable [96, p. 193]. Even though it is recommended to determine the differences between respondents and non-respondents, this was not conducted in this thesis due to time and resource constraints. However, if the distribution of respondents from public or private sector, or at different hierarchical levels deviated more than assumed, it could have been necessarily to compare respondents and non-respondents.

Distribution method

The questionnaire was hosted on an online application called Nettskjema which is a digital data collection tool hosted and maintained by the University of Oslo (UiO) [107]. The main reasons for choosing Nettskjema as the survey tool were due to promised anonymity and privacy aspects (e.g. IP-addresses or other personal information about the respondents are not collected), professional reputation, suitable export methods (.csv) enabling statistical analysis afterwards, and that both of the researchers could corporate and access the form and results during and after the collection phase.

Even though surveys traditionally have been distributed via either mail or email, surveys should be distributed to potential respondents through communication methods that the targeted population is currently using [101]. Therefore several different social media platforms, which facilitate engagement between individuals [108], were used to distribute the questionnaire.

LinkedIn is a business and employment oriented online social media for professional networking and career development [109], and is widely used by recruiters to identify and target talented candidates to potential job positions [108]. Therefore, LinkedIn profiles usually contain information about users education, experience and skills, as well as abilities and strengths [108]. Compared to Facebook and other more general social media, LinkedIn also enables professionals in various fields, e.g. cyber security, to connect, and therefore provides the ability to efficiently target data collection in research to appropriate social networks [101].

Although not every individual within an industry population, or other populations, use LinkedIn, LinkedIn communities might however be considered suitable for initial targeting of subjects or respondents, which is an important step in snowball sampling. Some claims that if initial contact and request for participation is directed to appropriate persons from the target population, a representative sample can be collected [101].

The distribution process was divided in two different approaches due to the mix of purposive sampling and snowball sampling, as well as the proposed means of increasing the response rate:

1. Direct messages
    - Recruiting respondents within the researchers' professional network
    - Recruiting respondents outside the researchers' professional network

  - Obtaining "gateways" (referrals) into target populations or hidden populations

2. Publicizing on social media

The questionnaire was initially distributed via digital communication platforms such as email, Facebook messenger, LinkedIn and Signal to potential respondents, based on the sampling criteria, within the researchers' professional network which primarily contained current and earlier colleagues and students.

The researchers distributed a generic message including a short presentation of the researchers, information about the project, link to the questionnaire, as well as the encouragement of forwarding the questionnaire to other relevant respondents. To increase the response rate, minor adjustments of the generic message were required to personalize the request for each individual. This type of distribution method was assessed to be more fruitful than it actually was. Each individual was assessed to provide two or three additional respondents, however, only a few extra respondents were recruited based on this method. Accordingly, the distribution method was revisited.

Since direct messages to individuals within the researchers' existing professional network did not provide the expected amount of respondents, the network required to be expanded to recruit additional respondents for the questionnaire. In this case LinkedIn was assessed to be the most suitable social media platform as LinkedIn profiles usually contains information which could be mapped to the sampling criteria.

The sampling criteria for the purposive sampling were used to identify potential respondents for the questionnaire, as well as potential gateways into networks of potential respondents. Such targeted sampling enables greater control over the resulting sample, as the recruiting can be adjusted regularly, which contribute to increase the probability of collecting a more representative sample of the targeted population [101].

The networking approach on LinkedIn contained three steps and were conducted as an iterative process:

- Potential participants or referrals based on the sampling criteria were identified,
- connection requests to appropriate individuals were sent, and
- questionnaire invitations were sent to those who accepted the connection requests.

Firstly, potential participants and referrals were identified based on the sampling criteria. Individuals within different industries and hierarchical levels were identified by searching for relevant organizations within the different industry categories, given by SIC 2007, in combination with relevant job titles at different hierarchical levels. When potential participants were identified, additional individuals were identified via the individual's *Skills Endorsements*, where acquaintances can give endorsements, and via the *People Also Viewed* feature.

Secondly, after potential participants or referrals were identified, connection requests were sent. Since message content within connection requests is significantly limited on LinkedIn, only empty connection requests were sent to potential respondents. With hindsight, a short message explaining why the connection request was sent might have increased the connection request acceptance rate.

Lastly, if the individual accepted the connection request, a generic questionnaire invitation with certain personalizing adjustments was sent to the individual. The message contained: a short statement of why the individual received a connection request, a briefly presentation of the research project and why the individual was relevant for the survey, as well as a link to the questionnaire. The first part of the message aimed at making a good first impression of the researchers, establish survey importance, provide sufficient information such as guarantee for anonymity and estimated length of the questionnaire. The last part of the message aimed at motivating the respondent to answer the questionnaire by offering the results of the study, and making the individual aware of a future LinkedIn post about the study and the questionnaire. This was done to increase the probability of the individual to either share or "like" the post so that the post would appear in the individual's own professional LinkedIn network later and fortunately increase the number of relevant respondents. Additionally, the individual was asked to forward the questionnaire to its acquaintances or providing names of potential respondents the researchers could ask for participation.

The procedure of obtaining gateways into potential networks of respondents was similar to the recruiting approach described above. To increase the opportunities of recruiting respondents, the researchers also reached out to not qualified persons either within their network or persons assessed to likely have access to the hidden populations within the secret services, even though the snowball sampling technique traditionally suggests that only qualified persons that fulfill the criteria shall give referrals. Accordingly, Chief Executive Officers, top and middle managers, as well as analysts within other domains, etc. were contacted. These individuals shared the questionnaire internally with its organization, and the method seemed to provide several qualified respondents as the number of respondents with the industry category increased. A concern when applying snowball sampling to recruit respondents for a questionnaire, however, is the researchers ability to scrutinize the qualifications of the refereed subjects [101]. On the contrary, the questionnaire was created in such a way that the sampling criteria were included in the first part of the questionnaire avoiding people outside the target population to be included in the analyzed data.

	Sent	Accepted / response	Pending / no response
Connection request	281	188 (67%)	93 (33%)
Message	164	96 (59%)	68 (41%)

Table 4.4: Response rates on the social media website LinkedIn to questionnaire invitations.

LinkedIn is a social network site commonly used by malicious actors to gain information from or of individuals, or persuade victims to perform an action that will benefit the malicious actor in some way [110]. Since non of the researchers used LinkedIn actively prior to the data collection phase, one of the researchers updated its profile to appear more legitimate, increasing the probability of being accepted by the potential participants. Despite this, the connection request acceptance rate was assessed to be lower than 100% due to reasons such as organizational information security policies, as well as individuals' personal online security policies. Feedback from a few respondents indicated that the long response time of the connection request was related to social engineering concerns. However, after having scrutinized the profile, they decided to accept the connection request due to the legitimate appearance of the profile. Despite this, it is assessed that the high number of connection request non-respondents was due to security concerns. Another reason for non-respondents is the extent to which the LinkedIn users are active on LinkedIn. In the aftermath of the collection phase, several connection requests were accepted. However, this is not included in the response rate statistics.

A total of 281 connection requests were sent from one of the researchers' personal LinkedIn profile to potential participants or gateways. The amount of connection requests sent were significantly higher than the sample size due to concerns related to probability of connection request rejections. Within the data collection period, 188 individuals accepted the connection request, which represents a connection request acceptance rate of approximately 67%. Only 164 messages were sent as some of the potential respondents or gateways were either found not relevant, or recruited as an interview object instead. A total of 59% responded that they would participate in the study. This response rate does however not reflect the actual response rate of the questionnaire since the questionnaire was anonymous, preventing the researchers from knowing whom had responded or not. Additional details related to the connection request acceptance rate and the message response rate are shown in Table 4.4.

In addition to recruiting potential respondents directly through messages or via referrals, information about the questionnaire and a request for participation was posted on two social media platforms to reach beyond the researchers' professional networks.

The post was written and designed based on several LinkedIn posting tips provided by Fornes [111], to increase the reach and interest of the post. The most important posting tips applied were:

- Limiting the post length - maximum of 2000 characters,
- use spacing - line breaks every third line of text,
- limiting the number of hashtags - maximum of three hashtags,
- tag other people - maximum of three, and
- emojis - maximum 9 emojis.

As recommenced, only three, well selected hashtags were used (#nationalsecurity, #cybersecurity, #infosec) to reach people interested in either national security, cyber security or information security outside the researchers' network. Three individuals within the researchers' network were tagged in the post to increase the reach and to legitimate the post and survey. Additionally, in order to increase the response rate, the post offered the results of the study as recommended in [73, p. 172], as well as it aimed at establishing survey importance by gaining public attention from recognized individuals within the Norwegian cyber security community.

The posting on social media aimed at recruiting respondents to the questionnaire outside the researchers' network, in addition to increase the response rate, as the post would work as a follow-up activity providing a reminder to every individual within the researchers' network that had been contacted in advance. Since the most active data collection period was during the summer vacation, person-to-person reminders were not sent in order to prevent interfering more than necessarily with the potential respondents.

The post was posted on the researchers' own LinkedIn profile, and in a private Facebook group for ICT security in Norway. The extensive networking process described above facilitated for an extended reach as new network connections either "liked" or shared the post in its own network. The LinkedIn post was re-shared by 22 unique LinkedIn profiles both within and outside the researchers' network. Due to anonymity of the questionnaire, it was not possible to identify whether already contacted potential respondents were reminded and answered the questionnaire or if "new" respondents were recruited.

Since the distribution of the questionnaire included different approaches including both direct messages, referrals forwarding the questionnaire, and the publicizing of the questionnaire, it was not possible to assess the total response rate due to the unknown number of people who had received an invitation to the questionnaire or had seen it on different social media platforms.

4.4.3 Processing

In this subsection the processing of the quantitative data is described. When analyzing and interpreting mixed methods data, Leedy & Omrod [73, p. 336] argue that deciding what weight the quantitative and qualitative data will have when drawing conclusions is vital and should be done as early as possible in the research process, linking it to avoid any potential subsequent bias or unwanted adaptation of the data sets. Hence, general criteria according to embedded design was chosen as early as during the research project plan in early 2022, several months before data collection started. As previously described in Section 4.2.2 Mixed methods research design, embedded design describes when one research method dominates, with the other method serving a supplementary role. In such designs, the qualitative data may assist the researcher to analyze and interpret the statistical findings of the quantitative data [73, p. 331].

Thus, despite what some researchers hold as the "gold standard" in terms of processing mixed methods data, namely corroboration [76][112], corroboration was not the intended goal of this study. As the different types of data are biased by the assumptions and methods that elicit them, there are a number of possible outcomes, in which corroboration is only one [113]:

a) *Corroboration*: The same results are derived from both qualitative and quantitative collection methods,
b) *Elaboration*: The qualitative data exemplifies how the quantitative findings apply in particular cases,
c) *Complementarity:* The qualitative and quantitative results differ, but *together* they generate insights,
d) *Contradiction*: Where qualitative and quantitative findings conflict.

As per the previously described desired end-state and reasoning by choosing a mixed-method study, the desired outcome was to achieve *elaboration* between the qualitative and quantitative data. In limited cases where found necessary and applicable, the other outcomes were also used in order to provide nuance.

In mixed method studies, some scholars argue that there are no fixed procedures for analyzing and interpreting data [73, p. 337]. Despite this, several studies show significant advantages from integrating the to data types and propose techniques to do so [114][76][113]. Some advantages are when qualitative data used to assess the validity of quantitative findings, quantitative data used to help generate the qualitative sample or explain the findings from the qualitative data [114]. Additionally, qualitative data can assist in the development or refinement of quantitative instruments [114].

In this thesis, several processing methods were considered. Some researchers argue that qualitative data should not be used to illustrate quantitative results without first being analyzed in their own right using techniques appropriate for the type of data collected [76]. Others emphasize that the correlation between the responses from the different sampling methods are rarely examined [76], while some argue against corroboration through reference to the quantitative data, instead analyzing the data sets in relation to the relevant research questions [113]. Leedy & Omrod [73, p. 310-314] circumvents the issue, but instead propose several general guidelines for the analysis. Thus, no commonly agreed method of analyzing mixed methods data exists, as proposed by [73, p. 337].

Merging of different data sets or data from different sources are commonplace and known as *multi-disciplinary* or *all source* analysis within the intelligence community [115]. Due to the lack of established procedures to analyze mixed methods data in the research community, the authors of this thesis chose to utilize procedures established by the intelligence community. *Processing* entails five subprocesses [116]:

a) ***Collation*** - The registering and logging of the incoming information followed by its decomposition into individual information items. These individual information items are subject to categorizing according to either predefined categories or to new identified adapted categories. The categorized information items are finally cross-referenced with each others,
b) ***Evaluation*** - There are two types of evaluation within intelligence processing. The evaluation of information derived by human sources require subjective evaluation, and evaluation of information derived from technical sensors. In this thesis, both collection methods involve information collected from human sources, ergo the technical aspect will not be subject to further elaboration,
c) ***Analysis*** - Information is subjected to review in order to identify significant facts for subsequent interpretation. It consists of a number of interacting sub-processes to answer questions like "what is it?", "what does it mean?" and "why is it happening?" etc.,
d) ***Integration*** - Where analyzed information is selected and combined into a pattern. The process involves building pictures of current and predictive situations from the gathered and analyzed information,
e) ***Interpretation*** The significance of the analyzed and integrated information is assessed in relation to the current body of knowledge. In this thesis, this involved comparing the findings of this study to prior research, most notably that of Zibak & Simpson [37][13].

In the following paragraphs, each step in *processing* the quantitative data is described in further detail.

Collation

The *quantitative* data was both collected and tabulated through Nettskjema. By this, all data was directly and readily available for subsequent processing steps post collection.

Evaluation

The quantitative collection method was subject to rigorous evaluation prior to collecting data in order to mitigate bias in preparation of- and during data collection. This limited the need for evaluation during the processing phase. However, entries within the set of data which not met the requirements given by the sample criteria were discarded. A total of six entries were discarded due to this. Since all but the feedback and comment questions were mandatory, there were non uncompleted responses. A frequency count of the set of data was conducted prior to the analysis in order to verify the data and disclose any errors in the data set, as proposed by Gay et al. [96, p. 322].

Analysis

The analysis of the quantitative data included both *descriptive statistics* and *inferential statistics*. As the name indicates, descriptive statistics only describes the data, while inferential statistics can be used to draw inferences from the data [96, p. 29][117]. Inferential statistics was used in addition to descriptive statistics since descriptive statistics can not be used to make conclusions beyond the analyzed data such as drawing conclusion or making generalizations about a larger population [96, p. 341][117]. In order to assess whether the qualitative statistics were representative to the Norwegian cyber security community (the population), inferential statistics were applied. One important limitation with inferential statistics is that it provides data about a sample, not a fully measured population, and therefore, a degree of uncertainty will exist [117]. As inferential statistics use probability to determine the confidence level of conclusions made by the researcher, this holds also true for the analysis in this thesis.

In descriptive statistics there are typically five major types of statistics used to describe the data [96, p. 322]:

- frequency
- measures of central tendency,
- measures of variability,
- measures of relative position, and
- measures of relationship (correlation).

Within this thesis, *measures of relative position* will not be applied in the quantitative analysis of the data since scores given by individual respondents are not analyzed in light of the other respondents. However, correlation was applied to provide information about whether hierarchical level, experience or sector of the respondents affected the perceptions and attitudes toward CSIS.

Scale of measurement The scale of measurement determine the statistical procedures that can be used in analyzing the data [73, p. 110]. According to [73, p. 237][96, p. 151-152], there are four different scales of measurement:

a) **Nominal scales** - typically used to identify categories of people, objects or other entities in which there are no "degree" or quantity to be measured,
b) **Ordinal scales** - are similar to nominal scales, except that the categories have assigned numbers reflecting an order or sequence. In ordinal scales, the intervals between the ranks are not equal,
c) **Interval scales** - as with ordinal data, the values reflect differences in degree, but also *how much difference* exists within the variable being measured. In interval data, the value of 0 does not necessarily indicate a complete absence of the variable measured,
d) **Ratio scales** - are similar to interval data in that they reflect the intervals between values of the variable being measured. However, they have a 0-point, reflecting an absence of the measured characteristic.

The questionnaire comprised several different measurement scales resulting in different analysis procedures. All questions except for those considering feedback and comments, were close-ended questions of either single select or multiple select multiple-choice (part 1, 2 and 4), Likert items and Likert scales (part 3) or semantic differential (part 4). The close-ended questions in part 1, 2 and 4 were analyzed as nominal data.

When analyzing data collected through Likert scale, Likert items are treated as ordinal data when each statement, referred to as an *item*, is individually analyzed. In ordinal scales, the intervals between the ranks are not equal which limits the statistical methods used to analyze ordinal variables [96, p. 151-152]. When several Likert items are grouped, they constitute a Likert scale, and therefore the data can be analyzed as interval data [118]. Likert scales, in light of statistical analysis, contain multiple Likert items and are represented by totals or averages of answers to multiple Likert items. Accordingly, Likert scales are likely to be more reliable than individual Likert items. Despite this, the reliability of Likert scales should be verified by Cronbach's alpha coefficient of >0.7 or another appropriate reliability estimate [118]. When grouping several Likert items into a Likert scale additional statistics can be applied in order to describe the data. The different Likert scales used in the analysis were: *operational*, *organizational*, *economic* and *policy*. In this thesis, Cronbach's alpha was used to test reliability when testing for inference between the statements and contextual responses.

Analysis of semantic differentials can be done in several different ways as proposed by [119]. However, just like Likert items, the semantic differential items in part 4 were analyzed as ordinal data, while the semantic differential scale was analyzed as interval data [96, p. 157].

Frequency In descriptive statistics, *frequency* refers to the number of times each value of a variable occurs [96, p. 322]. For especially nominal and ordinal variables, a frequency count will provide descriptive information about the data [96, p. 336]. For interval scales, the overall average - *the mean* - provides a better description of the data than frequency count [96, p. 323]. Frequency counts were used to describe the distribution within the sample, as well as the nominal data in part 2 and 4.

In addition to measuring the central tendency and the variance of each Likert and semantic differential item, the distribution of responses (the percentage) were also measured to provide additional information about the perceptions and attitudes of the respondents.

Measure of central tendency A *measure of central tendency* is given by a single value and represents the central position within a set of data. Central tendency is a convenient way of describing a set of data with only a single number [96, p. 323]. The three most common measures of central tendency are: *mean*, *median*, and *mode*. The scale of measurement and whether the data is normally distributed determine what type of central tendency is most convenient to describe the central position in a set of data: the mean is used for interval or ratio data, the median for describing ordinal data, and the mode for nominal data [96, p. 323]. If the data is normally distributed, the mean, median and mode are identical and will all provide the most typical value in the set of data. However, if the data is skewed the mean will not be the best central position for the data because the skewed data is dragging it away from the typical value. On the other side, the median is not as strongly influenced by the skewed data. The more skewed the distribution is, the more the median will represent the central tendency compared to the mean [120][95].

As each Likert item or semantic differential item was analyzed as ordinal data, the central tendency of each Likert or semantic differential item was described with the median, while the four Likert scales (categories) or semantic differential scales (CSIS categories) were described with the mean as Likert scales and semantic differential scales are analyzed as interval data.

Measuring variability In cases where there are high degrees of variability in the collected data, the central tendency is accompanied by a description of the dispersion and deviation. To derive meaning from data, then, it is important to determine not only their central tendency but also their spread. And it often helps to pin down their spread in terms of one or more statistics. The more the data cluster around the point of central tendency, the greater the probability of making a correct guess about where any particular data point lies. The three most common measures of variability are the *range*, the *quartile deviation*, and the *standard deviation* [96, p. 325].

When the median is used to describe the central tendency of a set of data, the quartile deviations is more appropriate than the other types of variability measurements [96, p. 325].

When appropriate, the variability was described by either highlighting the distribution or by describing the *interquartile range*, due to its applicability on both ordinal, interval and ratio scales. To ensure easy correlation and readability, no other variance measures are used unless explicitly stated. The interquartile range is measured by dividing the distribution into four equal parts (*quartiles*), and subtracting the Q1 value to the Q3 value, as denoted in the following formula [73, p. 246]:

$$\textit{Interquartile range (IQ)} = \textit{Q3 - Q1}$$

To summarize, both the Likert items and semantic differential items were described by the median accompanied by the interquartile range representing the variability of the data.

As measures of variability are usually inappropriate for nominal data [73, p. 247], frequency counts of the close-ended questions in part 1, 2 and 4 were used to provide the distribution of each answer options provided by the respondents.

Measuring correlation *Correlation* is the process of discovering and measuring whether two or more variables are associated and affect each other. The resulting statistic is called a *correlation coefficient* and is represented by a number between +1 and -1. The correlation coefficient is used to assess both the **direction** and **strength** of the correlation. In case of a negative number, this indicates that the correlation is also negative, e.g. that a decrease in one variable will result in the other variable also decreasing and vice versa. The strength of a relationship is indicated by the size of the coefficient, e.g. a +1 or -1 indicate a perfect correlation [73, p. 249]. A coefficient close to either +1 or -1 indicate a strong correlation, e.g. that the two variables are closely related and thus allows for predictions on the level of the other variable with significant accuracy.

As half of the Likert statements were negative and the rest positive, the values for the negative questions were reversed to achieve correspondence between the response categories, making low and high scores respectively indicate negative and positive attitudes when testing for inference [121].

Then, the statements were processed to ensure that the data adhered to prerequisites or assumptions for the following statistical procedures. The most widely used statistic for calculating correlation is the *Pearson product moment correlation*, further referred to as *Pearson r* [73, p. 249]. The Pearson r was the main correlation statistic used in this thesis when examining two interval or ratio variables. The second correlation statistic used is the non-parametric *Kruskal-Wallis test*, which is used to examine the inference between a nominal independent variable and an ordinal dependent variable. Correlation does not, however, necessarily indicate causation by itself. As this study is performed by mixing methods, the qualitative results were used to enhance the diagnostic and predicative value of the quantitative analysis where applicable, further exploring causal relationships found in the quantitative results.

A major goal for the inferential analysis was measuring whether there were any inference or correlations between the respondents' backgrounds and their attitudes toward the categories stated in Table 5.12. This was pursued to map potential biases or influences inflicted by the respondents' role, experience or sector. As a purposive non-probabilistic sampling method was used (as described in Section 4.4.2 Sampling method), the assumption of independent selection of participant is at least partially violated. As the population was small, hard-to-reach and well interconnected prior to the study, in addition to the researchers' efforts to recruit participants from different sectors, with different roles and experience, it was assessed that inflicting major sampling biases likely was averted and that random sampling could be assumed. Given that all other assumptions were met when conducting the statistics, more powerful parametric tests like independent samples *t* test and Pearson's Product-Moment Correlation were preferred [96, p. 350].

To test whether the variables adhered to the parametric assumption that the measured variable must be normally distributed, a *Shapiro-Wilk test* was run. Shapiro-Wilk was chosen over the *Kolmogorov-Smirnov normality test* due to the sample size. If the assumption was met, an independent samples t test was performed to determine inference between the variables. Independent samples was chosen over paired samples as the independent variable (e.g. various groupings) splits the sample into differentiated subgroups, not affecting the values of the other sample groups. As this study is descriptive, a larger alpha value of 0.5 was chosen.

Given normal distribution, the Pearson product correlation[1] was used to measure inference between ordinal independent variables and composite dependent variables assuming that the sample was normally distributed.

$$r^x y = \frac{cov(x,y)}{\sqrt{var(x)}(x)\sqrt{var(y)}}$$

In this test, a -1 indicates a perfectly negative linear relationship, 0 indicates no relationship, while +1 indicate a perfectly positive linear relationship. E.g., 1 < | r | < .3 ... indicates a weak correlation, .3 < | r | < .5 ... indicates a moderate correlation while .5 < | r | . . . indicates a strong correlation.

[1] The Pearson product correlation is also known as Pearson's Product-Moment Correlation and Pearson correlation.

The *Mann Whitney test*[2] was used as a non-parametric alternative to the independent samples t test using the following test statistic

$$U_1 = n_1 n_2 + \frac{n_1(n_1 + 1}{2} - R_1$$

$$U_2 = n_1 n_2 + \frac{n_2(n_2 + 1)}{2} - R_2$$

to test which of the hypotheses are most likely correct:

$$H_0 : \text{The populations are equal,}$$

$$H_1 : \text{The populations are not equal.}$$

The Mann Whitney test only assumes that the observations are independent, but are less powerful than the independent samples t test and thus less likely to display statistically significant results [122, p.100-102].

Integration and interpretation

As the quantitative data was the dominant set of data, integration and interpretation of the statistical results were conducted prior to integrating the qualitative data. The integration and interpretation of the quantitative and qualitative data is elaborated in Section 4.5.3 Processing.

4.5 Qualitative research method - In-depth interviews

As described in Section 4.2.2 Mixed methods research design, the in-depth interviews were chosen as a complimentary collection method to achieve triangulation of data from the questionnaires, which is described in Section 4.5 Qualitative research method - In-depth interviews. As the questionnaire was non-dynamic and rigid, the interviews enabled the collection of deeper insight and more detailed, holistic and nuanced reflections from cyber security professionals.

The qualitative method is described by dividing the research process into four parts, mirroring the sectionalization of the research process as a whole: *1) Direction and planning*, *2) Collection*, *3) Processing* and *4) Dissemination*.

4.5.1 Direction and planning

In this subsection, all factors related to planning and preparing the qualitative data collection is covered - from selection of qualitative collection method, planning the interviews and up to the execution of the data collection.

[2] The Mann Whitney test is also known as the Mann Whitney U test, the Mann Whitney Wilcoxon test and the Wilcoxon Rank Sum test.

In-depth interview design

Within the mixed method design, questionnaires and interviews are regularly paired as they seen as having differing and arguably complementary strengths and weaknesses [76]. According to Johnson & Rowlands [123, p. 101], in-depth interviews excel when researching topics where individuals or groups have complicated, multiple perspectives on one phenomenon. Whereas questionnaires excel at generalizing results, in-depth interviews enable researchers to grasp and articulate multiple perspectives on, and meanings of, activities and events [123, p. 102]. In-depth interviews allows a researcher to build rapport which increases trust, honesty and willingness, allows clarification of ambiguous answers and seek follow-up information [73, p. 160]. But, they are much more resource intensive to conduct and thus are less practical than questionnaires when large sample sizes are important [73, p. 160].

Interviews are generally divided into two sub-categorizations [75, p. 65] [73, p. 160]:

a) *Exploratory - or semi-structured - interviews*, in which researchers may elaborate on standard questions with individually tailored questions. This allows for greater flexibility when conducting the interview and scientific discretion of the researcher,
b) *Standardized interviews*, in which all subjects are asked the same set of questions.

Semi-structured interviews were thus selected as the complimentary collection method to questionnaires due to its inherent in-depth and exploratory nature - fulfilling the researchers' criteria for selecting the mixed method research design.

To assist the researchers in conducting the interviews and ensure validity between the qualitative and quantitative research designs, both researchers took part in producing both the questionnaire and the in-depth interview guides. As some adjustments, improvements and adaptations were applied to the questionnaire (as described in Section 4.4.1 Questionnaire design), the interview guide was made *after* the questionnaire was tested and amendments were made.

A vital goal was synchronization between the collection methods and ensuring viability during the analysis of both qualitative and quantitative approaches. To achieve this synchronization, the following steps were made:

1. The interview guide was mirrored against the final questionnaire design consisting of four parts (excluding part 5 regarding feedback on the questionnaire) as described in Section 4.4.1 Questionnaire design,
2. The questions were formed and wording aligned with the questionnaire,
3. Finally, a thorough review of the interview guide was performed, ensuring both compatibility in wording and definitions, and comparative alignment

to the research questions.

It must be noted that minor adjustments were made to the original questionnaires. Questions not relevant to this research was removed, and relevant questions were amended (e.g. simplification of wording, synchronizing terms and definitions) while still maintaining the intent behind each question. This intent was imprinted in each of the categories of the qualitative and quantitative approach. But, unlike the questionnaire, all questions were open-ended and neutral to mitigate any applied bias to the subjects.

As with the questionnaire, the interview guide contained four parts:

1. The context and experience of the interview subject,
2. Questions regarding CSIS in Norway: how they would define CSIS, if and who they share information with and if their organization participate in any CSIS partnerships (CERT, CSIRT, ISAC or other partnerships),
3. Questions on current perceptions regarding benefits and challenges with CSIS in Norway,
4. An open-ended variant of the equivalent questionnaire part 4, as described in Section 4.4.1 Questionnaire design, intended to achieve insight into willingness and usefulness of the four CSIS categories.

Part 1 included questions regarding the interview subject itself and their organization. In the in-depth interviews, part 1 served several purposes. On the inter-personal plane, part 1 served as a "warm up", containing non-controversial and non-sensitive information, building rapport and trust between the subject and researchers [73, p. 160][75, p. 73][124]. It also gave information which in some cases was not publicly readily available regarding the organizations' role in FNFs, elaborated on their position and responsibilities, and their previous experience in cyber security. The latter was important to map any bias formed through previous experiences, potentially skewing the qualitative results. As with the equivalent part on the questionnaire, the purpose was not aimed at answering any of the research questions.

Part 2 was aimed at mapping the subjects' organizations' engagement in CSIS and who they share information with, thus partially answered RQ1. In addition to being fact-oriented (e.g. *who do you share information with?*), it also explored the underlying cases leading to any information sharing cooperation) and if CSIS partnerships were made, burrowed into what led them to initiate this cooperation's and why the subjects and their organizations still partake in them.

Part 3 was designed to answer RQ2. Unlike the close-ended statements used in the questionnaire, a highly open set of questions were used to map the subjects' perceptions. However, the interview guide also contained elements from the questionnaire part 2, where a more detailed elaboration on benefits and challenges when performing vertical and horizontal CSIS was added. These nuanced specifications were chosen as the research planning unveiled confronting attitudes when private organizations perform CSIS and cooperate with national services (e.g. NSA, NPSS and NIS) [68].

Part 4 was specifically designed to mirror the equivalent questionnaire part as much as possible, and accordingly answering both RQ1 and RQ3. Even though the questions were still open-ended, the same CSIS categories as were used in the questionnaire served as prerequisites to ensure compatibility and validity between the collection methods. The categories used were based on Zibak & Simpson [37] and intended to be exhaustive[3]:

a) **Data sharing** aims to give a receiving organization a more complete picture of the nature of a cyber security threat, incident, or vulnerability. The main goal of this type of sharing is to inform a decision or assessment or to increase the chance of a successful detection of, triage of, and response to, cyber threats. Such information can be shared in e.g. intelligence reports.

b) **Alerts & Triggers for action** aims to direct the receiving organization to an unknown threat or vulnerability, and often bring to attention the need for decisions of the receiving organizations did not know prior to the alert. In this category, timeliness is more important than the degree of data processing and confidence in assessments.

c) **Knowledge sharing** is not intended to share immediate or time-sensitive information, but aims to build a common pool of knowledge, advisories and lessons learned across different organizations. This may be done through post-breach reports, case studies or intelligence and security products provided by security vendors, national organizations or security organizations.

d) **Expertise sharing** aims to bring together individuals from separate organizations to exchange and apply multidisciplinary expertise to tackle common security issues or challenges. In contrast to knowledge sharing, expertise sharing brings people and their expertise together either physically or digitally.

Upon transitioning to part 4, all subjects were presented with the categorization and were able to voice any questions. Additionally, they were given a written handout with the categories to assist during answering part 4. One observation made by the researchers was how subjects with intelligence background had more trouble understanding and distinguish category a) *Alerts & triggers for action* and b) *Data sharing*. This was attributed to cultural biases, as intelligence literature strictly divides data, information and intelligence by degrees of processing and insight [115]. The etymological uncertainty could have easily been avoided by labeling the category as *information sharing*, which is further described in Section 6.4 Improvements to the study.

[3] The categories are previously listed in Section 3.3.3 Information sharing categories but reiterated for the readers' convenience.

Even though the interview guide part 4 mirrored the questionnaire part 4, the question wording were carefully altered to allow for more holistic answers, while still measuring RQ1 (engagement in CSIS), RQ3-1 (perceived usefulness of CSIS efforts) and RQ3-2 (perceived willingness to engage in CSIS efforts). One example is the last question of part 4: "*Which organizations is your organization most willing to share information with?*"

a) Cyber security organizations (e.g. ISAC, CERT, CSIRT, SOC, etc.),
b) National services (e.g. NSM/NCSC, PST, NC3, FCKS, etc.)[4],
c) Similar organizations as your own,
d) Not applicable.

Instead, the equivalent question in the interview guide was "*Who are you most and least willing to share information with, and why?*". These changes in question wording was done to allow subjects to express their own ideas and perceptions spontaneously in their own words, avoiding leading questions which may portray biases onto the subjects [75, p. 74].

Anonymization

Anonymization of interviewees are subject to a number of ethical and legal considerations, and may threaten the integrity of the study [125]. Although there are no consensus on how to define *research integrity* [126], several studies agree that it both encompass positive personal characteristics of the researchers themselves, in addition to the research process (including data, analysis and subsequent dissemination in publications) and the result itself [126][127][128].

However, the practice of anonymization prevents transparency as the the sources and source material are not publicly available, a key characteristic of a research project with high integrity and reliability [126][128]. DuBois et al. [129] argues that this may be less relevant when conducting qualitative research, as "there is no reason to drag qualitative research into the mire of reproducibility". As there are numerous ways to interpret qualitative data and because it is highly affected by external factors and thus also subject to bias, they conclude that there is no reason to think that any two researchers would come to the same conclusions when conducting qualitative research on the same research questions [129].

Sanders et al. [130] make several recommendations for addressing the issue of anonymization based on their experience:

1. Devising elaborate strategies for disguising, including changing non-essential details,
2. Using several pseudonyms when presenting extracts from the same subject,

[4] As the survey was distributed to the Norwegian cyber security community, the Norwegian acronyms for NSA, NPSS, NIS, NC3, and Norwegian Joint Cyber Coordination Centre (JCCC) were used.

3. Giving realistic expectations to the extent of the anonymity the researchers may provide, both prior to the interview and as part of the formalities tied to the interview itself,
4. Including the potential for readers to identify the subject through cross-linking online information with interview data, emphasizing the risk if the subject either has or in the future exposes herself in open forums.

These recommendations are in conflict with what other qualitative researchers promote, especially the use of pseudonyms or "smoke screening" (as proposed in [125]), e.g. changing personal traits to make identification difficult. DuBois et al. [129] further argues that while this approach may succeed in anonymization, it does this by introducing inaccuracies. They instead propose de-identifying participants by excluding identifiable information or making some identifying data more vague.

Several possible anonymization schemes were originally considered:

a) Fully disclosed identities: name, position and organization is stated,
b) Partially disclosed identitites: only the position and organization is stated, whereas the subject's name is withheld,
c) Fully anonymized identities: only non-specific traits and characteristics are used. The interview subject mass is described in general and individual expressions are not linked to any specific individual.

After careful consideration alternative c) was chosen. Even though this have implications on the transparency and reliability of the study, it was the only feasible method of recruiting interview subjects from the previously described so-called "secret services", which in Norway constitute the backbone of the Norwegian governmental Cyber Security Information platforms. By possibly excluding this interview subject category, the risk to the project's viability were seen as superior to the risk posed by over-anonymizing the informants. This approach also had several benefits of the qualitative viability: A major concern was the subjects' ability and willingness to speak freely, truthfully and disclose all relevant perceptions as they may have been restricted by perceived or actual policies by their employer.

By choosing alternative c), informants were decoupled from their enterprise or organization, thus possibly reducing politicization of their answers and mitigated bias. Some of the informants stated during the interviews that this approach was crucial to their participation, or enabled them to elaborate on their experiences more freely than they otherwise would have. Additionally, the authors of this paper argue that the use of mixed methods reduces the contextual significance of each individual statement, as the qualitative research has a reduced role in "only" enriching, explaining and exemplifying the quantitative findings. Considering all factors stated above, the value of heavily anonymizing was assessed as outweighing the risk to academic validity.

4.5.2 Collection

Sampling method

Non-probabilistic purposive sampling were used due to a number of factors: 1) the limitations in sample size and its practical implications, 2) to ensure a dispersion in both sectors and positions of the subjects, and 3) to include interview subjects from the Norwegian so-called "secret services" (NSA, NPSS and NIS). If a random *probability sampling* method was used, it was deemed as less likely to recruit subjects from this personnel category due to their focus on personnel security and perceived organizational reservations against participating in unclassified research projects. A non-probabilistic approach is supported by research, as random sampling is, by some, deemed as inappropriate for qualitative studies [131]. With small sample sizes, sampling errors are likely to be so large that bias are inevitable. Additionally, Marshall [131] argues that a random sampling of a population only is likely to produce a representative sample if the characteristics researched are normally distributed within the population - where some subjects are more likely to provide insight and understanding to the researcher.

To ensure the external validity, sampling by utilizing PMESII categories was used to include cyber security professionals from separate sectors and organizations. The only prioritized common denominator was their experience with CSIS. PMESII is a common modeling technique within the NATO intelligence community for describing variables of the operational environment. The variables presented through the PMESII model were assessed as adequate preliminary inputs with regards to providing external reliability through dispersion of interview subjects. Each factor (e.g. Political) is designated as a *domain*.

P **Political** - Cyber security personnel working in a political body (the parliament or ministries) in which one of the prioritized FNFs conclude,

M **Military** - Cyber security personnel working within the defense sector and national security organizations which engage in CSIS,

E **Economic** - Cyber security personnel working in financial entities supporting FNFs,

S **Social** - Cyber security personnel working in health care, educational organizations etc.,

I **Infrastructure** - Cyber security personnel from organizations providing constructing and maintaining infrastructure, such as telecommunications, transport, cyber infrastructure etc.,

I **Information** - Cyber security personnel engaged in public or private media organizations, or otherwise primarily engage in information dissemination to the public.

Using the PMESII categorizations, several relevant undertakings within each domain were identified during the research project planning process. This selection were based on the researchers experience and professional knowledge, central nodes in the Norwegian cyber security landscape (as previously discussed in Section 3.4 The Norwegian cyber security landscape) and a preliminary assessment on ease of access versus perceived value to the research. The list of relevant organizations formed the stepping stone for identifying relevant *individual subjects*, which in turn was approached by the recruiters. The recruitment process is further elaborated later in this section. To select relevant individuals, the following criteria was formed:

a) They must have a comprehensive understanding of CTI or CSIS,
b) They must have comprehensive experience with CTI or CSIS,
c) Their organization must be part of a supply chain supporting Norwegian FNFs,
d) Their organizations' domain according to PMESII,
e) Their positions within their organization to ensure a varied sample.

Sample size

The sample size of in-depth interviews are, at best, heavily discussed among researchers. While some researchers provide a specific recommended number of interview subjects [132], most provide general guidelines ensuring validity and reliability [73, p. 336]. In this study, two interview subjects per PMESII domain was assessed as sufficient to mitigate individual subjects' bias and achieve a more holistic and valid representation, while limiting the total number of respondents. This limitation enabled longer interviews, thus providing a deeper insight and a better understanding of the subjects, and their reflections.

Sampling techniques

Identifying and recruiting interview subjects Face-to-face interviews have the distinct advantage of enabling a researcher to establish rapport with potential participants and therefore gain their cooperation. Thus, such interviews yield the highest response rates - *the percentages of people agreeing to participate* - in survey research [73, p. 160]. Despite this, some researchers note that recruiting subjects may be challenging, recommending a number of recruiting strategies [133], including:

a) Conducting the research in partnership with communities, consumers or advocacy groups that are affiliated with the desired subjects,
b) Recruiting through informal networks, community organizations or agencies,
c) Recruiting through existing organizations and networks, assisted by a contact person to gain entree,
d) Using available lists or other accessible sources naming relevant personnel,
e) Sending personalized messages and follow up, stressing the importance of

Category	# of subjects	Percentage
Pseudo-random	3	23%
Referrals	5	38%
Acquaintances	5	38%

Table 4.5: Distribution of in-depth interview sampling selection.

the potential subject for the research and how this would benefit the community.

A combination of the recommendations above were used in sampling for the in-depth interviews. The researchers were also helped by several external factors: a) Both researchers have partly overlapping, partly complimentary professional networks within the Norwegian cyber security community, b) the war in Ukraine and c) several recent cyber attacks against Norwegian public and private organizations which have resulted in an increased public awareness on external threats and the need for cooperation, especially within the cyber domain [6][5][134][135].

Based on the list of desired organizations and the criteria for selecting interview subjects (as shown in Section 4.5.2 Sampling method), the researchers identified suitable subjects in their own professional networks thought to have the necessary prerequisites for fruitful participation in the study. However, most acquaintances of the researchers were either in middle management or practitioners. To recruit subjects from relevant organizations' top management, the researchers identified key contacts within their professional networks which could assist in identifying and recruiting suitable subjects. However, to ensure a sufficient variety in the sample, it was also necessary to recruit subjects outside the researchers' professional personal and extended network.

Thus, the recruitment process was divided in three distinct approaches: *1) Pseudo-random* selection where subjects were identified based on openly accessible information regarding position, their organizations' relationship to FNF and PMESII domain through social networks (primarily LinkedIn): *2) referrals*, where highly connected and experienced personal acquaintances were used to pinpoint and recruit relevant interview subjects: and *3) acquaintances*, where a professional connection to the relevant subjects existed prior to the research. Note that *pseudo-random* in this context only describes the non-existing relationship between the researchers and the interview subjects - it is still non-probabilistic and purposive. The dispersion of interview subjects are depicted in Table 4.5.

Conducting the interviews When conducting interviews, there are traditionally four forms in terms of the number of participants [136]: the most common form is a one-to-one interview, involving one interviewer and one subject. Another form is the joint interview (also known as *couple interview, conjoint interview or dyadic* *interview*), where there is one interviewer and two subjects. The final two interview types are the group interview and focus group, in which a researcher studies a group of subjects of which the former typically refers to one interviewer studying "a horde of subjects" [136]. However, studies rarely discuss the number of *interviewers* [136], but some advocate the approach of using multiple interviewers, in which most recommend two [136][137][138][139]. An interesting note is that most available studies advocating a multi-interviewer approach, originate from the late mid-nineteenth century to the mid nineteen eighties. However, no studies have disproved this approach as an effective sampling method.

There are both advantages and disadvantages when using two interviewers. Firstly, both Kincaid & Bright [138] and Bechhofer et al. [139] note that they experienced an increased efficiency in collecting data combined with gains in validity and reliability. In Kincaid & Bright's study, they found that when using two interviewers, the subject always had the complete attention of one of the interviewers. It was not necessary for the subject to talk to a person who was partially or wholly occupied with note-taking, making the subject more comfortable and able to talk more freely. They also note the advantages of utilizing the individual differences of the interviewers: they each bring their different personal qualities and backgrounds in training, interests and personal experience. This also had an impact on the *rapport* built with the subject - in some cases, the subject responded better (or even had negative reactions) to one interviewer, enabling the interviewers to build off on these interpersonal relations formed during the interview [138][139]. Using two interviewers also increased the precision of the questions posed: one or the other interviewer was likely to detect if the subject did not understand the intended meaning of a question and rephrased it accordingly [139]. They also experienced that *tandem teams* (Kincaid & Bright's [138] term for a two-interviewer team) served as a check on leading questions and other sources of bias which may have influenced the collected data.

During an interview it will often take unexpected digressions following the subject's interest or knowledge. Even though they are likely to be productive, it is vital that the interviewer is assertive enough to return the interview to its planned course when necessary [124]. Bechhofer et al. [139] experienced that by being two, they were able to "cover ground" faster and it made it easier to change the subject.

However, there are some clear disadvantages by using two interviewers: First and foremost, the method is very resource intensive as both researchers have to allocate time, and it requires interviewers which are sensitive to both the subject, the interview content and between themselves [139]. When comparing the obvious advantages and disadvantages, the researchers find it surprising that not more in-depth interviews are conducted by two interviewers.

As a result, a two-interviewer approach for the in-depth interviews were chosen for this research project. The experiences during this research process support all the previous findings stated above. The flow of information during interviews was more effective, and the two researchers were able to play off of each other and thus create a positive environment in which rapport with the subject was more easily established. An additional advantage (which is also mentioned by [137]) was that during the interviews, some subjects covered almost all intended topics as a coherent (and most often highly interesting) monologue without any guidance from the interviewers. When facing this kind of subjects, it is easy to miss central questions from the interview guide and thus reduce value and coherency of the collected data. By being two, one of the interviewers were able to take notes on which topics were already covered, and directed the interview toward those missing topics.

Before conducting interviews, the researchers reviewed a list of bias and mitigating measures (as shown in Table 4.6), and conducted a de-brief after each interview. This debrief functioned as an informal hot wash-up with a talk-through of the researchers performance regarding bias and interview techniques, the most interesting topics and viewpoints, and consistencies and inconsistencies between previous interviews. This session increased awareness on the researchers' own performance and possible pit-falls which would require special attention during later interviews. Additionally, the subsequent analysis was easier as the key content was synchronized between the researchers.

Right before the interviews, the researchers de-conflicted who would "lead" the upcoming interview. This role included revisiting the rights of the subject, the intended goal of the study and leading the interview itself. This was done to have a more fluid start of the interviews, thus supporting the development of rapport and improving the perception of the researchers' professionalism. The "passive" interviewer was responsible for noting especially important or interesting themes brought up during the interview, and keep track of topics covered. As the "passive" interviewer was less involved in the interview itself, the person was often more effective in identifying relevant follow-up questions and keep the interview on topic. Often, the roles between the "active" and "passive" interviewer were spontaneously reversed during the interview if the "passive" interviewer identified key topics to be discussed or wanted elaboration on previously covered topics.

Even though both researchers were present during all but one interview, all interviews were recorded. This was done to enable the researchers in focusing on the interview at hand with as few distractions or unnecessary "chores" as possible. By recording all interviews, the need for revisiting previous interview subjects to clarify certain items was also reduced to a minimum. All but one interview were conducted face-to-face (one subject got sick with COVID-19 and were forced to isolate himself) at a location chosen by the interview subject. This was done to ensure that the subject was comfortable and felt in control of the situation, as the researchers assessed that the subject would be more likely to speak freely and relaxed. After the interview was concluded, the recording was transcribed and coded, primarily following the same categorizations as described in the in-depth interview design. However, part 4 regarding CSIS categories were written out in detail. In addition, a short summary on key topics and statements were formed on all interview objects. The processing is further described in Section 4.5.3 Processing.

In the interview guide (shown in Appendix A.4 Interview guide), only the main questions were described in detail. This is contrary to what some scholars [73, p. 282] recommend. Even though it was not due to a conscious choice by the researchers, identifying suitable follow-up questions for all interviews would have been challenging, as the interview subjects' answers varied both in form and content. While some subjects had a more passive approach and required more active guidance from the interviewers, others had to be frequently "reigned in" to get back on the intended course, with multiple highly fruitful alternative avenues and digressions prompting more active interviewers to fully explore the topic at hand.

Johnson & Rowland [124] argue that an impersonal approach, in which the interviewers are to stick to the stated questions, avoiding offering any kind of personal information or revelations about their own opinions or other actions that may influence the subjects, is not a realistic ideal for in-depth interviewing. This is because the research question(s) itself usually involves a deeper process of mutual self-disclosure and trust building [124]. However, the researchers chose a middle ground between the two extremes: as little leading as possible, but still exploiting the researchers' background and professional experience to build rapport, trust and gain access to the subjects inner reflections.

Response rate

The response rate on interviews were surprisingly high. A total of 28 suited subjects were identified in the subject mapping process and categorized according to PMESII and the individual subject criteria. Based on this list, two individuals per PMESII domain were selected and approached, while the remaining was "in reserve" in case the primary subjects rejected the initial approach or withdrew from the study. Of those approached, 76% agreed to participate, whereas the remaining 24% proposed personnel within their organization which they though were more suited to participate in the study.

4.5.3 Processing

The theoretical backdrop applicable for both research methods were previously discussed in Section 4.4.3 Processing. Thus, this subsection expands on those presented in quantitative processing and elaborates on special features present for processing qualitative data.

Collation

Whereas the quantitative data was readily available for subsequent processing post collection, the *qualitative* data demanded several additional steps after each interview was concluded. Immediately after any given interview, the interviewers performed a quick de-brief, in which the main topics and impressions of the interview in question was discussed and recorded. Then, each interview was transcribed. As every interview was voice recorded, the nuances as they were presented by the interviewee was preserved and written in separate text document which included brief summaries and initial evaluation of similarities and discrepancies between the content of different interviews. Additionally, key topics or subjects according to the categories described in Section 4.5.1 In-depth interview design were color coded. Subsequently, coded and categorized data was transferred to an excel-document. Upon identifying key characteristics and themes, the mixed methods and qualitative analysis software NVivo was used to perform a thematic analysis based on both the interview guide/questionnaire sections and initial coding schema.

Evaluation

Both collection methods were subject to rigorous evaluation prior to collecting data. This was done to mitigate bias in preparation of - and during data collection. In both methods, the bias mitigation efforts identified in the research plan (depicted in Table 4.6) were actively utilized when forming the questionnaire and interview guide, but also when recruiting participants. In the qualitative data collection, it was also used as preparation before conducting the interviews, to minimize the risk of biases thwarting the end results.

Evaluation normally involves evaluation of the source's trustworthiness or reliability and the information content [140]. In this thesis, both researchers partook in all information collection, and had control over collection gathering, limiting the number of uncontrolled factors. As previously described in Section 4.4.2 Sampling method and Section 4.5.2 Sampling method, non-probabilistic sampling were chosen as the main sampling method. Thus, the researchers were able to select the most suited participants which was assessed as having direct access to the information (e.g. experiences and knowledge) that was sought. This is fully true for the qualitative sampling, but external influencing factors were harder to detect during the quantitative sampling. This was part due to the level of anonymization during the qualitative collection, part due to snowball sampling and the fact that the researchers had no way of confirming which individuals participated and if they answered truthfully.

To summarize, evaluation was mainly addressed by careful and precise planning before collection took place. In addition, both researchers participated in both creating the questionnaire and interview guide, thus are intimate with the workings of both collection methods. This limits the need to address evaluation in the processing phase.

Analysis

A thematic approach was chosen for analyzing the qualitative data as its purpose was to identify, analyze and report patterns within data [141], in contrast to other widely used qualitative analysis methods more heavily involving interpretation as grounded theory or hermeneutic phenomenology. This choice was made to limit importing or inflicting biases onto the processing process and subsequent findings.

Due to the chosen descriptive mixed methods research design and the emphasis on the quantitative data, the qualitative thematic analysis was modeled after the RQs and interview guide to prepare integration with the quantitative results. The analysis itself was done using NVivo. Other analysis software such as MAXQDA were considered, but NVivo was the only free software for qualitative analysis available for NTNU students off-campus. The NVivo software enabled the identification and categorizations of themes, and collation into *codes* which in turn made comparison and integration with the the quantitative results easier and more thorough. The synchronization used the same guidelines and considerations as described in Section 4.5.1 In-depth interview design. The thematic codes were created to mirror the intention and theme of each part in the questionnaire and interview guide:

a) *Attitudes*, including who the interviewees were most and least willing to share Cyber Security Information (CSI) with,
b) *Usefulness* and *willingness* toward sharing CSI with similar organizations, cyber security organizations and national services,
c) *Benefits & challenges* to sharing CSI with regards to general considerations not applicable for *b)* or *c)*,
d) *Information sharing platforms*, with social arenas and technological solutions as subcategories,
e) *Answers given to interview and questionnaire part 4*, subdivided into each CSIS category and lastly,
f) *Partners* - ergo who they share information with.

Emerging themes and recurrent events not covered by the initial codes (themes) described above were collated in sub-categorizations of the initial codes.

Integration and interpretation

As introduced in Section 4.2 Research design and elaborated in Section 4.4.1 Questionnaire design, this research project is a descriptive mixed methods study with a dominant quantitative collection method, in which the qualitative findings aimed to describe and elaborate on the findings made in the quantitative data. The *internal integration* were made in NVivo after collation and theme analysis in order to link interviewees' statements on the same or similar topic against each other. Due to this approach, the *external* integration (e.g. with the quantitative findings) was conducted in Section 5.2, in which statements made in the interviews were coupled against key words, statements and phenomenons in the questionnaire data.

The qualitative interpretation was conducted in conjunction with the quantitative findings in order to achieve data saturation on all relevant topics. This approach had a high yield, due to the thorough correlation, joint planning, collection and processing. The tight correlation between both research methods enabled a high resolution on the findings. To avoid adding biases and achieving the most nuanced and realistic outcome, divergent answers were both included in Section 5.2 Analysis and integration.

4.6 Considerations on validity, reliability and research ethics

This section describes the researchers' considerations to ensure the validity and reliability of the research process. The section gives an overview of the most important issues considered and the main measures taken, whereas methodology-specific considerations were more thoroughly described in Section 4.4 Quantitative research method - Questionnaire and Section 4.5 Qualitative research method - In-depth interviews.

4.6.1 Considerations on validity

Validity is understood as the likelihood that a given study will yield accurate, meaningful and credible results [73, p. 103]. In simple terms, validity ensures that what is intended measured is what is in fact measured. Throughout the research process, the concept of *internal* and *external* validity was used. Internal validity is the extent to which a research study's design and the data it yields allow the researcher to draw accurate conclusions on the causal relationships of the data [73, p. 103], while external validity is the extent to which a study's results apply to situations beyond the study itself - e.g. the ability to generalize its results [73, p. 105]. Several measures were implemented to address validity. By conducting a feasibility study in the research planning phase, three main success factors related to the validity were identified:

1. Ensuring that sampling and interviews were free of biases and errors,
2. Ensuring a varied pool of respondents and informants, and
3. Synchronizing the questionnaire and in-depth interviews to measure the same factors.

To achieve validity, possible biases and errors were mapped and countering efforts were identified to each corresponding bias (the full list of biases and counters are depicted in Table 4.6). Even though purposive sampling were used, the selection of suited participants (e.g. quantitative respondents and qualitative informants) was made based on predetermined criteria to ensure both the suitability of the individual participants and a intra-sample variety using PMESII domains to represent the target population as accurately as possible. The main source of error in relation to purposive sampling, was the potential for inaccuracy in the defined criteria and the resulting sample selection [96, p. 141].

The researchers' background (i.e. knowledge, experience, current job and security clearance level) might have influenced both the willingness of the participants to partake in the study, and the extent of which informants managed to speak freely, truthfully and disclose all relevant perceptions related to scope of the thesis. As the researchers have several years of experience in national security, this likely increased the quality of the qualitative sampling (i.e. interviews), resulting in additional relevant information contributing to a more accurate and deeper understanding of the scope of the project which might not have been disclosed otherwise. Even though only unclassified information was revealed by the interview objects, the security clearance level of the researchers might have led the informants to reveal more honest and direct answers. It is also likely that the researchers' background led to an increased confidence in the protection of revealed information and anonymity.

Additionally, some of the informants were acquaintances of the researchers, which might led the informants to provide more honest and direct perceptions. However, these informants had prior working experience within either national services or law enforcement even though they represented another PMESII domain or private sector within this thesis - increasing the degree of homogeneity in the qualitative sample population. Despite potentially negatively skewing the sampling, this may also had a positive effect as the informants might had a deeper and more nuanced understanding of CSIS due to their experience in both public and private sectors.

As both snowball and non-probabilistic purposive sampling were used to recruit respondents for the questionnaire, the actual response rate of the quantitative survey were not obtained - affecting the validity and ability to generalize the findings. The chosen sampling technique also introduced the *self-selection bias*, in which the group of people being studied can decide whether to participate or not [142]. Often, this causes undesirable conditions in the sample, and can result in skewed responses as those choosing to respond (volunteers) are usually different from those not responding (non-volunteers). Volunteers may be more motivated or interested in the studied problem, possibly leading to more extreme responses. To counter this possible source of error, follow-up contact with non-respondents could have provided insights about potential bias provided by the respondents [96, p. 140-141]. This was however not done due to time constraints.

In addition to this, the obtained sample described in Chapter 5 Results indicated a skewed distribution of hierarchical roles, as the *middle management* group were notably larger than the other groups. Surprisingly fewer practitioners attended the questionnaire compared to managers, possibly indicating either a weakness with the recruiting method (LinkedIn), or that cyber security professionals in management roles have a higher personal engagement and interest in the research problem (self-selection bias). Another reason could be to what extent persons actually use LinkedIn, despite that they have accounts.

Additionally, there are strong indications of sampling errors in the quantitative research. Several questions contained variations of the answer option stating "my organization does not participate in CSIS". The number of respondents opting this answer varied between each questions in which this option was present. This may indicate the presence of a number of biases, most notably response fatigue. The questionnaire included an option to revise and return to already answered questions, thus indicating that the erroneous data were submitted unintentionally, either due fatigue or a lack of personal investment.

Furthermore, the questionnaire's contextual questions on distribution of cyber security personnel per industry and hierarchical level were prone to misinterpretations by the respondents, possibly causing inaccuracy in the collected data. The list of possible sources of errors in questionnaire sampling is extensive, and much effort was put into the simplicity and specificity of each question and statement. Sections particularly prone to misinterpretations (like Part 4 - *Attitudes toward CSIS* containing specific categorizations) were accompanied by explanations or iterated definitions to assist the respondents.

Due to the close-ended nature of the questionnaire, errors may have been introduced as respondents were forced to make choices on predetermined alternatives, without the possibility to comment these, except for in the last two feedback oriented questions in the questionnaire. To mitigate this, a pilot test was run on suitable test subjects with both a technical and non-technical background. The pilot focused on wording and phrasing of the questions, identifying leading questions, measuring response fatigue and questionnaire length, in addition to whether sufficient answer options of the close-ended, single select multiple choice questions were provided. In hindsight, a more extensive pilot study should have conducted, which is further elaborated in Section 6.4 Improvements to the study. To further increase the validity of the questionnaire, several contradictory statements could have been included in Part 3 - *Perceptions on CSIS*, however this was not done due to the possibility of response fatigue.

During the analysis of the quantitative data, it was identified that the wrong scale range had been used to measure the willingness to engage in CSIS efforts in part 4. The scale range that was used was "least willing" to "most willing", whereas it should have been "not willing" and "extremely willing" given that the study was intended to replicate Zibak & Simpson [37]. Despite this, it was assessed to not have major inflicts on the results as the respondents probably interprets the lowest value (1) as "negative" and the highest value (5) as "positive".

Analysis of factors involving the respondents' years of experience is another issue that might influence the validity of this study. Approximately 72% of the respondents had more than five years of experience within the field of cyber security, whereas 17% and 11% had two to five years, and less than two years respectively. This distribution may have led to skewed data and findings of this study, especially when crosstabulating experience with other factors. To limit the introduction of errors, only findings with distinct observable differences in experience are included in the results.

To ensure validity between the quantitative and qualitative research designs, both researchers participated in producing the questionnaire and in-depth interview guides. A thorough review of both guides were made to ensure compatibility in wording and definitions, and comparative alignment to the research questions. As the quantitative design was dominant, the interview guide was mirrored against the final questionnaire design. To mitigate any erroneous factors affecting the qualitative results, the interview itself was audio-recorded and transcribed. To avoid leading questions and the researchers inflicting biases onto the informants during the interviews themselves, both researchers were present for all but one interview. After each interview, an "after action review" type walk-through were performed to discuss key takeaways and provide feedback on each other with particular interest to areas to sustain or improve before the next interview.

Additionally, extensive research on acclaimed measurement and analysis methods related to quantitative, qualitative and mixed methods studies were performed. Before conducting inference testing, all Likert and semantic differential scales were tested for normality and internal reliability, and suited parametric and non-parametric tests were identified prior to testing to ensure that they were suitable with regards to testing the hypotheses in question. Despite the researchers' best efforts, there may be statistical procedures more applicable for processing the data collected in this thesis. Additionally, as this thesis was intended to replicate and expand on the findings of Zibak & Simpson [37][41], the researchers were bound by some aspects and procedures of Zibak which may have introduced inadvertent erroneous factors or biases. This is further elaborated in the section below.

4.6.2 Considerations on reliability

With regards to the qualitative processing, inter-rater reliability (where several individuals evaluate the same entity) was mainly used. As stated in the previous subsection, both researchers partook in all interviews except one. Even though the individual interviews were subject to an evaluation immediately following their conclusion, an emphasis was placed in not significantly altering how the interview was conducted. During the sampling process, efforts were made to ensure that informants from each PMESII domain were represented by at least two informants in order to reduce the influence that individual experiences, biases and focal points had on the data. No particular emphasis was placed on the other criteria (role and experience) other than following a general intention of internal variance within the qualitative sample. Based on the resulting analysis, these measures likely had the intended effect of generalizing the analytical findings. There were, however, some discrepancies between the perceptions represented in the quantitative versus the qualitative data. It cannot be ruled out that diverting opinions had a more significant impact on the results due to the comparatively small qualitative sample than a larger sample would have provided.

The quantitative sample was primarily tested for reliability through normality and distribution tests, of which none of the categories (operational, organizational, economic and policy) had a statistically significant influence on the results of the statements from part 3. As the thesis was intended to replicate Zibak & Simpson, the statements in part 3 were assigned to the same categories as in [13]. Some of the statements could have been assigned to a category better reflecting the statement. Even though the pairing of categories and statements might affected the inferential statistical significance of each category, the detailed analysis of each statement correlated with the qualitative findings likely mitigated this potential source of error.

It is the researchers' opinion that the scope of the sampling and the purposive diversified sampling enabled generalization. However, due to the rapid technological and procedural advancements in cyber security, further accelerated by increasing geopolitical tensions, the will to improve on the challenges and sustain the incentives found in this study has probably never been higher. Thus, the findings are expected to both be of high value when addressing areas in which to focus information sharing efforts going forward, but also to become obsolete within a short time frame.

4.6.3 Ethical considerations

It is important that all research projects reflect on the researcher's ethical and legal responsibilities as research often affects the privacy of participants, and the researcher(s) must be aware of not influencing the research or being influenced themselves. Due to the interactive nature of the sampling processes, the Norwegian Research Ethics Committee's (NEST) guidelines for Research Ethics in the Social Sciences, Humanities, Law and Theology was used over those provided by the committee for Research Ethics in Science and Technology. As the researchers gained access to sensitive personal and business-related information through the qualitative sampling in particular, a special emphasis on ethics were implemented. Most notably, this is apparent from the extensive sanitization and anonymization previously discussed in Section 4.5.2 Sampling method.

Previously, the need for anonymization in order to recruit informants from national services were discussed, but confidentiality through anonymization was also critical for several of the remaining informants as business sensitive information could be exploitable if not anonymization had taken place. Each participants were made aware of that all interaction with the researchers were under voluntary informed consent and could be withdrawn at any time, that confidentiality would be ensured and other relevant and applicable laws and regulations (see appendixes A.1 and A.2). All informants were also offered to read through their statements and the final analysis in which their statements were included to maintain the integrity and allow a final opportunity to withdraw from the study if concerns had arisen. However, none of the informants opted for a read through. Additionally, all data processing and management were in accordance with the legislation under the Norwegian Personal Data Act and General Data Protection Regulation.

Source of bias or error	Bias	Countering efforts
1. Question design		
1.1 Wording issues	Ambiguous question	- Use Likert scale or semantic differential - Avoid preconditions for questions - Test questionnaire before dissemination
	Complex question	- Use precise wording - Avoid unnecessary preconditions and limitations in question. - Test questionnaire before dissemination
	Double-barreled question	- Ensure that each question is intended to measure one factor
	Short question	- Precise wording - Test questionnaire before dissemination
	Technical jargon	- Test questionnaire before dissemination - Ensure dissemination to participants meeting sampling qualifying criteria - Provide definitions on key or ambiguous terms
	Uncommon word	- Avoid uncommon terms - Provide definitions if needed - Test questionnaire in pre dissemination
	Vague wording	- Provide definitions if needed - Precise wording - Test questionnaire in pre dissemination
1.2 Missing of inadequate data for intended purpose	Belief vs. behavior (hypothetical question, personalized question)	- Determine whether question is intended to collect on belief or behavior - Include varieties of questions in questionnaire (e.g., if you wrote X, then answer question Y)
	Starting time	- Only conduct collection within a short time span - Clearly define time periods (instead of “in the last 12 months”, use “in 2021/2022”).
	Data degradation	- Be aware of question design and degradation - Less valid for this project as there are few relevant static references
	Insensitive measure	- Use Likert scale or semantic differential with enough possible variations in responses to enable differentiation through discriminating power
1.3 Faulty scale	Forces choice (insufficient category)	- Use Likert scale or semantic differential consistently - Formulate questions with Likert scale in mind
	Missing interval	- Use Likert scale or semantic differential consistently
	Overlapping interval	- Use Likert scale or semantic differential consistently
	Scale format	- Use Likert scale or semantic differential consistently (no consensus as to whether odd or even scales are better)
1.4 Leading questions	Framing	- Precise and similar wording when two questions are used to cast light on two sides of a matter - Use Likert scale or semantic differential consistently
	Leading question	- Test questionnaire and interview guide prior to dissemination
	Mindset	- Use similar wording in similar questions while only swapping out the relevant factor being tested
1.5 Intrusiveness	Reporting (self-report response)	- Ensure anonymity to ensure honest and correct answers from participants - On loaded questions, consider providing an introduction sentence to reduce perceived
	Sensitive question	- Questions on sensitive topics are not relevant for this project
1.6 Inconsistency	Case definition	- Not applicable
	Change of scale	- Use Likert scale or semantic differential consistently
	Change of wording	- Use similar or the same wording as Zibak & Simpson
	Diagnostic vogue	- Use definitions and ambiguous or contested terminology - Use same definitions and wording as Zibak & Simpson to ensure validity
2. Questionnaire design		
	Juxtaposed scale (questionnaire format)	- Avoid, use Likert scale or semantic differential consistently
	Left alignment and right alignment	- N/A as Likert scale is used
2.2 Questionnaire too long	No-saying and yes-saying	- Avoid no- or yes-saying bias by using both positive and negative statements about the same issue to break pattern
	Open question (open-ended question)	- Avoid open-ended questions, relevant inputs are covered by using in-depth interviews
	Response fatigue	- Minimize time required to complete survey - Avoid several questions covering same topic - If questions covering same topic is needed – ensure spacing between similar questions to avoid fatigue
2.3 Flawed questionnaire structure	Skipping question	- Test questions before dissemination
3. Administration of questionnaire and interviews		
3.1 Interviewer not objective	Interviewer	- Obtain interviewer training prior to conducting or disseminating interviews/questionnaire - Review this table prior to forming questionnaire and performing interviews
	Nonblinding	- Recommended to ensure interviewer is blind to study hypotheses (however, not an option as of now). - Review of Table 2 prior to forming questionnaire and performing interviews
3.2 Respondent’s subconscious reaction	End aversion (central tendency)	- Ensure anonymity to encourage truthful and honest answers - Awareness when interpreting data
	Positive satisfaction	- Avoid or rephrase questions where positive satisfaction may occur
3.3 Respondent’s conscious reaction	Faking bad (hello-goodbye effect)	- Providing information sheet on study to enable understanding and encouraging truthful and honest answers
	Faking god (social desirability, obsequiousness)	- Ensure anonymity of participants - Awareness when interpreting and analyzing data
	Unacceptable disease	N/A
	Unacceptable exposure	N/A
	Unacceptability	- No sensitive questions are included in questionnaire or survey - Ensure anonymity to enable truthful and honest answers
	Underlying cause	- Precise wording in questions
3.4 Respondent’s learning	Learning	- Consider spacing up “follow-on” questions based on previous answers
	Hypothesis guessing	- Avoid questions that may give participants bias on hypothesis (logical or actual) - Rearrange order on follow-on questions - Avoid leading questions
3.5 Respondent´s inaccurate recall	Primacy and recency	- Use Likert scale consistently
	Proxy respondent (surrogate data)	- Only include data from personnel adhering to qualifying criteria in
	Recall	- Only personnel currently within cyber security community is included in the survey
	Telescope	- Awareness when interpreting and analyzing data
3.6 Cultural differences	Cultural	- Only include participants from Norwegian cyber security community (ensured through question in the survey) - Awareness when comparing results from Norwegian vs. other nations

Table 4.6: Mapping of possible biases with countering efforts based on [74].

Results

In this chapter, the sample is first described through descriptive statistics. Then, the results following the questionnaire design is subsequently analyzed and integrated with the qualitative results. The four parts in this section are as follows[1]:

a) **Sample description** - descriptive statistics of the sample,
b) **CSIS in Norway** - containing basic information regarding the respondents' affiliation and organization's current engagement with CSIS and cyber security organizations,
c) **Perceptions on CSIS** - descriptive analysis of perceived benefits and challenges of CSIS in light of operational, organizational, economic and policy factors, and
d) **Attitudes toward CSIS** - measurement of engagement, perceived usefulness and willingness to engage in CSIS.

5.1 Sample description

This section describes the quantitative sample and its overall characteristics. As described in Section 4.4.2 Sample and population, all respondents with 1 year or less of working experience within cyber security was excluded to enhance the external validity of the study. This resulted in a somewhat altered distribution of the full and valid sample shown in Table 5.1. The qualitative sample is not described due to anonymization considerations. However, the qualitative was sampled in accordance with the sample variance principles. A detailed description of the qualitative sampling process was previously described in Section 4.5.1 Direction and planning.

Interestingly, respondents with less than 1 year of working experience within cyber security is evenly dispersed between both the full and valid sample. As a result, the dispersion in percentage does not change significantly.

As shown in Table 5.2 and Table 5.3, the distribution of respondents are evenly split between both top management and practitioner at roughly 25%, and roughly half of the sample are in middle management. The intended distribution was a

[1] The questionnaire parts and their link to the research questions are described in Section 4.4.1 Questionnaire design.

Which sector is your organization part of?
No exclusions

	Frequency	Percent
Public	45	39.1
Private	70	60.9

Which sector is your organization part of?
Sample excluding all respondents with
<1 year of cyber security experience

	Frequency	Percent
Public	43	39.4
Private	66	60.6

Table 5.1: Both the full and the valid quantitative sample, excluding all respondents with less than 1 year of working experience within cyber security. The full sample is included to briefly show who was excluded from the valid sample.

How many years of professional experience do you have in cyber security?

	Frequency	Percent
$<$ 2 years	12	11.0
2-5 years	19	17.4
$>$ 5 years	78	71.6

Table 5.2: The sample distribution with regards to the respondents' years of experience.

What is your role in your organization?

	Frequency	Percent
Top management	27	24.8
Middle management	53	48.6
Practitioner	29	26.6

Table 5.3: The sample distribution with regards to the respondents' role.

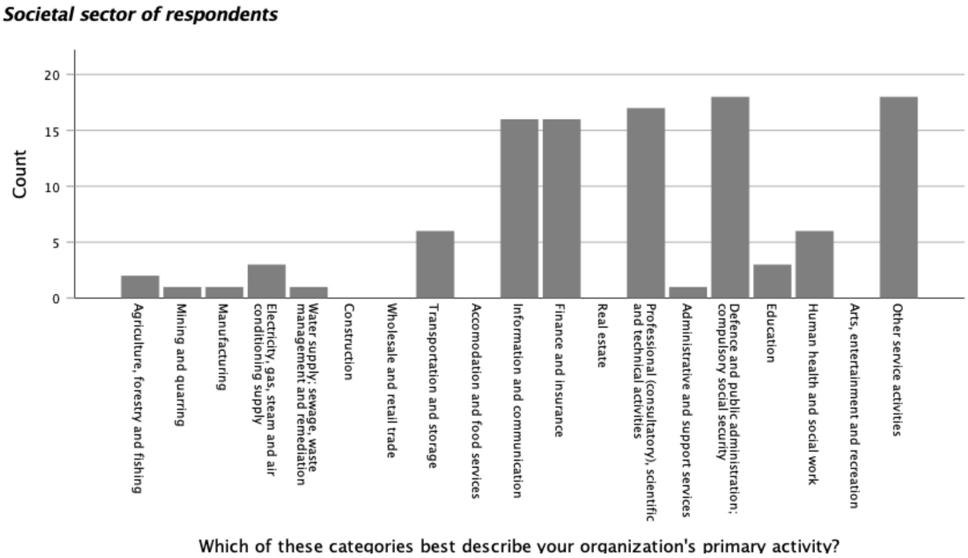

Figure 5.1: Bar chart depicting distribution of respondents per industry.

large percentage of practitioners, with descending numbers of middle and top management due to the logical hierarchical structure as described in Table 4.3. Thus, the findings may be skewed as the sample likely is not representative for the Norwegian cyber security community as a whole.

The vast majority, as many as 72%, of respondents were professionals with more than 5 years of cyber security experience, whereas respondents with less than two years, and between 2 to 5 years of cyber security experience constitute 11% and 17% respectively. Accordingly, as the number of respondents within the two groups of least experience in cyber security were significantly less than of those with more than 5 years of experience.

As Figure 5.2 shows, the distribution of high-experience respondents (>5 years) are significantly higher among top and middle management than that is seen among the practitioners, as expected prior to conducting the sampling.

Figure 5.1 shows that the majority of respondents identify as working within the following societal sectors;

1. Defence and public administration,
2. Professional (consultatory), scientific and technical activities,
3. Information and communication, and,
4. Finance and insurance.

Note that "*Other service activities*" are not included, as may include a variety of different sub-activities. Additionally, a noteworthy point is that there were no rep-

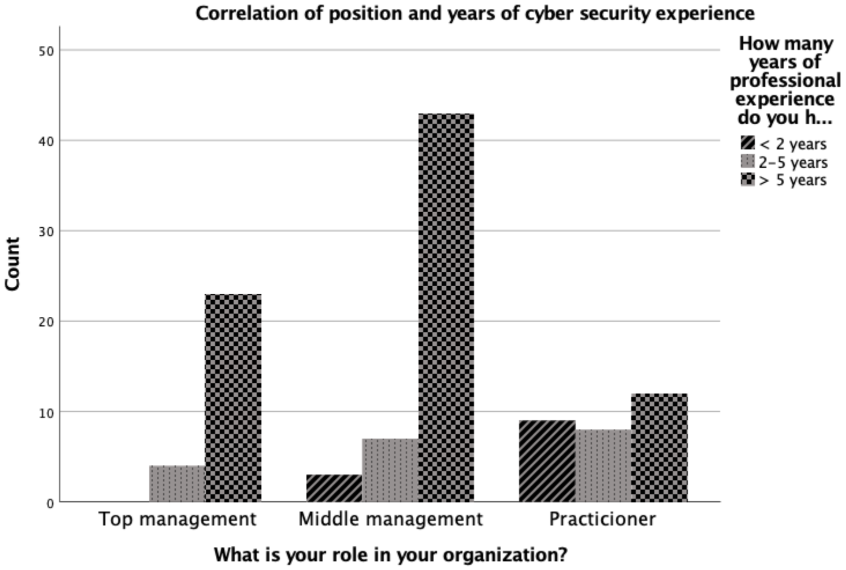

Figure 5.2: Correlation of respondents' role and years of experience within cyber security. Note that all respondents with <1 years of experience have been excluded from the sample.

resentatives within construction, wholesale and retail trade, real estate or arts, entertainment and recreation to the quantitative survey.

The percentages of employee distribution per industry versus respondent distribution is shown in Table 5.4. The distribution of employees in the Norwegian population was also previously depicted in Table 4.3 on page 62. This table shows that there are significant differences between the corresponding percentage distribution in Norwegian industries and in the sample. This may have been caused by several factors: the maturity and cyber security focus of the different sectors, the subordination and classification to Norwegian Fundamental National Functions (FNF) and hence subsequent legal requirements and a heightened focus on cyber security resulting in a higher number of relevant personnel within the industry. As described in Section 4.4.2 Sample and population, there are no official statistics depicting how many cyber security professionals that work in each sector. Norwegian official statistics has published reports detailing the number of personnel working in ICT, such as network architects, leaders of ICT units, network developers, network technicians etc.[2]. However, none of these parameters are exclusive to the professional combination of cyber security and ICT. Thus, the researchers were left with a much broader categorization than the targeted population.

As is shown in Table 5.5, 64% of the sample was during their questionnaire

[2] Statistics by Statistics Norway, accessible from https://www.ssb.no/statbank/table/12542/

Which of these categories best describe your organization's primary activity?			
	Frequency	% of sample	% of pop
Agriculture, forestry and fishing	2	1.8	2.3
Mining and quarring	1	0.9	2.1
Manufacturing	1	0.9	7.6
Electricity, gas, steam and air conditioning supply	3	2.8	0.6
Water supply; sewage, waste management and remediation	1	0.9	0.6
Construction	0	0.0	8.6
Wholesale and retail trade	0	0.0	12.7
Transportation and storage	6	5.5	4.7
Accommodation and food services	0	0.0	3.4
Information and communication	16	14.7	3.9
Finance and insurance	16	14.7	1.7
Real estate	0	0.0	1.0
Professional (consultatory), scientific and technical activities	17	15.6	5.6
Administrative and support services	1	0.9	4.9
Defence and public administration; compulsory social security	18	16.5	6.3
Education	3	2.8	8.3
Human health and social work	6	5.5	20.8
Arts, entertainment and recreation	0	0.0	2.1
Other service activities	18	16.5	2.7

Table 5.4: Distribution of employees per industry in 2021, Norway [99] (population) compared to respondents per industry (sample).

Cross-tabulation of role and employment in Cyber Sec Org

Role		Top management	Middle management	Practicioner	Total
Do you work in a cyber security organization?	Yes	17	31	22	70
	No	10	22	7	39
Total		27	53	29	109

Table 5.5: Crosstabulation of respondents' roles and cyber security organization affiliation.

response employed in a cyber security organization[3]. Regardless of affiliation to a cyber security organization, middle managers were the most numerous hierarchical categorization, with the amount of top managers were smaller, but similar at approximately 25%. With regards to practitioners however, the percentages differed significantly. When examining respondents which worked in cyber security organizations, 31% of the respondents characterized themselves as practitioners, whereas only 17% of those not employed in cyber security organizations did the same.

5.2 Analysis and integration

5.2.1 CSIS in Norway

This section describes the quantitative and qualitative results on the participants' relationship to CSIS, and (where applicable) why they chose to participate in CSIS. The resulting analysis is later correlated against theoretical findings of Section 3.4 The Norwegian cyber security landscape in Section 6.1 The state of CSIS in Norway to compare theory and practice on how CSIS is performed in Norway, including:

1. the extent of participation in CSIS among the participants,
2. which entities the participants shared Cyber Security Information (CSI) with, and
3. what incentivized undertakings to share CSI.

Figure 5.3 depicts the distribution of respondents participating in CSIS when the questionnaire was submitted. Note that later in this section, the number of respondents answering non-participatory in their engagement in CSIS varies, and thus is assessed as invalid. However, the graph shows that almost all respondents in some way participates in CSIS. Over 90% of respondents in the public sector answered that their organization was currently involved in CSIS, while 85% of those in the private sector did the same[4]. The qualitative data also depicted a

[3] Previously defined in Section 3.4.2 Cyber security organizations and SRE as CERT, ISAC, CSIRT, SOC, etc.).

[4] Note that the statistics in Figure 5.3 depicts the percentages against the total sample, whereas

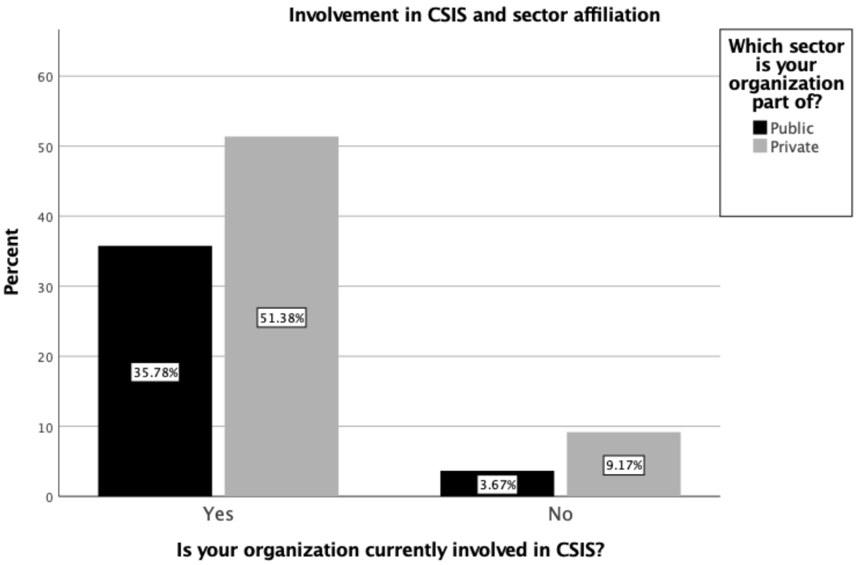

Figure 5.3: Distribution of respondents engagement in CSIS and sector affiliation.

strong support of CSIS in general: "Within the cyber security community, you are completely dependent on being connected to the flow of information, everyone in the cyber security community is. It's a natural part of doing cyber security since you work against the same threats". Another informant elaborated: "In this line of work there are few enough resources as it is, which means that information sharing means that more people can be involved in handling matters across areas of responsibility. It makes you better at maintaining your own security and which other benefit from". This matter is further nuanced through analysis of both qualitative and quantitative data later in this chapter.

the statistics referenced to in the text refer to percentages within the public or private sub-sample.

Which internal factor led to your organization's engagement in CSIS?

	Frequency	Percent
Access to government agencies	21	19.3
Access to other companies and their cyber security information	33	30.3
Access to external expertise and knowledge	19	17.4
Access to professional networks	14	12.8
Unknown	6	5.5
My organization does not share cyber security information	6	5.5
Other reasons not covered above	10	9.2
Total	109	100.0

Which external factor led to your organization's engagement in CSIS?

	Frequency	Percent
Geopolitical context and security situation	24	22.0
Own or similar organizations targeted by cyber criminals	36	33.0
Requirements from superior organizations, laws or regulations	16	14.7
Unknown	7	6.4
My organization does not share cyber security information	5	4.6
Other reasons not covered above	21	19.3

Table 5.6: Depiction of the internal and external factors which lead to involvement in CSIS.

By examining Table 5.6, over 30% of the respondents answered that gaining access to other companies and their CSI was the most important factor leading to their organization's involvement in CSIS. The second most answered alternative was access to government agencies, accounting for 19% of all respondents. Following access to government agencies, access to external expertise and knowledge and professional networks was stated as the third most important factor by 17% and 13% of the respondents respectively.

As for external factors, 33% of the respondents answered that cyber attacks on their own or similar undertakings was the main external factor leading to their organization's involvement in CSIS. 22% answered that the geopolitical context and security situation was the leading factor, while 15% answered that requirements from superior organizations, laws or regulations was the main factor. 19% of the respondents responded that there were other factors than those stated that led their organizations to pursue CSIS - indicating a reduced validity of this question as the results may be skewed due to inadequate provided answer options.

Another validity issue is apparent when examining the number of respondents choosing "*My organization does not share cyber security information*". In the question regarding internal factors, six respondents opted that their organization does not participate in CSIS, while five responded the same to the question regarding external factors.

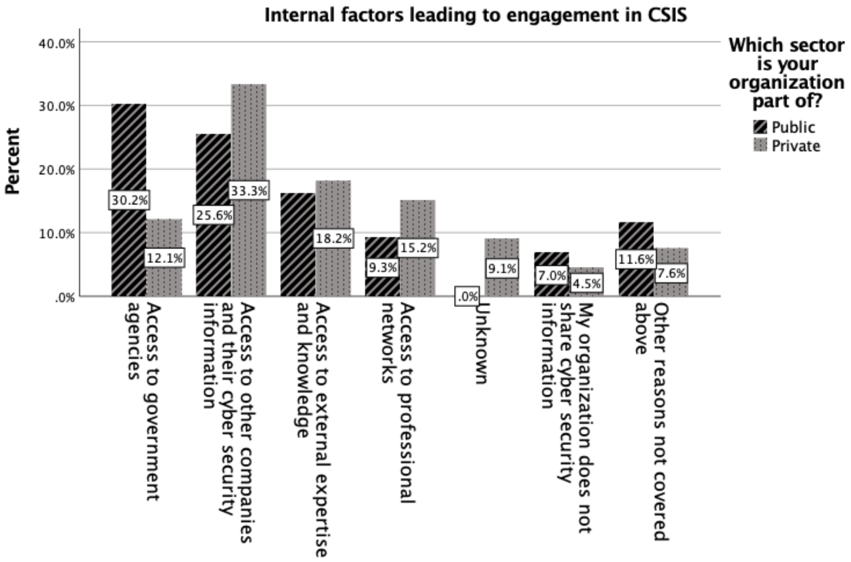

Figure 5.4: Bar chart depicting which internal factors lead to their organizations' engagement in CSIS, clustered by the correlating sector.

By examining Figure 5.4, cyber security personnel within the public and private sector displayed distinct differences in why their organization engaged in CSIS. While 30% of the respondents in public sector stated *Access to government agencies* as the dominant reason for their organization's engagement in CSIS, only 12% of the private respondents chose the same. A lessened, but similar difference can be seen in the most prevalent answer within the private sector - *Access to other companies and their cyber security information*. One third (33%) of the private respondents stated this answer, whereas 26% of public sector respondents answered the same.

Accordingly, the perceived value of access to government agencies (e.g. national services) was significantly more predominant among public organizations than private, whereas private organizations ranked access to other companies' CSI as more important. One private middle manager underlined this finding by stating: "The classified briefings are so watered-down they lose almost all value. I can go to any other private actor and get better information". However, a private top leader noted that leaning on assessments made by national services has distinct advantages: "It is important to understand the incident, but more important to un-

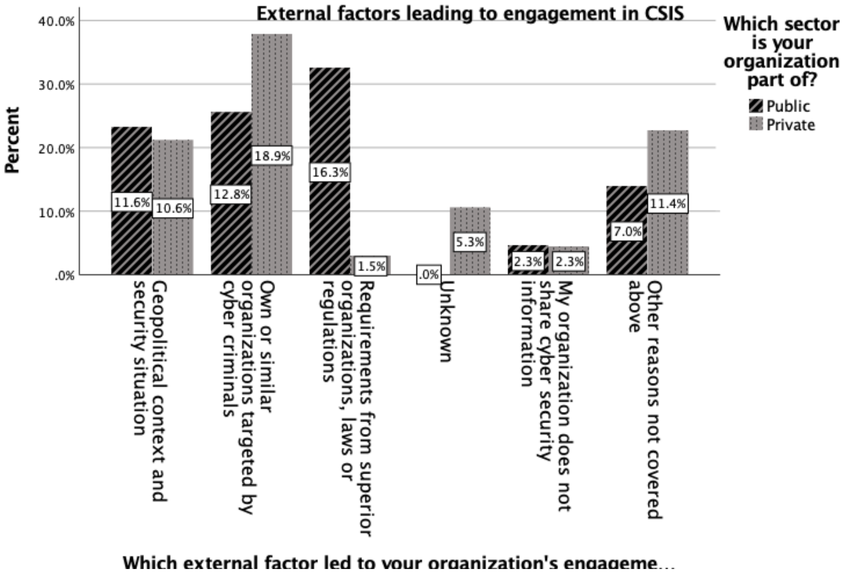

Figure 5.5: Bar chart depicting which external factors lead to their organizations' engagement in CSIS, clustered by the correlating sector.

derstand the threat dimension, what we need to protect ourself from, why we need to protect us and the threat actors' maturity level[...]. In [national service], Russia is discussed in a completely different way, and it helped alot when [representative] discussed this with our senior management, and it gave us greater authority". Several other informants from both public and private sector also acknowledged the utility and value of unclassified annual assessments from the national services.

The most distinct difference between why public and private organizations engaged in CSIS may be seen in Figure 5.5, where 33% of respondents in the public sector chose the leading external factor for engagement in CSIS as *Requirements from superior organization, laws or regulations*, with a corresponding 3% of respondents in the private sector. This finding was expected as more public undertakings than private counterparts in general were subject to the Security Act or other legislature. The qualitative findings also supported the quantitative ones related to the private dependency and preference for access to other companies CSI. When asked why they participated in CSIS, one middle manager for a cyber security organization stated that "As a private actor, you are not required to do anything, but it's added business". He also elaborated on a possible causal relationship: "our customers are primarily interested in what hits our other customers - *is that something that will affect me as well?*".

Another informant from a private undertaking subjected to the Security Act elaborated on the benefits of horizontal cooperation with similar enterprises versus vertical dependency on national services: "We only get very general guidance

To whom does your organization share cyber security information with?		
	Frequency	Percent
Cyber security organizations (e.g. ISAC, CERT, CSIRT, SOC, etc.)	81	74.3
National services (e.g. NSM/NCSC, PST, NC3, FCKS, etc.)	86	78.9
Horizontally (to organizations similar to your own)	74	67.9
Top-down (from cyber security organizations or national services to subordinated organizations)	38	34.9
My organization does not share cyber security information	7	6.4

Table 5.7: Table showing which entity types the respondents' organization's share CSI with. Note that the question allowed for multiple answers per respondent.

from [national service], it's very little specifics, which we criticize them for. [...] I still understand them, with likely a thousand undertakings knocking on their door, asking *well, what about us?* [...] [Similar organization] is completely different. They see huge value in working together". When asked about whether the two enterprises regard themselves as competitors as they competed in the same market, the informant responded that they were: "Partners. We help each other in all security aspects. [...] And they are way bigger than us, so the fact that they want to help us - they should be commended for that". Even though the informant found it hard to establish new partnerships with other undertakings, he noted: "those similar to ourself are interested in the same things as us, so it's easier".

An informant - a top leader of a newly established cyber security entity in a major undertaking in its sector - stated: "Information sharing - you can never have enough. But it's important to get qualitative data that is representative for the industry you're in". Ergo, the sampled data showed a clear preference for sharing information with those similar to themselves or others whose information sharing give a direct positive effect.

Table 5.7 depicts whom the respondents' organizations engage in CSIS with. The three most frequent responses was sharing with national services (79%), cyber security organizations (74%) and to organizations similar to their own (70%). The informants' preference toward horizontal sharing is stated above, while almost all interview subjects stated a highly positive attitude toward sharing information with the national services, despite the same informants critiquing governmental challenges related to over-sanitization, timeliness and over-classification. In general, the qualitative analysis are identical to that of the quantitative. A more detailed view on perceptions toward CSIS is explored in Section 5.2.2 Perceptions on CSIS.

Does your organization pay for membership in any cyber security organizations?

	Frequency	Percent
Yes	64	58.7
No	26	23.9
Unknown	19	17.4
Total	109	100.0

Table 5.8: Distribution of respondents whose organization pay for CSIS membership

If your organization is not participating in any cyber security organizations, state the most relevant reason why

	Frequency	Percent
My organization is a member of a cyber security information sharing organization	41	37.6
Cost of membership	1	0.9
Lack of information quality, utility or value	2	1.8
Inability or lack of resources to manage additional information processing	4	3.7
My organization participates in cyber security organizations	37	33.9
Other reason	24	22.0

Table 5.9: Reasons why the respondents' organizations chose not to participate in CSIS

As is seen in Table 5.9, the most relevant reason (excluding "other reasons") for not participating in CSIS, was an inability or a lack of resources to manage additional information processing to that is acquired organically within the organization. Some respondents also answered cost of membership and lack of information quality, utility or value. However, as "other reason" was the most frequent answer of those who not already participating in CSIS, this indicates that the available options were not sufficiently applicable for the sample.

Another factor which supports this indication is the variance observed between the questions related to a lack of involvement in CSIS. In Table 5.6, five and six respondents (approximately 5% and 7% of the sample) respectively chose the option indicating a lack of involvement in CSIS. The sample variance of those stating they *do not participate in CSIS* in Table 5.9 and 5.6, calculated by using

$$s^2 = \frac{\sum(x_i - \bar{x})^2}{n-1}$$

is measured as a highly significant 5.33, resulting in a sample standard deviation of 2.31 through

$$s^2 = \sqrt{\frac{\sum(x_i - \bar{x})^2}{n-1}}$$

Ergo, the statistical findings of Table 5.9 were thrown out and not included in the following Section 5.2.2 Testing inference between statements and respondents' background.

Perceptions on the role of NSA, NCSC and the SRE model

Positive attitudes toward the SRM model One topic not covered by the questionnaire but extensively brought up by the informants, was reflections on how the informants perceived being subjugated to the Security Act. One informant in an organization not currently subject to the Security Act, stated that he saw the main advantage in having access to classified information, even though they still could not share classified information with the consumers of their cyber security assessments, as they generally lacked security clearances: "I see the main advantage of being able to take part in how to declassify information and what to declassify - and [being subjugated to the Security Act] enables us to take part in that discussion. That we're able to get our hands on more information to understand why it's relevant for the consumers. I think that's the main advantage of the Sector Response Entities (SRE) - that you get security clearances. Everything depends on how it's done in practice, but I truly believe in the SRE model. [...] You wouldn't have the same degree of sharing and available information if you structured it in any other way". However, almost all informants in undertakings already subjected to the Security Act and with security clearances, did not perceive that it led to greater access to information. This challenge is further described in

Section 5.2.2 Policy.

Informants in sectors where a formal SRE existed were highly positive of having this coordinating entity, whereas informants in sectors lacking a SRE underlined the need for one. In those sectors lacking a formal SRE, two intermediate solutions were present: either leading organizations took the responsibility upon themselves, or separate SRE equivalents were created by the sector community. The main responsibility for SREs or SRE equivalents were to collate, process and issue sector-specific assessments to aid subordinate undertakings in enhancing their security posture. Additionally, some SREs also aided subordinated undertakings in breach detection and recovery. The coordination and cooperation between SREs were also perceived as good, in which one informant stated that cross-sectoral meetings were conducted weekly between practitioners of the different SREs.

One major disadvantage of the SRE equivalents was lack of access to Norwegian National Cyber Security Centre (NCSC): "We get all publicly available information that NCSC disseminates, but for now we don't get any more than TLP:GREEN [second lowest TLP label, as described in Section 3.3.4 Traffic Light Protocol] as we are not an SRE". Even though SRE equivalents did not have access to NCSC, informants from SREs described cooperation with these entities as well-functioning and fruitful, and often had bilateral or multi-lateral cooperation with them.

Ratification of the Security Act and guidance from NSA Even though the informants were generally positive toward the idea of the Security Act and the SRE model, most perceived that the current scheme was sub-optimal compared to the intent of the Security Act and the creation of NCSC. "When you're subjected to the Security Act and have a security clearance, it's just a matter of authorizing us for what we're going to talk about. It's a strange approach on the part of the authorities. With the new Security Act, I think that the understanding of it, the scope and how it actually works has been extremely low. We've put alot of effort in this at [informant's undertaking], which has not been done in other sectors. It's very worrying that [. . .] there are so many people who are afraid of it. But it's nothing to be afraid of - it's functional, cost-benefit-based, but you have to sit down and assess what to protect and how it should be implemented. If everyone's not on the same page, you're limited in all aspects. [. . .] The Security Act is very important, and with the new revision we've received great follow-up from our sector ministry. But there is an issue when you're looking at others and wonders *why aren't they subjected, they have a huge responsibility* [for FNFs and critical infrastructure]. But the subjugation is a ministerial responsibility, which currently is severely lacking and excuses are constantly being made".

The latter perception was supported by another informant with intimate knowledge on the classification and identification process of critical functions. This informant presented his experiences with central challenges on how the process was being supervised from both the National Security Authority (NSA) and the responsible ministries: "I've been a part of [the FNF mapping process] [. . .], I know how it's done in other sectors, and I experience two challenges: The ministries interpret it very differently. If it was an intention to harmonize between sectors, as I perceive it has been, corresponding assets should have been defined as critical. What's critical is critical, regardless of which sector you're in. There's a different understanding of criticality between the sectors. [. . .] It's up to each individual ministry to assess the criticality in a national perspective, which is done very differently from one sector to the other. [. . .] The competency of the ministries is also very different. Some ministries have been working with this over a long time and has supposedly established a relatively good level of competency, while other ministries have no competency in this what so ever. And yet, they are the ones stating requirements for the sector and formally make decisions". As of how to improve the experienced challenges, the informant proposed that: "This could've been solved with a more centralized management guiding [the ministries] in how to do it".

Perceptions on trust in NSA's prioritization of effort Even though some informants perceived the support they received as satisfactory or good, most felt they were not prioritized by the NSA and NCSC: "I wouldn't say we have any cooperation based on how I define the term. [. . .] There are without doubt some prioritized sectors. [Informant's sector] does not have as high of a priority as [sectors with a high degree of critical infrastructure]. I think it's associated with there's alot more going on in [sector with a high degree of critical infrastructure] than in [informant's sector]. I think we're mainly affected by cyber criminals, while the really serious cases happens in [aforementioned sectors]. [. . .] We've tried to send requests for information[5] without getting replies. Especially from [a certain national service]. I'm not surprised, but it serves as an example of the problem. Our worries are simply not prioritized".

Some informants supported this apparent prioritization of certain sectors and individual undertakings: "In terms of national security and those actors supporting it, you have to differentiate sectors and say that some sectors get more than others, and that it isn't equal treatment for each sector". However, none of the informants stated that they knew how this prioritization was made and questioned whether the government had assessed their organizations' criticality correctly: "We aren't the single most important element of Norway A/S, but everyone is a piece of the puzzle". When asked on his perceptions of the national services' willingness to assist them specifically, the informant further explained: "Even though we invite [the national services] to us to elaborate on their unclassified assessments, [. . .] it's hard to get a straight answer. [. . .] [National service] say they may be able

[5] Also known as RFI, a common type of request format when asking for specific information. The RFI format is extensively used by armed forces and among national services.

allocate on hour per year. May be? We supply [vital part of FNF], that's pretty important. And they respond with *if you don't hear anything from us, everything i A-OK*. I'm not very happy with that reporting technique".

The apparent prioritization of some undertakings had a disincentivizing effect on some informants in supporting NCSC: "We're feeling that NCSC is on their heels when it comes to us. [. . .] We know that being subjected to the Security Act is followed by alot of expenses. And having alot of expenses without prior guidance is an awkward situation to be in. [. . .] However, we're also thinking of joining the NCSC. We are currently not an affiliate, because then we would have to be included in the National Warning System for Digital Infrastructure (WSDI). If joining the WSDI gives them [NCSC] greater access to information, but doesn't give us guidance and support in incident management, then we feel that we give information but get nothing in return. We also don't receive support with regards to threat assessments - I've always wondered when [national service] is going to brief us about an increased threat against [informant's sector]. [. . .] When are we going to use our secret security clearance? [. . .] As of now, it's more about giving NCSC an even bigger network and exhausting our resources which we could've used to strengthen ourself first. Therefore, we are more restrictive in joining the partnership before we've become more robust internally".

Even though some informants were negative toward participating in the WSDI network, the majority was positive but regarded it as a supplementary detection measure and primarily in enhancing NCSCs access to information. When asked if participation in the WSDI was mandatory for undertakings subjected to the Security Act, an informant responded: "I don't think so, but its smart to be in it. However, if you think being part of WSDI makes you secure, you are mistaken. You should have some security measures on your own behalf as well. WSDI is sensible to have, as if you're compromised, then NCSC is quicker to respond".

Perceived reluctance of national services in sharing classified information
Previously in this section, both benefits and shortcomings of the practical implementation of cyber security in relation to the Security Act and the SRE model has been presented. All but some informants had NCSC as their only point of contact with the national services. However, several informants with access to classified information systems and information also critiqued the national services for not sharing all relevant information they possessed, which could have been used to enabled a more resilient cyber security posture on a national level. As previously discussed in this chapter, several informants were of the impression that they did not receive information in the extent in which it could be shared with them, even if they possessed the necessary formalities (e.g. both security clearance and an evident need to know). According to their perceptions, information existing in the Norwegian Joint Cyber Coordination Centre (JCCC) (which was presented in Section 3.4.1 National services) were to some degree kept from eligible recipi-

ents with the necessary formalities: "Often, there's information that could've been shared with us but isn't, because it has become a matter for the national services. So then JCCC has become a collective for the lucky members. We know there's information that is shared in that arena which would've been beneficial for us, but which is not shared with us. And it has nothing to do with classification considerations [as the informant was had a valid and extensive security clearance]. This topic is further discussed in Section 5.2.2 Policy.

Others also critiqued the role of NSA as the apparent point of contact to the national services: "We uncovered a vulnerability so significant and uncomfortable that we knew we had to spend a lot of time with it. We shared that we had this vulnerability and that we needed to understand the threat actor [working against the undertaking]. The bear thinks long-term - so what do they [the national services] know about it, what can they say, how can they share information on that which possibly is or could be a serious incident? Who could we talk to? While [national service] were very professional, [. . .] NSA was not so much. Because NSA wanted to be the focal point for everything". The same informant also stated that the assistance they were offered was highly technical: "We had internal capacity and [security measure] from the supplier - we didn't need technical and analytical assistance. What we needed was the other dimension: how serious is this now, in six months, in 15 months? What risk does the executive committee run? [. . .] A top leader in [undertaking] can't talk with the people *down there*, he has to talk with someone on his level".

Perceived discrepancy on the role of NSA and NCSC The last issue regarding some informants' perceived discrepancy between NSAs and the NCSCs role as a strategic entity in ensuring the national security was further exemplified: "What exactly is the NCSC and who are they for? The leader of [a private interest group] said: *Why should I pay 70.000 NOK to have a place in that room? I don't meet with anyone who has my knowledge!* When [said leader] was there, he met a variety of personell types, like technical personnel, lawyers, etc. Why should you pay for a seat there, but meet people who have completely different expectations than you? You can have several different arenas, but you [NSA] have to state that *if you are going to have a place in this room, it is intended for this type of personnel*. NSA must decide that they have a national responsibility, and speak from the authorities' point of view. [. . .] They have to be clear on who they're here for, because they [NSA] have a limited amount of personnel and a certain budget".

Summary of CSIS in Norway To summarize, the informants perceived both positive and negative aspects of being subjected to the Security Act. While subjugation results in at least some relevant personnel within the given undertaking receiving a security clearance, informants with a security clearance stated that they rarely had use of it. This was mainly due to a perceived reluctance of NCSC in sharing classified information[6]. Additionally, several informants raised concerns on the classification process of critical assets and FNFs, in addition to a perceived lack of prioritizing *their* undertaking. One informant with intimate knowledge of the classification and FNF identification process stated a lack of harmonization between ministries and insufficient competency in the individual ministries. The sense of not being prioritized even led to some informants restricting the cooperation with NCSC in favor of focusing their cyber security resources on strengthening themselves.

Additionally, several informants stated that they perceived NCSC as reluctant in sharing classified CSI with them, even though they had the necessary formalities and knew the information existed. NSA and NCSC were also critiqued for not being clear in their task and purpose - resulting in a loss of confidence and perceived relevance for informants in higher management echelons in particular, as well as a perceived intention to be the focal coordinating entity toward the national services, even in matters in which they were not suited to be so - by both undertakings and among informants from other national services.

5.2.2 Perceptions on CSIS

This section contains the analysis and integration of both quantitative and qualitative findings regarding the participants' perceptions on CSIS. As the findings were extensive, the page numbers are stated for each subsection:

a) general considerations made from the initial analysis of the quantitative and qualitative data (page 122),
b) statistical inference testing measuring the inference between the statement categories and the respondents' background (page 121),
c) the respondents' perceptions toward benefits and challenges given by their median and interquartile range (page 123), and
d) perceptions toward benefits and challenges within the different categories of CSIS (from page 123).

Perceptions on CSIS were measured by asking respondents within the Norwegian cyber security community to agree or disagree with 26 statements about CSIS derived from the literature, mainly based on the research of Zibak & Simpson [13]. The full set of statements along with the median and interquartile range (IQR) of each item are listed in Table 5.12.

The next section covers the statistical inference testing conducted in order to measure whether there were any inference or correlations between the respondents' backgrounds and their attitudes toward the categories.

[6] This topic is further elaborated on in Section 5.2.2 Policy.

Tests of Normality

	Kolmogorov-Smirnova			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Organizational	0,134	109	0,000	0,937	109	0,000
Operational	0,131	109	0,000	0,963	109	0,004

Table 5.10: Tests of Normality for the composite variables (e.g. scales) operational and organizational. Note that policy and economy was excluded due to them failing the reliability test.

Testing inference between statements and respondents' background

Before testing for inference, a reliability test for each Likert scale (e.g. categories according to Table 5.12) was conducted. Only the Likert scales constituencies *operational* and *organizational* achieved a Cronbach's alpha coefficient of above 0.7, with alterations. Two statements from the organizational category and one statement from the operational category had to be discarded from further analysis due to low total correlation coefficient. Both *policy* and *economic* scales did not achieve a sufficient Cronbach's alpha and were excluded from further inference testing.

Then, the scales were tested for normality by calculating the p value using the Shapiro-Wilk test for normality. Even though normality testing is not necessary for Likert scales, several parametric statistics such as t tests, Pearson's Product-Moment Correlation and the Kruskal-Wallis one-way analysis of variance, require normal distribution for internal validity. As Table 5.10 shows, the p values of both scales were well below 0.5, indicating that the samples were not normally distributed. Ergo, the non-parametric independent samples Mann-Whitney test was used to test for inference.

As previously stated, the main goal of inference testing was measuring whether there were any inference or correlations between the respondents' backgrounds and their attitudes toward the categories stated in Table 5.12. Thus, the Mann-Whitney test was conducted on the categories which passed the Cronbach's alpha delimiter. As all categories had similar shapes in the response distributions, the median was used to test inference. To test the experience and role against the organizational and operational categories, the responses had to be transformed into binary nominal variables:

- *Experience* previously had three responses: $<$ 2 years, 2-5 years, and $>$ 5 years. The transformed responses used in the Mann-Whitney test was ($<$ 2)-5 years and $>$ 5 years of experience in cyber security.
- *Role* originally also had three responses: Top management, middle management and practitioner. The transformed responses used in the Mann-Whitney test was management (including both top and middle-) and practitioner.

Mann-Whitney test for inference

	Sector		Experience		Role	
	Operational	Organizational	Operational	Organizational	Operational	Organizational
Total N	109	109	109	109	109	109
Mann-Whitney U	1453	1242	1199.5	1318	1240	1005
Wilcoxon W	3664	3453	4280,500	4399	1675	1440
Test Statistic	1453	1242	1199.5	1318	1240	1005
Standard Error	146.483	157.751	135.210	145.611	132.442	142.629
Standard Test Statistic	0.232	-1.122	-0.070	0.749	0.604	-1.087
Asymptotic Sig.(2-sided)	0.816	0.262	0.944	0.454	0.546	0.277

Table 5.11: Mann-Whitney test for inference against operational and organizational categories (note that Policy and Economy has been excluded due to insufficient Cronbach's alpha coefficient). Neither respondents' role, experience or sector had a statistical significance on their perceptions to the Likert scales.

As shown by looking at the *p* values in Table 5.11, neither the respondents' role, experience or sector had a statistically significant impact on their responses within the *operational* and *organizational* CSIS categories. Despite this, at Likert item level, differences in perceptions due to the respondent's role, experience or sector were more significant - which is further described in the following sections.

Overview of agreement with statements

The respondents generally agreed with each other, and were extreme in their perceptions as both the medians were polarized, and the interquartile ranges were low in general, indicating less spread and divergences in their perceptions. The statements with which the most respondents concurrently agreed upon (i.e. highest median score with the lowest interquartile range), were:

- St1: *CSIS contributes to enhancing the national security posture and situational awareness*,
- St2: *CSIS contributes to enhancing the organizations' security posture and situational awareness*,
- St9: *CSIS enhances defensive agility and resilience*, and
- St13: *CSIS strengthens the relationship with government agencies*.

However, several challenges which may significantly hamper effective CSIS were also highlighted. The most agreed-upon existing challenges were a shortage of qualified CSIS analysts, and challenges with interoperability and automation to utilize received CSI.

In the following subsections, findings from the quantitative analysis are described in detail and integrated with the qualitative findings from the in-depth interviews. The following analysis is structured according to the categories in the following order: Operational on page 123, Organizational on page 126, Economic on page 130, and lastly, Policy on page 132.

Statement	Category	Dimension	Median (IQR)
(St1) CSIS contributes to enhancing the national security posture and situational awareness	Operational	Benefit	6 (1)
(St2) CSIS contributes to enhancing organizations' security posture and situational awareness	Operational	Benefit	6 (1)
(St3) Threat actors are deterred by CSIS among organizations	Operational	Benefit	4 (3)
(St4) CSIS supports incident response efforts	Operational	Benefit	6 (2)
(St5) CSIS contributes to breach detection and recovery	Operational	Benefit	6 (2)
(St6) CSIS reduces duplicate information handling [...]	Operational	Benefit	5 (2)
(St7) CSIS strengthens and expands professional networks	Organizational	Benefit	6 (2)
(St8) CSIS validates and complements other sources of information	Organizational	Benefit	6 (2)
(St9) CSIS enhances defensive agility and resilience	Organizational	Benefit	6 (1)
(St10) CSIS helps in combating cyber security skills shortage	Organizational	Benefit	5 (3)
(St11) CSIS reduces overall cyber security costs	Economic	Benefit	4 (2)
(St12) CSIS supports security investment decisions	Economic	Benefit	5 (2)
(St13) CSIS strengthens the relationship with government agencies	Policy	Benefit	6 (1)
(St14) Standardization issues hinder CSIS	Operational	Challenge	4 (2)
(St15) Inconsistent definitions and terminology undermine efficient CSIS	Operational	Challenge	5 (2)
(St16) It is difficult to determine the accuracy and quality of received cyber security information	Operational	Challenge	5 (2)
(St17) It is difficult to ensure the timeliness of shared cyber security information	Operational	Challenge	5 (2)
(St18) The interoperability and automation of CSIS are difficult to achieve	Operational	Challenge	5 (1)
(St19) CSIS results in redundant and irrelevant data	Operational	Challenge	3 (2)
(St20) There is a shortage of analysts with skills required to handle shared cyber security information	Organizational	Challenge	6 (2)
(St21) It is difficult to trust the other participants in CSIS efforts	Organizational	Challenge	3 (2)
(St22) Setting up the CSIS infrastructure is expensive and drains resources	Economic	Challenge	4 (2)
(St23) CSIS reduces clients' confidence in the organization that shares information with others	Economic	Challenge	2 (2)
(St24) Government over-classification undermine effective CSIS	Policy	Challenge	5 (3)
(St25) Privacy and antitrust legal concerns hinder CSIS	Policy	Challenge	5 (2)
(St26) Inconsistent legal frameworks undermine CSIS	Policy	Challenge	4 (2)

Table 5.12: Questionnaire items and their corresponding median and interquartile range (IQR) scores, where 7 = strongly agree; 1 = strongly disagree.

Operational

Figure 5.6 depicts to what extent the respondents agreed to the operational benefits and challenges proposed by the theoretical literature.

Impact of CSIS on national and individual organizations' security posture At the operational level, the respondents acknowledge the positive role of CSIS in improving both individual organization's security posture and situational awareness, and national security posture and situational awareness. Improved security and situational awareness in individual organizations and at the national level were rated approximately even by the respondents, where a total of 84% either agreed or strongly agreed to improvements at the organizational level, and 81% at the national level. However, when only considering responses which agreed or strongly agreed, respondents within the public sector (87%) were more positive than respondents within the private sector (77%) to that CSIS contributes to enhance national security posture and situational awareness. Top managers, when compared to both middle managers and practitioners, were generally less positive about the enhanced national security posture and situational awareness due to CSIS. Despite this, less difference between the roles was found considering the security posture and situational awareness in individual organizations.

Even though respondents from both public and private sector agreed that CSIS improved both the individual organizations' and the national security posture and situational awareness, the findings indicate that personnel in the public sector is somewhat more inclined to share CSI with national services and the authorities. Almost all interview subjects stated that they were very inclined in sharing infor-

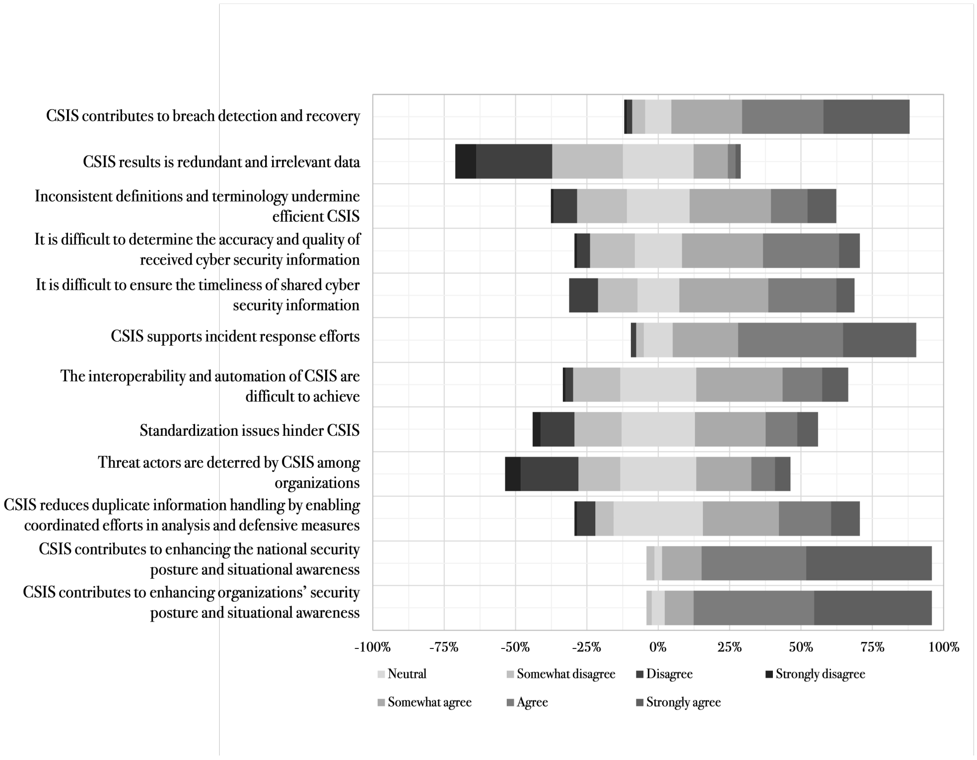

Figure 5.6: Respondents' attitudes on benefits and barriers in CSIS - Operational category.

mation with national services, including those subjects which extensively critiqued the frequency and usefulness of the information they got in return. The reasons why were, however, varied. Some stated they were required to do so through the Security Act, while most saw an independent value in contributing to "the greater good", both in regard to information sharing toward national services or even competitors. A senior middle manager stated that "nobody wants to see [critical entity] being subject to a ransomware-attack, it would be disastrous".

Impact of CSIS on defense, detection, response and recovery efforts By looking at Table 5.12, it is seen that respondents expressed a high level of agreement with the ideas that CSIS supports incident response efforts, contributes to breach detection and recovery, and enhances defensive agility and resilience. A total of 85% of the respondents agreed to some extent that CSIS has a positive effect on the above-mentioned operational factors.

55% of the participating cyber security professionals from both public and private sector also agreed that CSIS reduces duplicated information handling by coordinating analysis efforts and defensive measures.

Quality of shared cyber security information Almost 60% of the respondents disproved that CSIS results in redundant and irrelevant data, with 34% either disagreeing or strongly disagreeing, whereas 25% somewhat disagreed with the statement. This does however not automatically mean that CSIS provides unique and relevant data. Even though the participants had more positive attitudes toward the relevance of shared CSI than the theoretical literature proposed, a total of 62% expressed to some extent that determining the accuracy and quality, and ensuring timeliness of shared information are difficult. Interestingly, a greater part of the top managers (81%) compared to middle managers (57%) and practitioners (55%) expressed that it is difficult to assess the accuracy and quality of shared data. The top managers also expressed a stronger agreement to the difficulty of ensuring timeliness when sharing CSI than the other groups. Despite this, nearly 70% confirmed that CSIS both validates and complements other sources of information, indicating that organizations engaged in CSIS receive relevant information from others.

The quantitative findings were supported by those acquired through in-depth interviews. Several informants stated that data and alerts & triggers for action had to be detailed and actionable for them to have value. Both governmental and private companies have either specialized dissemination units or offers Cyber Security As A Service (CSaaS), whereas both are simultaneously contested and acclaimed: "[...] extensive sharing is nice, but makes it hard to distinguish what's important. You can apply technical filters, but you still need to verify and assess the source etc. This is both time-consuming and challenging - a regime for source evaluation is needed, but there are no working automatic solutions at this time.

How useful is all this focus on sharing if you need to use crazy amounts of time and resources on evaluating the information in order to use it? [...] There are way too many useless IOCs being disseminated".

Another subject also exclaimed extensive challenges with regards to timeliness, especially on information originating from national services: "it can take not only hours, but weeks, and I even have some examples where months have gone by before the information reaches us. This is partly due to how the information flow is structured with NCSC and Sector Response Entities. [...] This leads to the creation of various alternate avenues of information instead of restructuring the current scheme of reporting in order to ensure that the information which is relevant to us, actually reaches out". Other informants also supported this challenge in which the abundance of information channels leading some to confusion: "Part of the challenge is that there are no common guidelines or routines in how to sort out information and which channels to use. There's a lot of initiative. [...] Even though NSA tries to give the impression that this is the way they've always done it, it doesn't seem like it".

One informant stated that even *within* the NCSC partnership, information is distributed and shared through various means: "In NCSC, it's mainly emails [...] or [Microsoft] Teams. It depends on what is shared. If it's conceptual things, emails with PDFs are typically used, while indicators are shared through MISP, Teams or direct messages".

Organizational

The respondents' perceptions toward organizational CSIS benefits and challenges are depicted in Figure 5.7. Some of the statements are extracted and reported in the section above (operational level).

Professional networks and personal relations At the organizational level, one of the most agreed upon statements were CSIS' positive effects resulting in both extended and strengthened professional networks within the cyber security community. All respondents with less than two years of working experience in cyber security either agreed or strongly agreed to that CSIS contributes to an improved professional network.

Almost all informants stated that CSIS positively influences professional networks and vice versa. Most of the informants either frequently participated or hosted conferences and similar events. These forums exist both in the public and the private sector, and in national and international arenas. One informant stated that "The personal relations among individuals on both sides obviously contributes to information sharing which otherwise would not have been shared. You are totally dependent on personal relations".

This was also supported by another informant, which highlighted the positive aspect of personal relations: "The deal is I get to know things, but they are classified. I can only further disseminate that information to other individuals with the necessary security clearance and authorization. But the knowledge I gain personally makes me better equipped to make assessments on behalf of all our members. [...] We have a secret handshake where we agree that he [an acquaintance in the national services] gives me a report, which is a sign that I should read it and that it is important for us. By this, he hasn't neglected his role and I haven't learned anything I shouldn't know". Other informants stated the codependency and role differences between interpersonal and formal information sharing structures: "I would say that formalized information sharing agreements are superior to those based on personal relations. But formalized agreements are quite time-consuming to set up. Purely speaking of effectiveness, personal connections can give more *bang for the buck* compared to formalized agreements with all their challenges and administrative hassle. But I think that it often starts personal before it transitions to a more formalized manner".

The latter perception on formalized agreements was also supported by several top managers, critiquing the interpersonal nature of CSIS: "We need to take the step from doing sharing between people to establish a structure between enterprises - which does not depend on personal relationships".

As described in Section 3.3.4 Traffic Light Protocol, TLP:RED limits the shared information to the eyes and ears of *individual* recipients only, and in nature contradicts the exclaimed goal of several informants. A top manager further elaborated on this challenge: "We had to enter into a wrestling match with [national service] over TLP, and had to say: *If you share this information with someone in* [informant's enterprise], it will be further shared within [the enterprise]. Because it's the function and not the person that matters. And we had to work alot on that matter, internally as well. People were of the opinion that *no, this is information I have received*. No, you received this information because of your role in our business. We need that information, so you are obligated to make an assessment of relevance to others and upward within our organization. Otherwise the CERT functions become autonomous teams running their own besserwisser[7] environments". The informant also stated that this reluctance to further sharing and negative dependency on personal relationships were commonplace within cyber security organizations.

Establishing trust within the Norwegian cyber security community Generally, the respondents did not find it difficult to establish trust with other people that engage in CSIS efforts, as approximately 60% did not agree that it was diffi-

[7] Besserwisser is a common Norwegian negative term stemming from German. The term has an equivalent English meaning as a "know-it-all".

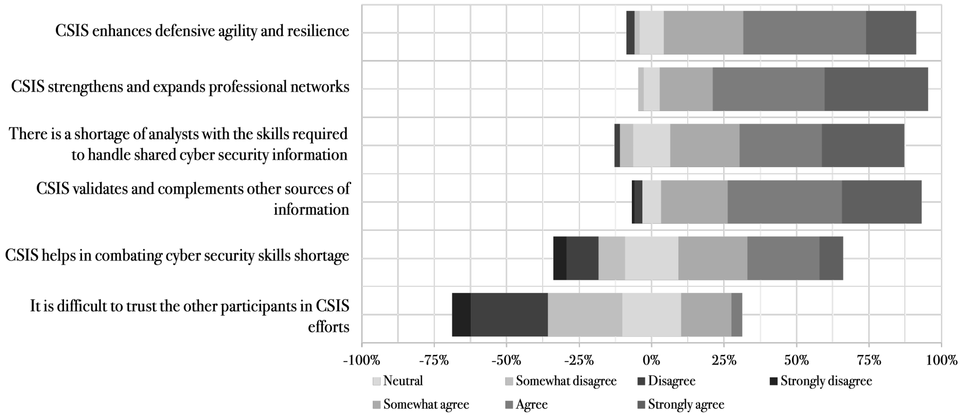

Figure 5.7: Respondents' attitudes on benefits and barriers in CSIS- Organizational category.

cult. A total of 33% disagreed or strongly disagreed, and the distribution were approximately similar considering the role of the respondent. However, both middle managers and practitioners were less concerned about the challenge with establishing trust among participants attending in CSIS fora than top managers. Another interesting finding was that over twice as many agreed or strongly agreed that trusting other participants in CSIS was difficult in the public sector compared to the private sector. Establishing trust with partnering organizations was debated among all qualitative informants. However, no clear distinction between the opinions of top and middle managers, and practitioners were evident in the qualitative sample. For example, one top leader exclaimed that "I think you should share as much as you can, and think again if you can share even more. Because I think we aren't more than we are in this field, all hands should be on deck. [...] We cannot provoke more sharing by holding back on our part". Others have a more nuanced perspective to establishing trust: "[...] the level of trust depends on the importance of the information shared - when you share your sensitive and valuable information and the recipient acknowledges it, you tend to get the same in return".

The wide-spread willingness to trust other parties of interest was further exemplified by a top manager within the public sector: "Firstly, information sharing means that people can be involved in managing cases across areas of responsibility and enables you to maintain the security outside of yourself which other benefit from. Secondly, others gain insight into your capacities, which means they know where to ask if they need help. And thirdly, information sharing assists in helping yourself, and not turning information sharing into a battle for resources - information sharing should be seen as a necessity to do your own job. If you think of information sharing as a fight for resources or to protect one's own job and responsibilities - then I think we are on the wrong track". However, some state that there still exists challenges with regards to information sharing on their own vulnerabilities and incidents: "[...] the willingness to share may get better because we still find that some of our members are a little difficult because they do not understand how it benefits the sector and everyone".

One informant also stressed the importance of trust: "We have built up a large degree of trust to [organizations] we regularly cooperate with. Due to a mutual understanding of each other's roles and good common understanding of the sharing culture, there's a low threshold for sharing both ways. If we cooperate with another organization with which we have not developed this understanding, then there are slightly different requirements from our part. Maybe a higher threshold, since we're not as familiar with their culture and they are not familiar with the sharing culture we expect. The requirements you make depend entirely on how established the relationship is, how much trust there are and how they process your information. And what type of undertaking the receiving party is. If its an established government service, you automatically place higher degrees of trust in them [...] than you can place in a private enterprise. There's a certain type of information shared in the two places, and it will rarely be the same information" .

Personnel shortages within the Norwegian cyber security community Over 80% showed some degree of agreement that there is a shortage of cyber security analysts with the required skills to handle shared CSI. This finding was supported by the statements of an informant in top management, which exclaimed that even though SREs are a good idea on paper, they further increase the already strained personnel situation, which he claimed is ever getting worse: "The more sector CERTs we get, the larger the personnel gap is going to get. Personally, I have been in strong opposition to the SRE idea from the start, and said we don't have enough people. [...] The intention is good, but we don't have enough personnel with the required skills to fill all the positions needed".

The same informant also gave an example where the lack of sector- or enterprise-specific knowledge could have had significant consequences: "In one case, we never received [vital alerts & triggers for action] through national channels, but got it from international partners - because in Norway [the information] was suddenly classified. It was given to all European entities which supported [a certain FNF], but didn't reach us through national channels. A few months later, we understood that the Norwegian national services didn't understand how this information was relevant to us".

Other informants also confirmed the difficulties of recruiting competent personnel. An informant in an attractive and well-known enterprise described their struggles in recent recruiting efforts: "We need a more technical CTI analyst, but it's really hard to recruit nowadays, even though we have extensive ongoing promotion campaigns". A third informant stated: "We are currently in the process of hiring eleven new people, but we've recognized that we won't be able to get hold of eleven seniors. We need to think long-term with these people and use the seniors to develop the juniors. There will always be people leaving us for other firms after being here for some time, but we need to think bigger and think that the current juniors will, in time, become seniors".

Effect of CSIS in combating cyber security skills shortage Almost 60% agreed to that sharing CSI helps in combating cyber security skills shortage. Accordingly, the respondents expressed that sharing CSI might contribute to mitigate the perceived challenge with the lack of cyber security personnel with skills required to utilize CSI. One informant in top management of a public organization stated that CSIS also has a positive effect on recruiting attractive cyber personnel: "In this line of work, there are limited of accessible personnel, and that means that appearing more relevant with greater access to information also has a recruiting effect". Another informant in top management presented other possible solutions to fight the deficit: "NCSC should have an increased staffing and dedicated personnel working toward each sector. Instead of each SRE having their own 24/7 environment, it would be far more effective to centralize the capacities in NSA and fly them out to the enterprises in need. And the need for information is very different if they are subject to the Security Act and has an operational interface with NSA, in contrast to smaller enterprises which is and do not. [...] You don't need all the middlemen. We need people in the enterprises and centrally. By establishing SREs, they drain people from both NSA and the enterprises - the two entities which has the most need for competency and capacity".

Economic

At the economic level, the respondents were less explicit in their perceptions as depicted in Figure 5.8.

Cyber security costs and investment decisions The respondents were not clearly agreed on whether CSIS reduces overall cyber security costs or not, and if establishing CSIS infrastructure is expensive and drains resources. However, the personnel in public sector were more positive to that CSIS contributes to reduced cyber security costs compared to the personnel in private sector. In fact, the two groups had opposing perceptions where 60% of the respondents in public sector to some extent agreed to that CSIS reduces costs, whereas only 35% in the private sector expressed the same. On the other side, only 14% in public sector disagreed that CSIS reduces cost, in contrast with 42% in private sector. With respect to the idea that it is expensive to establish CSIS infrastructure, sector association had less influence on the answers given by the respondents. However, the respondents in private sector were still more agreed than the public sector to the expensiveness

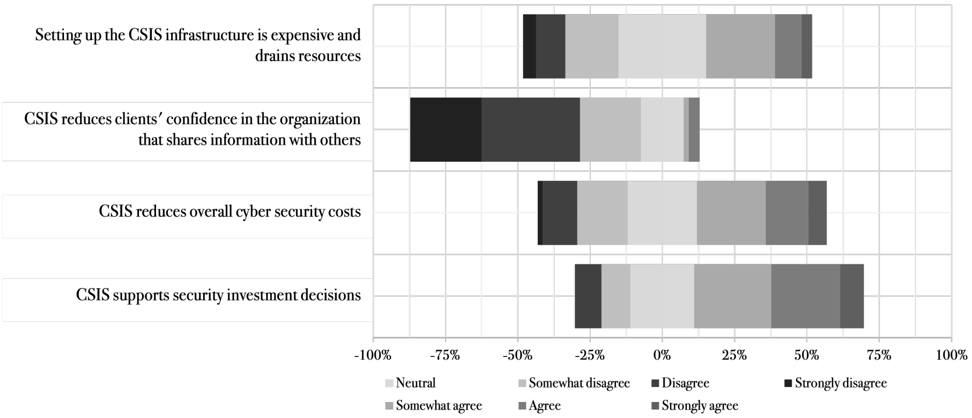

Figure 5.8: Respondents' attitudes on benefits and barriers in CSIS - Economic category.

of CSIS infrastructure.

35% of the respondents either strongly agreed or agreed to that CSIS supports security investment decisions. Despite this, middle managers with over five years of working experience in cyber security were the only personnel category which strongly agreed to the statement. Respondents' role had less influence of those who were generally positive to that CSIS supports cyber security investment decisions.

The qualitative findings indicate that CSIS' contribution to reducing costs and support decision-making are dependent on the enterprise's maturity within cyber security. A private sector middle manager exclaimed that: "The most important thing we do is that which support concrete decisions. A CSIO is preoccupied with who might attack their organization, how they are going to do it and what they can do to protect themselves. [...] We don't care about whether Russian cyber actors will attack Norway, others are far better equipped to assess who does it. What we do is say *they use this malware, we're bad on detection in this area, we need to use more resources on these detection areas*. We prepare ourself for if they do it - but whether they do so is not something we preoccupy ourself with". The same informant also stated the value of CSI in system architecture: "A major focus of ours is assessing what is going on in the current threat landscape, build situational awareness and which attack vectors we see the most. This is to give more guidance and backing to the system architects". More directly, several informants stated that the ability to transform and convert high-level information or collate and process low-level information into suitable preferably predicative assessments was key in aiding their organizations in efficiently implementing and adjusting their cyber security efforts to counter digital threats.

CSIS affecting clients Even though the loss of clients confidence and satisfaction were reported as a challenge to CSIS in the theory, the majority of the respondents were to some extent disagree to this. Approximately 60% either disagreed or strongly disagreed to that sharing of CSI reduces clients' confidence in the organizations that shares information with others. This challenge was contested in the qualitative findings, at both positive and negative impressions were present. One informant exemplified this issue: "You often share less than you can because you're afraid that third parties may react to your information sharing, and makes you insecure". When asked to elaborate on who typically reacts, the informant responded: "it could be anyone - from [other departments within their organizations], it can be perceived as wrong to share with other sectors, it may be that the person which coordinates cross-sectorally says *you're not the one to share that, we are*. This is due to the sector principle, where the information has to flow through your ministry via another ministry and then to the intended recipient, which takes significantly more time". In some cases, CSIS may also negatively impact the survivability of an undertaking, even when CSI is shared to the authorities: "From previous jobs, I recognize that you don't dare to report if you are on the stock market - it's a challenge if the stock price drops if you report an incident.[...] Undertakings are worried that they'll go bankrupt if they publicize incidents, but still want it to be investigated".

Others highlighted that sharing CSI may have a positive impact on clients' trust: "We also have some companies that wants their information to be shared with everyone because they want their willingness to share to be known to others, but we also have those that to not want to be referred to at all". Even though CSI often emerge from detected attacks or exploited vulnerabilities which has potential negative consequences to e.g. the undertakings' stock prices and reputation, some informants also saw positive aspects in transparency and openness: "With regards to the cyber attack, we wanted to take social responsibility by being as transparent as we could be [...] - simply be a good example for others". Another informant stated that one main consideration led to them intentionally going public with an incident: "There was one intention by doing this: To tell those who had stolen the information that we knew about them, and if others got hold of that information they would not be able to use it - as it would be a criminal act".

Policy

Figure 5.9 depicts to what extent the respondents acknowledged or disproved the statements related to policy. The positive perceptions related to cooperation with government agencies clearly overweight the negative perceptions.

Attitudes toward relationships with government agencies As many as 83% had a positive attitude toward strengthened relationship with government agencies due to CSIS. However, respondents in public sector expressed a stronger

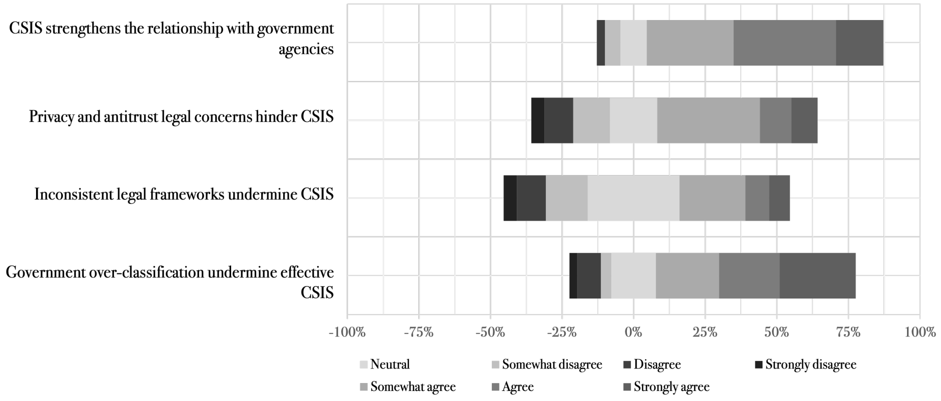

Figure 5.9: Respondents' attitudes on benefits and barriers in CSIS - Policy category.

agreement to that CSIS strengthens the relationship with government agencies than respondents in the private sector, where 28% of the public respondents strongly agreed compared to 9% in private sector. There was no significant difference between what the personnel in the different hierarchical levels perceived.

Issues regarding classification and over-classification Even though the majority perceived that CSIS strengthens the relationship with government agencies, over-classification done by government agencies were still perceived as a challenge toward effective sharing of CSI.

Over-classification was a subject which was heavily brought up by both public and private informants. Informants in the private sector, and those informants in public sector describing themselves as net consumers of CSI heavily critiqued the national services for either over-classification or over-sanitization[8] of information.

As described in Section 3.3.4 Protection and restrictions related to the Security Act, both personnel in public and private sector may obtain a security clearance and gain access to classified information and information systems. Accordingly, several informants had access to classified information. The terms over-classification and over-sanitization were associated with different challenges, both reducing the usefulness to the recipients.

[8] Sanitization is a process where intelligence products are rewritten in order to enable dissemination with a lower security classification, or to protect the source(s). In order to sanitize information, there must be an alternate source, the intelligence discipline must be disguised in order to protect the source of the information and a risk assessment must be performed [143].

One recurrent issue from informants in both sectors is either a lack of- or insufficient number of clients connected to a classified network such as National Restricted Net (NRN). An informant in the private sector stated that "[...] [classified information] worsens digital interaction and makes it complicated to share information when you are not on the same network. I hear that the same is a problem in the public sector due to few available approved rooms or accessible clients. I am part of [forum], but even there we don't have access to authorized premises, so if we want to talk classified we have to wait until we have access to one. As owner of critical infrastructure we have a need to understand more". The same informant also complained about a lack of guidance in how to handle and discuss classified information: "A common phrase I hear is that *it gets so complicated, there is so much that is classified*, but you have to learn to handle that in order to be able to have a dialogue. You have to know what you can and can't share, and here I think the authorities have been slow to dare to challenge themselves about what can actually be talked about". When asked about guidance and training in how to process classified information, one middle manager in the private sector stated: "You get *here's the authorization form, here are the rules, sign*, but you don't get *here's the guide and what you actually can do*, and it actually takes some experience to use classified information [...]. We in [enterprise] with prior experience from law enforcement and the armed forces etc., are somewhat used to it. But we would never hand over a piece of classified information to any of our customers".

With regards to over-classification, one middle manager exclaimed "I am disgusted by over-classification. I think there's a lot of fear regarding sharing classified information from the public to the private sector. There is an absence of trust, despite the fact that you often know the people working there. And the mistrust is not unfounded, I myself would have been very careful in sharing if I had worked in NIS. But then you can't brag about the cooperation between the public and private sector either". Even informants handling and producing classified information found it hard to classify correctly: "We often need to have a huddle and discuss it - the classification level is seldom obvious. We know the definitions stated in the Security Act, but it's not always the case that you read it and immediately understand that *if lost, this information can severely harm national security interests*. However, it is also possible to downgrade the information, regarding which one informant stated: "We can lower the classification on the information we ourself own, but we can't lower the classification of [other organizations], in those cases we have to return to the information owner. We have done this several times, where they in turn reassess the classification".

Despite this critique, the informants vastly preferred classified or over-classified information to over-sanitized information: "It is annoying [to receive classified information] - it's useful, but it has to be very well sanitized or you have to incorporate it into other information and use it to strengthen your own assessments". A senior practitioner supported this, and stated: "[...] the information and knowledge I receive makes me better equipped to make assessments".

Over-sanitization Of all the challenges associated with information sharing with the national services, over-sanitization was perceived as the most prevalent: "When we go to briefings down at [NCSC], we're more current if we read what's on Twitter. [. . .] They think they have to protect their sources and methods, while we try to get them to understand we're reading the same Twitter-feed, don't even bother. This isn't classified - if you have a secret source no-one is supposed to know about, [. . .] we don't need to know - we only need to know what information to search for in our own networks and some background knowledge on why it's is important, but that's not happening" . Another informant agreed: "We get nothing out of [public-private cooperation] because it's so generic. If we get something, we've already gotten it from somewhere else". A middle manager in a public organization processing classified information was asked whether he received unclassified TLP protected information, and responded: "If so, it's the same information which is shared with private organizations, but I don't think it's of any use as it's a sanitized version of the classified information NSA has. Most often it is shared with us at the original classification".

Based on the quantitative and qualitative findings, it is apparent that both over-classification and over-sanitization is an issue, especially for those enterprises which does not have personnel with security clearance. Even informants with security clearance were highly critical to the national services' ability to provide useful information on restricted or secret classification due to the governments' sanitization concerns. Those informants which to some extent were content with the information provided by the national services, all stated that trust was essential, and that this trust was build upon long-term cooperation.

Legal frameworks related to CSIS Around 1/3 of the respondents were neutral to whether inconsistent legal framework undermine CSIS. Additionally, about the same number of respondents showed either positive or negative attitudes toward the statement. Respondents in the private sector, on the contrary, showed less extreme attitudes toward whether existing legal framework in Norway challenge CSIS or not.

Around half of the respondents acknowledged that privacy and antitrust legal concerns challenge CSIS, where about 20% expressed a high level of agreement by either being agree or strongly agree. No significant difference were observed when comparing the perceptions in the private and public sector.

One informant elaborated on how privacy regulations affect information sharing: "Data sharing is a challenge. We want to share, but we see challenges in sharing because it can affect the privacy [of customers and employees]. As we've learned, I think this may be an issue for many others". Another informant shared this experience: "we manage to filter out irrelevant information, share it widely and automate as much as we can. [...] Sharing information without violating GDPR has been a huge challenge, but we've broken ground and now it's working well". Others stated that privacy issues were not a problem, as sensitive personal data is irrelevant to the information exchange". The two latter statements indicate that the maturity of undertaking and the information exchange at least partially reduces the challenges related to privacy concerns.

5.2.3 Attitudes toward CSIS

The vast majority of respondents agreed that CSIS has positive impact on both their own organizations, other organizations and improve the national security posture. This section goes deeper and examines the perceived usefulness, willingness and sharing frequencies to specific CSIS categories.

Usefulness Figure 5.10 depicts the quantitative results on perceived usefulness of the CSIS categories. When combining both those who responded "useful" and "very useful", participants responded that *expertise sharing* (86%) was the most useful form of CSIS, with *knowledge sharing* (84%) and *alerts & triggers for action* (84%) as the second and third most useful category respectively. The attitudes toward data sharing, alerts & triggers for action had similar distributions between both the private and public sector. However, there were recorded larger differences with regards to the respondents' roles: top and middle management reported the highest perceived usefulness of data sharing and alerts & triggers for action, while practitioners were generally more positive toward knowledge and expertise sharing. There were no distinct differences between the responses and years of experience.

The informants, on the other hand, had somewhat varied responses to which CSIS category they perceived as most useful. Top leaders were generally more concerned with having a broader understanding of the threat landscape, while practitioners were more concerned with alerts & triggers for action, which is contradictory results compared to what was discovered in the quantitative results. However, several informants in top and middle management responded that *all categories were equally important*: "If I had to reduce something, it would have to be a category which doesn't accomplish my tasks.[...] It's not like we can cut all alerts & triggers for action due to budgetary reasons. In that case, I would have to choose *which* alerts & triggers to manage, which I in turn must also share data and knowledge about. [...] It's a process, and I can't just do parts of the process when handling an incident, I have to do the whole process. If so, I'd rather say that *I will focus on these incidents* because they carry a larger risk and consequence than other incidents - that's the priorities I have to make, not which steps of the process I should do".

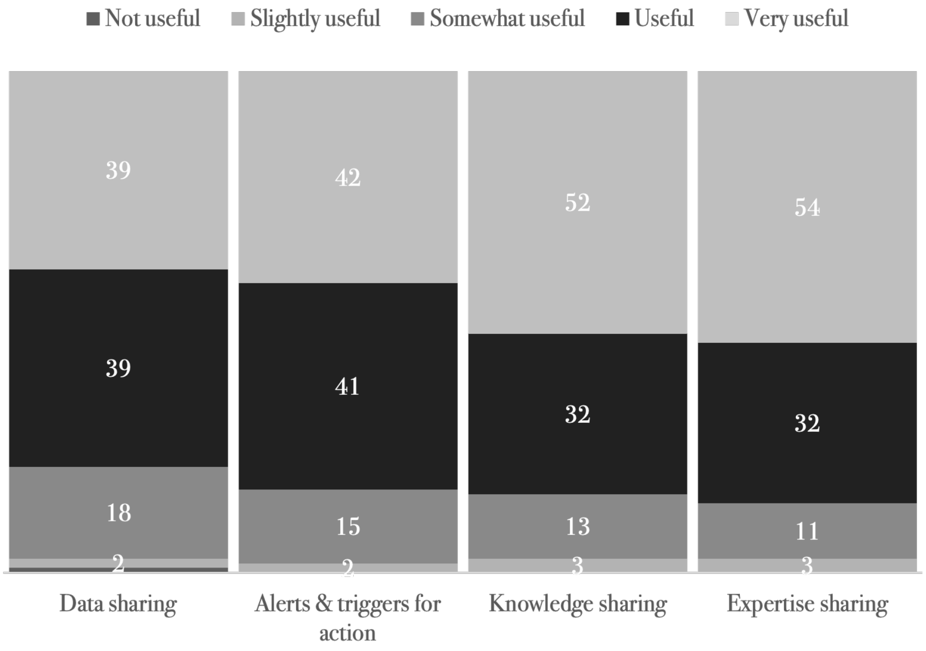

Figure 5.10: Questionnaire responses in percentages by the perceived usefulness of each CSI category.

To other informants, alerts & triggers for action were regarded as most important: "Alerts & triggers for action is what immediately contributes to prevention and detection". Another informant stated: "If I have to choose one category, I would define alerts & triggers as most actionable and useful. You get many good reports describing the context and methods, which are very useful to learn, understand and build context and threat picture, but strictly speaking of usefulness, it's alerts which gives us the most results. But if you don't have the remaining three the value decreases". Several also interlinks the value of alerts & triggers for action to accompanying data sharing: "Alerts & triggers for action will often be accompanied by data sharing. It happens that we only share alerts & triggers, but those reports will normally have less value - if you can supplement with data sharing it will have higher usefulness - [. . .] some technical information, but also context".

Multiple informants also links the CSI categories with the maturity of the organization: "We've moved from sharing very technical information [. . .] to wanting the level above - what is this incident likely about, how can we discuss the possible threat actor? [. . .] It's important to understand the incident, but it's more important to understand the threat dimension, why we need to protect ourself, what we protect ourself against and their maturity level. This is a prerequisite for CSI to have added value - if you share information with someone that doesn't understand the threat dimension it's only intimidating". A private informant in top management also added how more knowledge and expertise sharing would have added value to their enterprise: "If we were better at knowledge and expertise sharing, we would have gotten more out of sharing data than we do today".

While several informants in cyber security organizations emphasized data sharing and alerts & triggers for action, one informant in the public sector stated that: "In my perspective, the threat picture and the way that [respondent's organization], together with other public institutions and certain important industrial sectors, constitute the areas with the highest value, the same areas in which the most advanced threat actors are most interested - on that list, [the informant's organization] is high up. Our task is to protect one of the most important institutions in terms of security, so in that sense you can say that the methods and capabilities we have are sensitive. We cannot make [informant's organization] a softer target than [the organization] needs to be, by for example telling which tools we use etc. A threat actor should not have that information. In that sense, [informant's organization] is more sensitive than many others. More so than with others where the damage potential is only monetary. Fundamental National Functions are ranked higher than softer targets, which mean that there are higher requirements for sensitivity than with others".

Willingness Respondents from the public sectors were consistently more willing to share CSI than their private counterparts. Both respondents from the private and public sector were more willing to participate in knowledge sharing and expertise sharing, than they were to participate in sharing data and alerts & triggers for action. With regards to experience, respondents with less than two years of experience scored the highest willingness overall with an average of 94% stating they were willing or very willing to share CSI. The corresponding averages for 2-5 years and > 5 years were 79% and 82% respectively. Both respondents with < 2 years and > 5 years of experience were increasingly more willing to participate in sharing more comprehensive CSI (e.g. knowledge and experience sharing) than they were in sharing alerts & triggers for action or data. The responses from those with 2-5 years of experience are opposite - they were more inclined to share data and alerts, than knowledge and experience.

When comparing the respondents' roles and their willingness to participate in CSIS, there were no quantitative significant differences when averaging all categories - 80% of top managers, 83% of middle managers and 85% of practitioners were either willing or very willing to share CSI. Top and middle managers were also significantly more inclined to engage in knowledge and expertise sharing than data and sharing alerts & triggers, while practitioners' did not have the same category preference - the perceptions differed with less than 5 percentage points between data sharing and alerts & triggers for action (83%), and knowledge and expertise sharing (86%).

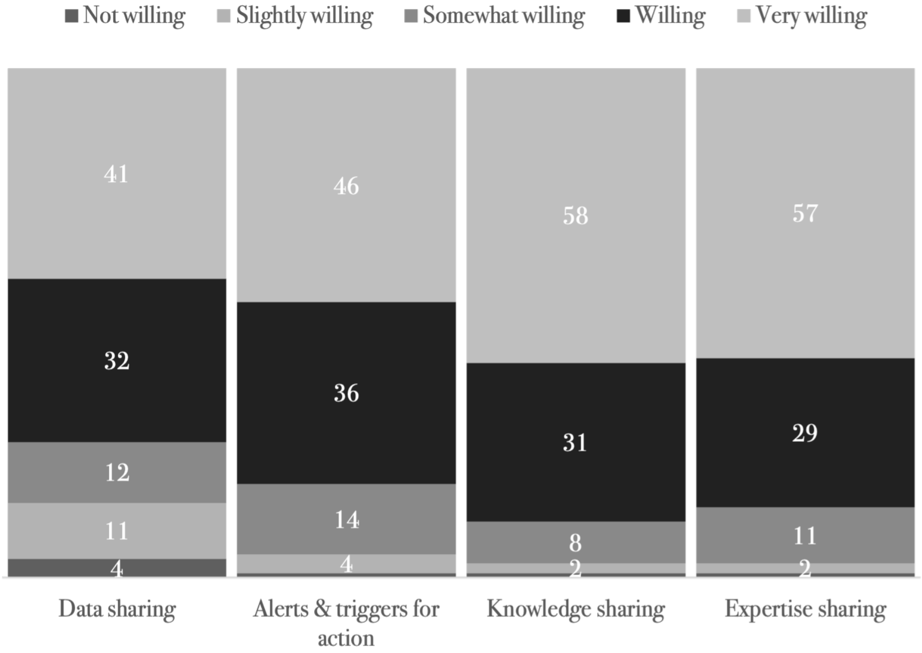

Figure 5.11: Questionnaire responses in percentages by the perceived willingness to share each CSI category.

The key take away given by the informants, was that the willingness to share CSI was mainly based on cost-effectiveness assessments and resources available: "Basically, we want to contribute as much as possible, the limitation is available resources. [. . .] It's simply whether we have the capacity. But we see that if we take the time to invest the time and resources, we get manyfold in return". Despite the critique previously described against national services and the government, most informants stated they were either very or most willing to share information with said entities: "We probably are most willing to share information with the government. [. . .] We don't think that the information shouldn't be shared if it's going to our competitors - we think that all security information should be shared". Some were more skeptic in sharing with competitors: "Own government is unproblematic. Alot of enterprises which we don't compete with is also not a problem. However, we are very careful about sharing with similar enterprises or enterprises we are in direct competition with. [. . .] But, we recently held a talk at [event] and told how we had configured [security architecture] in front of all our competitors, because we know how much work is behind it - you can't just clone it and get it up and running".

Several informants in private top management elaborated on why they were especially willing to share information with the government: "We have our membership model as our foundation - if we share with everyone, we basically erode our financial model. But we share with our members and partners, and we are very generous with the authorities. [. . .] We send all our reports to NCSC, NC3/NCIS, basically every government entity which wants access to our information". Another informant also noted positive aspects of using classified information and the Security Act to their advantage: "Of course we compete within the field of security. We don't want [the enterprises' competitor] to get attacked, as it would create extensive problems for ourselves, but what hurts them is good for us - it would increase our earnings. But sharing tactical experiences and talk about measures would've been of great help. [. . .] To meet in a SRE and talk classified, knowing that it would be inadmissible in strategic plans would've been useful. [. . .] I think that the journey into what we share for security reasons and for national security, which we cannot bring into a financial setting, would've been a good experience".

Frequency By measuring the singular responses with the highest rate per CSIS category in both public and private sector, the results are similar. Both public and private respondents participate in data sharing daily, knowledge sharing weekly and expertise sharing on a quarterly basis. However, respondents within the private sector opted that they share alerts & triggers for action daily, while those in the public sector shared this kind of information on a weekly basis. The responses also indicates that it is more common within the private sector to engage in expertise sharing on a weekly basis.

Respondents with 2-5 and > 5 years of cyber security experience stated that their organization most frequently participated in knowledge and expertise sharing than those with < 2 years. However, only 3 percentage points differed between how often they participated in data sharing and sharing alerts & triggers for action, possibly indicating that more experienced personnel has more emphasis on information sharing *in general*, while practitioners most often engage in more "hands-on" information sharing (e.g. data sharing and alerts & triggers for action) - rather than the more comprehensive knowledge and experience sharing.

When comparing roles and frequency in CSIS, respondents in top management consistently answered that their organizations participated more frequently in CSIS in all categories - significantly more frequent than what respondents in middle management and practitioners answered.

The qualitative analysis of which CSIS category shared most often were inconclusive, as most informants either stated that most of their information sharing happened through automated technical solutions, had a hard time determining which category they participated in the most, or found the question irrelevant: "It's all based on what's going on. It's like comparing apples and oranges. We're dependent on receiving all categories to do our job. [. . .] In an early stage, its important with low-level information sharing, e.g. data sharing and alerts. We receive both reports and more complex assessments as part of wrapping up major

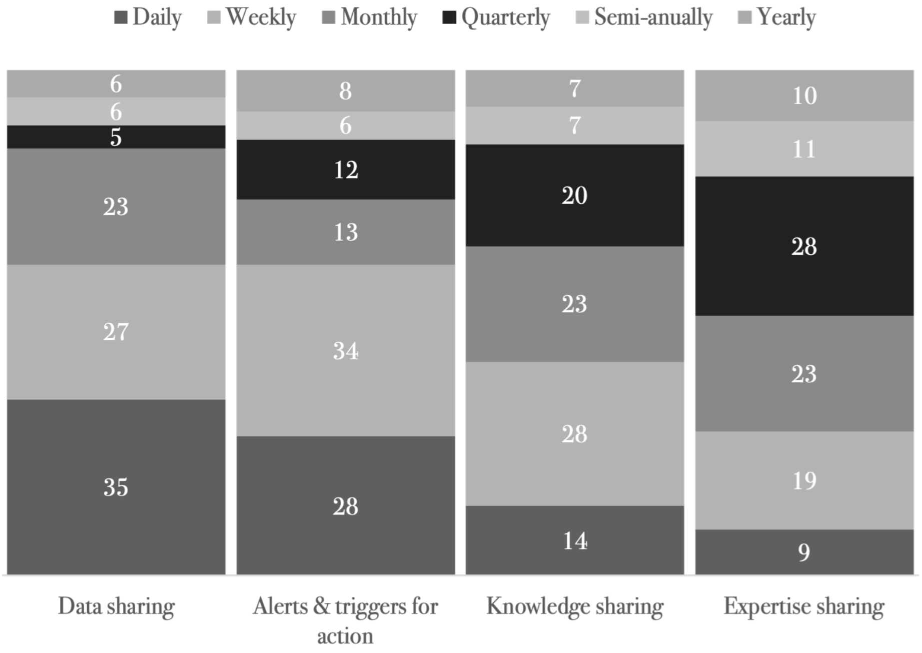

Figure 5.12: Questionnaire responses in percentages by sharing frequency of each CSI category.

	Mean			Median		
	Usefulness	Willingness	Frequency	Usefulness	Willingness	Frequency
Data sharing	4.15	3.96	2.36	4.00	4.00	2.00
Alerts & triggers for action	4.24	4.43	2.59	4.00	4.00	2.00
Knowledge sharing	4.34	4.22	3.01	5.00	5.00	3.00
Expertise sharing	4.38	4.39	3.42	5.00	5.00	3.00

Table 5.13: The mean and median overall scores for usefulness, willingness and frequency in which the respondents' organizations shares CSIS.

incidents, or as general assessments which may lead to a better understanding of the situation and threat - and we do expertise sharing as much as we can based on available resources".

As Figure 5.13 and Table 5.13 depicts, when comparing the mean scores for perceived usefulness and willingness to share the four CSIS categories without cross-tabulation against other variables, only small differences are found. Overall, knowledge and experience sharing are perceived as the most useful CSI, while the respondents are most willing to share alerts & triggers for action and expertise, while the willingness to participate in data sharing is significantly lower than what is observed with the other categories. Note that frequency is not depicted in Table 5.13, as the questionnaire contained six response options (ranging from daily to yearly), in contrast to usefulness and willingness, which had five.

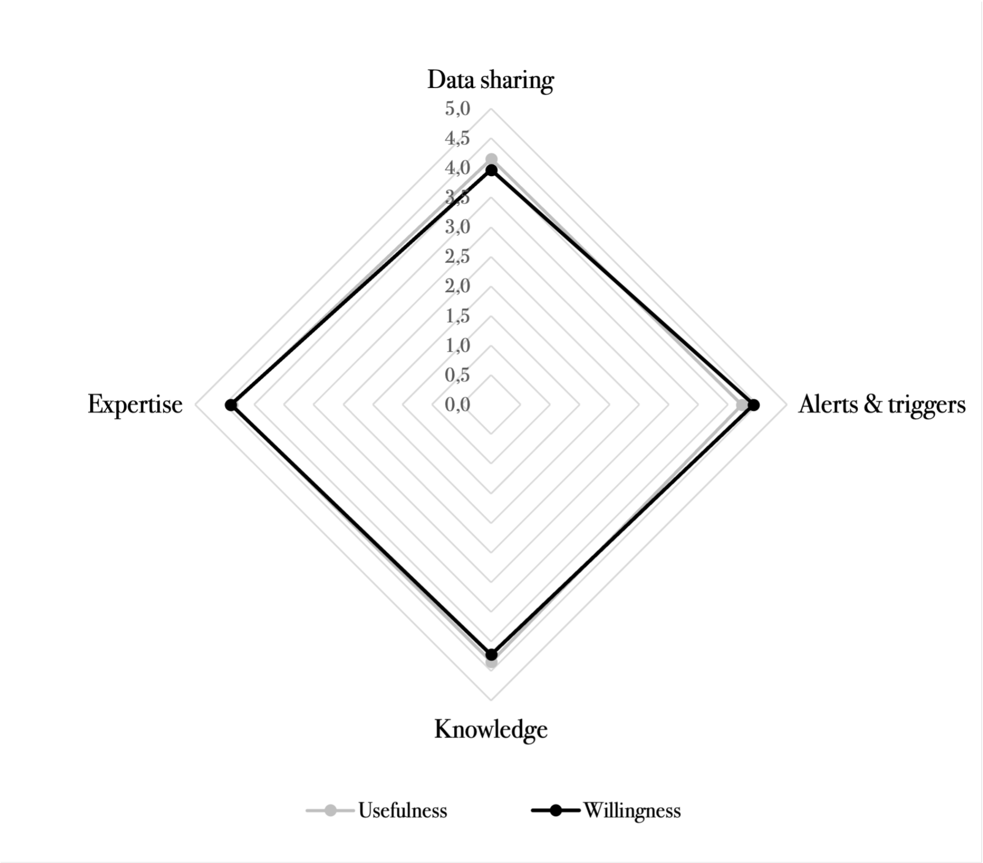

Figure 5.13: Difference between mean metric scores for the Usefulness and Willingness variables.

5.3 Results compared with former research on CSIS

In order to examine whether the perceptions and attitudes of the Norwegian respondents were supported or disproved by former empirical research of CSIS, the results in this thesis were compared with the findings in Zibak & Simpson [13][37]. Comparisons with other former studies described in Chapter 2 Related research are commented in the next chapter - Chapter 6 Discussion.

Looking at Table 5.14, the perceptions of the Norwegian respondents were both strengthened and weakened by the research of Zibak & Simpson [13]. As some of the statements examined in [13] were not included in this thesis, only statements measured in both studies were compared. The statements marked with a star (*) were not directly comparable as the statements were rephrased og adjusted in this thesis.

As the focus on both national and international cyber security have increased since the research of Zibak & Simpson [13] was conducted in 2019, it is uncertain whether the differences between the perceptions of the Norwegian and British cyber security personnel were due to the these last year's cyber security evolution.

However, the most interesting finding of the comparison was that the Norwegian respondents generally agreed more with each other, and were more extreme in their perceptions of benefits and challenges of CSIS than the British respondents as both the medians were more polarized, and the interquartile ranges usually were lower indicating less spread in the perceptions.

Despite this, neither role nor organization's sector in any of the studies accounted for any statistically significant differences in regards to the attitudes toward CSIS benefits and challenges [13].

Benefits with CSIS As depicted in Table 5.14, respondents in the UK and the Norwegian studies expressed strongest agreement with the ideas that CSIS supports breach detection and recovery efforts, develops and maintains strong professional relationships, and improves organizations' defensive agility and resilience [13]. The Norwegian respondents, compared to the UK, strongly agreed that CSIS also supports incident response efforts.

Even though the statements in this thesis and the British study regarding improved security posture and situational awareness were formulated slightly differently, they were still comparable. In contrast to the Norwegian respondents, the British cyber security professionals agreed less to that CSIS contributes to improved overall security posture and situational awareness. Of the Norwegians, almost every respondents agreed to some extent, compared to around 50% of the UK participants [13].

Statement	Category	Dimension	Median-N (IQR)	Median-UK (IQR)
(St1) CSIS contributes to enhancing the national security posture and situational awareness*	Operational	Benefit	6 (1)	5 (3)
(St2) CSIS contributes to enhancing organizations' security posture and situational awareness*	Operational	Benefit	6 (1)	5 (3)
(St3) Threat actors are deterred by CSIS among organizations	Operational	Benefit	4 (3)	3 (2.5)
(St4) CSIS supports incident response efforts	Operational	Benefit	6 (2)	4 (2.5)
(St5) CSIS contributes to breach detection and recovery	Operational	Benefit	6 (2)	5 (2)
(St6) CSIS reduces duplicate information handling [...](*)	Operational	Benefits	5 (2)	3 (3)
(St7) CSIS strengthens and expands professional networks	Organizational	Benefit	6 (2)	5 (2)
(St8) CSIS validates and complements other sources of information	Organizational	Benefit	6 (2)	5 (3)
(St9) CSIS enhances defensive agility and resilience	Organizational	Benefit	6 (1)	5 (2)
(St10) CSIS helps in combating cyber security skills shortage	Organizational	Benefit	5 (3)	4 (4)
(St11) CSIS reduces overall cyber security costs	Economic	Benefit	4 (2)	3 (4)
(St12) CSIS supports security investment decisions	Economic	Benefit	5 (2)	4 (3)
(St13) CSIS strengthens the relationship with government agencies	Policy	Benefit	6 (1)	5 (2)
(St14) Standardization issues hinder CSIS	Operational	Challenge	4 (2)	4 (4)
(St15) Inconsistent definitions and terminology undermine efficient CSIS	Operational	Challenge	5 (2)	5 (2)
(St16) It is difficult to determine the accuracy and quality of received cyber security information	Operational	Challenge	5 (2)	5 (2)
(St17) It is difficult to ensure the timeliness of shared cyber security information	Operational	Challenges	5 (2)	5 (2)
(St18) The interoperability and automation of CSIS are difficult to achieve	Operational	Challenge	5 (1)	4 (4)
(St19) CSIS results in redundant and irrelevant data	Operational	Challenge	3 (2)	5 (1)
(St20) There is a shortage of analysts with skills required to handle shared cyber security information	Organizational	Challenge	6 (2)	5 (2)
(St21) It is difficult to trust the other participants in CSIS efforts	Organizational	Challenges	3 (2)	3 (3)
(St22) Setting up the CSIS infrastructure is expensive and drains resources	Economic	Challenge	4 (2)	5 (2)
(St23) CSIS reduces clients' confidence in the organization that shares information with others	Economic	Challenge	2 (2)	5 (3)
(St24) Government over-classification undermine effective CSIS	Policy	Challenge	5 (3)	4 (2.5)
(St25) Privacy and antitrust legal concerns hinder CSIS	Policy	Challenge	5 (2)	5 (3)
(St26) Inconsistent legal frameworks undermine CSIS*	Policy	Challenge	4 (2)	5 (3.5)

Table 5.14: Median and IQR scores compared with the research of Zibak & Simpson [13], where Median-N (IQR) is this study and Median-UK (IQR) is the UK study [13].

The Norwegian cyber security professionals agreed upon the statement that that CSIS reduces duplicated information handling, whereas the UK respondents disagreed to the same statement [13].

Challenges with CSIS Considering the perceived challenges with CSIS, the Norwegian respondents agreed less than the UK respondents about the expensiveness of establishing infrastructure to facilitate CSIS. Additionally, similarly with the UK participants, the Norwegian respondents agreed upon the difficulty of determining the quality and accuracy of shared data, ensure timeliness, and that vaguely defined terminology undermines CSIS efforts. Despite this, the Norwegians agreed less to that CSIS results in redundant and irrelevant data compared to the UK participants. Actually, the Norwegian and UK respondents expressed opposite perceptions, where almost 60% of the Norwegians disproved the statement, while 61% of the Britons agreed to the statement [13].

Usefulness The usefulness of CSIS was perceived differently in Norway and the UK. Among the Norwegian respondents, *expertise sharing* was perceived as the most useful form of CSIS, while *triggers for actions*[9] in the UK. However, *knowledge sharing* was ranked as the second most useful category and *data sharing*[10] as the least useful in both Norway and the UK [37].

Willingness Considering willingness to engage in information sharing, *alerts & triggers for action* also scored the highest among the UK respondents, followed

[9] *Triggers for action* was used in Zibak & Simpson [37]

[10] *Threat data sharing* was used in Zibak & Simpson [37]

by *threat data sharing*. In Norway, on the other hand, the respondents were most willing to engage in *knowledge sharing* and *expertise sharing* as the second. Accordingly, the Norwegian and UK respondents had opposing attitudes regarding willingness to share the different types of CSIS as the UK respondents were more inclined to share more timely and concrete information, while the Norwegians valued processed and contextualized information [37].

When comparing the perceived level of usefulness and willingness to engage in the different CSIS categories, the Norwegian participants expressed approximately the same level of both perceived usefulness and willingness as shown in Figure 5.13. On the contrary, in the UK the usefulness of *expertise sharing*, *knowledge sharing* and sharing of *triggers for action* consistently scored higher than the willingness to engage in the same categories as shown in Figure 2.1 on page 13. Only the willingness toward *threat data sharing* was perceived higher than the assessed usefulness [37].

Participation in CSIS To what extent organizations were engaged in CSIS were measured differently in this thesis compared to that of Zibak & Simpson's research [37]. Zibak & Simpson in [37] used a more imprecise description as the frequency range was more vague [11] than the one used in this thesis [12]. Given that *often* indicates *weekly* and *always* indicates *daily*, both the Norwegian and UK respondents were equally engaged in both *data sharing* and *alerts & triggers for action*. Despite this, the UK respondents reported that their organizations participated significantly less in *knowledge sharing* and *expertise sharing* [37], while the Norwegian respondents engaged in *knowledge sharing* on a weekly basis.

[11] Never - Rarely - Sometimes - Often - Always

[12] Daily - Weekly - Monthly - Quarterly - Semi-annually - Yearly

Discussion

6.1 The state of CSIS in Norway

This section discusses and integrates the findings of Chapter 5 Results with that of the theoretical research of legislature and policy documents as stated in Chapter 3 Theory. The section provides a more detailed and nuanced understanding of how Cyber Security Information Sharing (CSIS) in reality is practiced in Norway in contrast to how the theory intends it to be.

Two main incentives for engaging in CSIS are derived from theory: a mandatory legislative incentive for those undertakings subject to the Security Act, and one voluntary based on the mutual benefits of the participating undertakings [7]. Each government ministry identifies and breaks down Fundamental National Functions (FNF)s of which they are responsible in a process resulting in the identification of specific public or private undertakings that are vital to functions or sub-functions supporting specific FNFs, as presented in Section 3.2.3 Classification of critical national assets and 3.4 The Norwegian cyber security landscape [2]. Accordingly, both public and private undertakings can be subjected to the Security Act.

The Norwegian cyber security landscape can be categorized into three distinct hierarchical levels:

a) *national services*,
b) *cyber security organizations and Sector Response Entities (SRE)*, and lastly
c) *individual undertakings*.

Norwegian cyber security landscape in theory and practice National Security Authority (NSA) and the Norwegian National Cyber Security Centre (NCSC) can be regarded as the the public face of the national services. NSA has access to Cyber Security Information (CSI) from participating undertakings directly through the National Warning System for Digital Infrastructure (WSDI) or through security reporting from either cyber security organizations or individual undertakings. NSA also exchanges information with international partners in addition to the other national intelligence, surveillance and security services, of which the latter information exchange mainly is conducted through Norwegian Joint Cyber Coordination Centre (JCCC) [45]. The resulting unclassified or low classified information is then processed and disseminated to subordinated entities through NCSC. However, the latter flow of information - originating from the national services through the NCSC - was highly critiqued in terms of over-sanitization, over-classification and due to insufficient timeliness. Participants from the national services and other organizations producing classified, and unclassified information had, however, a strong focus on disseminating as much unclassified information as possible or achieving as low classification level as possible on that information which was impossible to fully declassify. This implies that over-classification may not be the underlying issue, but rather that significant amounts of relevant information exists on a classification level in which most undertakings do not have access. However, over-classification may also be the result of the difficulty in assigning information the right classification level - resulting in over-classification as a safeguard.

Insufficient ratification of the Security Act and guidance from NSA Although the quantitative analysis regarding whether inconsistent legal framework undermine CSIS or not was ambiguous, the informants expressed several challenges with the Security Act and insufficient guidance from NSA. Even though the informants were generally positive toward the Security Act and the SRE model, most perceived that the current scheme was sub-optimal compared to the intent of the Security Act and the creation of NCSC. Key arguments for this assertion was the decentralized FNF identification process, lack of competency in certain ministries, lack of supervision from both NSA and the ministries, and a lack or insufficient prioritization of undertakings. The uncertainty related to how NSA and NCSC prioritize their support to the different sectors and undertakings had a disincentivizing effect on some informants in sharing CSI with NCSC in favor of focusing their cyber security resources on strengthening themselves. Additionally, almost all informants in undertakings subjected to the Security Act and with security clearances, did not perceive that being subjected led to greater access to information. This was mainly due to a perceived reluctance of NCSC in sharing classified or sensitive information.

Consequently, uncertainties related to the Security Act and insufficient guidance from NSA and NCSC were found to undermine CSIS. NSA and NCSC were also critiqued for not having a clear mission statement - resulting in a loss of confidence and perceived relevance for informants in higher management echelons in particular. Former empirical research also found that lack of a clear mandate challenged information sharing as it affected the relevance of shared information [30]. Additionally, NSA was also criticized for taking the role as the focal coordinating entity toward the national services, even in matters in which they were not best suited to be so.

Despite the critique of NSA and NCSC, informants in sectors where a formal SREs existed were highly positive of having this coordinating entity, whereas informants in sectors lacking a SRE underlined the need for one. In sectors lacking a formal SRE, two intermediate solutions were present: either leading organizations took the "SRE responsibility" upon themselves, or separate SRE equivalents were created by the sector community. The most valued responsibility for SREs or SRE equivalents were to collate, process and issue sector-specific assessments and guidance to aid subordinate undertakings in enhancing their security posture. Additionally, some SREs also aided subordinated undertakings in breach detection and recovery. The coordination and cooperation between SREs were also perceived as good, whereas one informant stated that cross-sectoral meetings were conducted weekly between practitioners of the different SREs.

One major disadvantage of the SRE equivalents was a lack of access to NCSC and their information with limited disclosure, only intended for NCSC partners. However, bilateral or multi-lateral CSIS agreements between SREs and SRE equivalents were commonplace and was regarded as well-functioning and fruitful from all participating parties.

The study also revealed that cyber security professionals from both public and private sectors raised concerns regarding the classification process of critical assets and FNFs, in addition to a perceived lack of prioritization of individual vital undertakings. The study also found an apparent lack of harmonization between ministries and perceived insufficient competency in the individual ministries. Both findings resulted in a reduced general trust toward the government and national services, but as is later discussed, this interestingly did not have an major effect on the willingness to share CSI with the national services.

Incentives and legislature promoting CSIS There were significant differences in why public and private organizations engaged in CSIS. The most prevalent external reason for public undertakings' engagement in CSIS was requirements from superior organizations, laws or regulations (33% of public respondents), whereas only a fraction of the private respondents (3%) opted the same. In contrast, the majority of private organizations stated that cyber attacks on own or similar organizations was the prevailing reason for them engaging in CSIS. Even though this result was expected as in general, more public undertakings are subject to the Security Act and other legislature than private counterparts. As is later described in Section 6.2 Perceptions on CSIS in Norway, this is possibly interlinked with the perceived importance and usefulness of CSIS among similar organizations.

The majority of the participants (83%) perceived that CSIS strengthens the relationship with government agencies. However, respondents in the public sector expressed a stronger agreement than their private counterparts. Additionally, the value of access to government agencies was significantly more predominant among public organizations than private, whereas private organizations ranked access to other companies' CSI as more important. This perception was present in both the qualitative and quantitative findings. The results indicate that cyber security professionals in the private sector value access to other companies' CSI higher than access to that of the national services. The analysis indicate that the even though CSIS results in a strengthened relationship with government agencies, this does not necessarily lead to an increased quality and usefulness of CSIS. This is further linked with a perceived lack of openness, transparency and intimate cooperation on the national services' behalf.

Even though information originating from the national services was perceived as having low usefulness, it was regarded as of high confidence and was particularly used to address top management and other non-technical personnel within their organization. Interestingly, former empirical research reported the opposite, in which the participants perceived information stemming from national services to be of high quality [30]. Furthermore, national services was also the most prevalent organizations to which the participants shared information. In fact, more respondents answered that their organization shared CSI with national services (79%) than cyber security organizations (74%). The qualitative findings point toward two key reasons: the non-competitive nature between national services and private cyber entities, and a willingness and perceived importance of contributing to national security.

This assessment is further supported by examining the participants' engagement in CSIS: 33% of the respondents in the public sector stated that requirements from superior organization, laws or regulations was their organization's main external factor for engaging in CSIS, whereas only 3% of the respondents in private sector did the same.

Sharing restrictions and unmanageable information flows As previously described, the national services were highly critiqued for over-classification. The unclassified equivalent to security classifications is the information sharing control system Traffic Light Protocol (TLP). TLP was initially created to enable cyber security organizations in exchanging sensitive information while limiting the number of recipients, which was stated as an important incentive for enhancing CSIS in the related literature from Section 2.2 Empirical research on CSIS. While the use of TLP was widespread among the participants of this study, several informants elaborated on possible damaging aspects of TLP, namely TLP:RED. TLP:RED restricts information to the individual to which it is shared. The main critique was that this hinder the further use of received information and can lead to toxic subcultures within organizations based on individuals' networks rather than a shared common pool of knowledge. However, opposite perceptions on "for your eyes only" information were also present in the sample, as this information may be used to either direct the cyber security professionals to perform their own research and thus sanitize the non-releasable information through the use of releasable sources.

Interestingly, the findings indicate that even though cyber security professionals critique national services' over-classification, a comparative regime of sharing restrictions has been created in the unclassified domain by private actors. Whereas the the government-sanctioned classification regime bases access to information on criticality in supporting FNFs on a "need to know" basis, its private counterpart is based on personal networks and interpersonal trust. The analysis also showed that the combination of unsatisfactory timeliness and insufficient information sharing by the national services, in combination with the emergence of grass root private counterparts, had lead to unmanageable parallel sub-avenues of information to that of NCSC, leading to an even more unclear and challenging landscape for individual undertakings to navigate in.

Despite the national services' theoretically more functional information sharing controls - where those in need of certain information and has the necessary formalities gain access to said information - the difference between theory and practice was perceived as substantial. Almost all informants with valid security clearances either did not, or rarely received classified information which could've assisted them in enhancing their undertakings' security posture - even in situations where they knew the information existed in the JCCC on a shareable classification level. This was due to a perceived reluctance of the national services in sharing classified information with undertakings and organizations outside the government, also reported as a challenge and social barrier in former research [30].

6.2 Perceptions on CSIS in Norway

This section discusses and integrates the findings of Chapter 5 Results with former empirical research on CSIS described in Chapter 2 Related research. The section provides a comprehensive insight in how cyber security professionals perceive CSIS in Norway.

Neither the respondent's role, experience nor sector had a statistically significant impact on how CSIS was perceived among the respondents within each of the four factors: operational, organizational, economic and policy. Despite this, the analysis and integration of both the quantitative and qualitative data revealed significant differences on individual concepts related to CSIS. The same lack of statistically significant differences between participants' perceptions and their position and sector was also recorded in Zibak & Simpson [13].

However, the Norwegian cyber security professionals were generally more homogeneous and extreme in their responses in contrast to that found when examining attitudes toward CSIS among their British counterparts [13]. Possible explanations to this might be that the Norwegian cyber security community is smaller than the British resulting in a more homogeneous community as professional networks are more interlinked, or due to self-selection bias noted in Section 4.6 Considerations on validity, reliability and research ethics, as volunteers may be more motivated or interested in the studied problem, possibly leading to more extreme responses.

Improved security posture and situational awareness Cyber security professionals within the Norwegian cyber security community acknowledged the positive role of CSIS in improving both individual organizations' and the national security posture, and situational awareness. Even though the surveys were not aimed at measuring the correlation between the positive attitude toward CSIS improving security posture and situational awareness, and the reason for engaging in CSIS, the positive attitude toward improved national security posture and the security posture in organizations might be explained by the two most reported reasons for engaging in CSIS - *the geopolitical context and security situation* and *own or similar organizations targeted by cyber criminals*.

As was also found in prior empirical research [13] and theoretical literature, the majority of respondents agreed that CSIS supports incident response efforts, contributes to breach detection and recovery, and enhances defensive agility and resilience. As described above, the analysis revealed that CSIS has a positive effect on four out of five functions in the NIST Cyber Security Framework: *protect*, *detect*, *respond* and *recover* [144]. Since these functions contribute to a successful and holistic cyber security program [144], the high level of agreement among the participants on the above-mentioned benefits might explain the overall positive attitude toward CSIS contributing to enhanced national- and organizations' security posture.

However, the participants also expressed several negative attitudes toward national services' engagement in CSIS, i.e. over-classification, frequency of sharing, and perceived usefulness of shared information, as well as as access to other companies' CSI were ranked as more important than access to CSI from national services. Accordingly, the positive attitude about CSIS improving security posture and situational awareness might depend more on the undertakings' engagement in CSIS and the faith in own contributions and contributions by similar organizations, than the usefulness and tangibility of CSIS originating from the national services. Accordingly, bottom-up sharing and horizontal sharing among organizations were therefore assessed to be the prevailing reason for why CSIS improves national security, rather than the information received from national services.

Personnel shortages within the Norwegian cyber security community Approximately half of the respondents perceived that CSIS combats the shortage of cyber security skills and reduces duplicated information handling by coordinating analysis efforts and defensive measures. A possible explanation to this is the role and function of Sector Response Entities (SRE), which provide and support its members with situational awareness and incident response when cyber incidents occur. In addition to SREs, as described in Section 3.4 The Norwegian cyber security landscape, numerous private and public organizations also provide centralized comprehensive cyber security support to external organizations. Private security organizations offer Cyber Security As A Service (CSaaS), whereas public security organizations (e.g. SREs, NCIS) or the national services (e.g. NCSC) provide cyber security to a larger degree support on a push or pull basis, or in case of an increased threat level against Norwegian interests and state of security. Former research did however not find that CSIS reduces duplicated information handling [13], possibly explained by the national focus on cyber security during the last years in Norway and the development in security organizations as described above.

Even though the respondents perceived that CSIS combats cyber security skills shortage and reduces duplicated information handling, a significant concern was raised regarding the shortage of cyber security analyst with the required skills to actually handle shared CSI. Lack of skilled cyber security personnel or frequent personnel replacement, were also reflected on among the informants. Both SREs and competition between employers were mentioned as a challenge resulting in inadequate staffing within the Norwegian cyber security community. Some informants perceived that the expansion of SREs drain cyber security personnel from both enterprises and national services and might result in a lack of cyber security professionals with sector- or enterprise-specific knowledge from where they were perceived to be needed the most - at either enterprise level or within the national services. This further complicates the utilization, or sharing of relevant CSI, at the right place. Ultimately, this challenge may undermine the collective national cyber security posture in Norway. Retaining cyber security personnel in enterprises and centralizing the sector specific capacities in NSA were proposed as solutions to counter the personnel shortage, as these two entities are assessed to have the largest need for enterprise- and sector-specific competency and capacity. Centralizing all of the sector CERTs in NSA would also likely have improved the cross-sectoral effectiveness of CSIS, as they would utilize the same information system, be co-located and have the necessary security clearances. The other reason contributing to the lack of experienced cyber personnel in Norway was the competition between employers, resulting in frequent personnel rotation between organizations as well as difficulties in hiring adequately skilled personnel.

Quality of shared cyber security information Former empirical research on CSIS addressed the *quality of information* as an important incentive for engaging in CSIS [30]. The theory suggests that the quality of information depends on several properties such as *relevance*, *accuracy*, *timeliness*, *standardized terminology* and to what extent the information is *complementary or validates other sources of information*. Accordingly, perceptions toward all of these properties of CSIS were measured in order to examine the overall perceived quality of shared CSI.

Almost 60% of the respondents disagreed that CSIS results in redundant and irrelevant data. This does however not automatically imply that CSIS provides unique and relevant data. As discussed in Section 6.1 The state of CSIS in Norway, informants expressed critique toward the national services for not sharing all relevant information in their possession, which could have been used to enabled a more resilient cyber security posture on a national level. Several informants were of the impression that they did not receive information from the national services, even if they possessed the necessary formalities like adequate security clearances.

The analysis further suggests that the access to- and flow of CSI is extensive, which makes it hard to distinguish what is relevant to the individual organizations in due time. Accordingly, skilled and experienced cyber security personnel were found as highly essential and valued resources for organizations to actually utilize shared CSI, and humans, in addition to technical filters, will still constitute an important role in order to identify relevant information. Former empirical research on CSIS also emphasized that both technical measures such as information filtering, subscription functionalities in CTI sharing platforms [39, p. 1414], organizational factors such as clear mandates, in addition to mutually agreed procedures and structures [30] were necessary measures to ensure that relevant CSI is shared within information sharing communities [30].

The analysis also revealed that right type of personnel engaged in CSIS is essential to ensure that relevant information is shared and requested. This was exemplified by the absence of clear expectations and guidelines from NSA on what type of personnel to attend in the NCSC. Former research within the field also draw attention to this, as they found that inappropriate types of organizations or personnel represented within the same CTI sharing community might act as a barrier to information sharing, especially if there is a lack of a clear mandate ensuring relevant information to be shared among the participants [30][39, p. 1413].

Even though the participants had more positive attitudes toward the relevance of shared CSI than the theoretical literature proposed, a total of 62% expressed that determining the accuracy and quality, and ensuring timeliness of shared information are difficult. Findings in related research on CSIS also agreed on this [13]. Interestingly, a significant portion of the top managers expressed that it is difficult to assess the accuracy and quality of shared data, compared to that of middle managers and practitioners. A possible reason may be that top managers usually do not directly handle or process CSI, and their hands-on skills could therefore be outdated or absent. However, why top managers perceive it as more difficult to ensure timeliness than the other groups may be due to stricter performance requirements at that hierarchical level.

The analysis suggests that the structure and hierarchy of the Norwegian cyber security community involving NCSC and SREs, leads to ineffective reporting lines, and challenge the timeliness of CSIS. The large variety of communication means, and the lack of common guidelines and routines in which channels to use when engaging in CSIS efforts, were also mentioned as challenges toward information sharing and supported the perceived difficulty of both interoperability and automation in information sharing communities. These challenges were also addressed in former research to affect timely sharing of relevant and high-quality information [40].

As found in former empirical research within the field, sufficient *quality, value and usefulness of shared information* and timely information sharing were rated as important incentives for participating in information sharing efforts [30]. This could explain why some organizations might refrain from participating in CSIS and therefore explains that 13% of the respondents answered that their organization was not currently involved in CSIS (Figure 5.3).

Despite the common agreement among the participants regarding the challenge of evaluating the quality of shared CSI, almost three quarters still confirmed that CSIS both validates and complements other sources of information, indicating that organizations engaged in CSIS actually receive some relevant information from others.

Importance of personal relationships and professional networks Similarly with former empirical research [13], this study also found that the cyber security professionals perceived CSIS to extend and strengthen professional networks within the cyber security community. This was particularly expressed by professionals with less than two years of working experience, indicating that CSIS is an important incentive to recruit and develop inexperienced cyber security professionals, mitigating the previously described challenge on the shortage of skilled cyber security personnel.

There was a common understanding that personal relations facilitate information sharing within the cyber security community. Despite this, some also raised concerns about the emerging vulnerability if information sharing depends on personal relations between individuals rather than established procedures and structures between organizations. Such relations makes it hard to establish institutional knowledge and common utilization of shared information, where shared information is only available for the one receiving it, i.e. through the use of TLP:RED. Additionally, if information sharing depends on individuals, the sharing between organizations might cease if certain individuals resigns. The negative perception of dependencies on personal relations related to TLP:RED were commonplace within the cyber security community. However, personal relations were still regarded to provide important information, which made the recipient better equipped to make better assessments and further disseminate, even though the information can not be used directly in the reporting or revealed to other colleagues due to e.g. sharing restrictions. Personal relations were also perceived to be more efficient and less resource-demanding to establish than formal structures. Additionally, personal relations were positively regarded as the participants perceived that formalized agreements often starts with personal relations.

As demonstrated, both social and formal structures are important to facilitate CSIS. Fruitful professional networks are however dependent on trusted relationships between individuals. Fortunately, cyber security professionals in Norway, similarly with the professionals in the UK [13], did not find it challenging to establish trust with others in the cyber security community. This could be explained by the relatively small size of the Norwegian cyber security community, resulting in few national arenas (e.g. security conferences) to attend in, leading to regularly meetings between cyber security professionals and the proliferation of interpersonal relationships. Several participants in the study had extensive prior experience across both public and private sectors, and national services, thus possibly leading to an increased cooperation and trust between different organizations. However, as depicted in Section 6.1 The state of CSIS in Norway, there are still challenges with information sharing from governmental entities, particularly national services, to external entities in both private and public sector. Trust was mentioned to be one of the reasons for the perceived low degree of information sharing from national services to other entities, even though several individuals in external entities have valid security clearances. The culture of secrecy was also found as a barrier to information sharing in former empirical research within the field [30].

Despite that both over-classification and over-sanitization was reported as major issues among the participants, all informants which to some extent were content with the information provided by the national services, stated that trust was essential, and that this trust was built upon long-term cooperation.

Even though the quantitative analysis suggested that middle managers and practitioners were less concerned about establishing trust among participants attending in CSIS efforts than top managers, this was not evident in the qualitative sample.

Furthermore, several informants were of the opinion that trust is established by sharing information, and that the level of trust established between entities depends on the importance of the information you share. However, some organizations were still reluctant to share information about own vulnerabilities or cyber incidents. This might be due to the fear of reputational loss caused by sharing sensitive information, which was found as an important barrier to information sharing in previous studies [30][39, p. 1415]. If the environment was perceived as safe, the participants were positive to share sensitive CSI, which was in accordance with the related research. The literature associated safe environments with strong management, participants of appropriate personnel categories, and not too many participants [30], whereas important factors stressed by the participants in this study included mutual understanding of each other's role, security culture (e.g. how shared information is handled and processed at the receiving part), and organizational type of the receiver. Governmental organizations were regarded as safer to share information with than private organizations due to the automatically higher degree of trust placed in governmental entities.

Even though the literature proposed a loss of clients' confidence and satisfaction as a challenge to CSIS, the majority of the respondents disagreed. About 60% either disagreed or strongly disagreed that sharing of CSI reduces clients' confidence in the organizations that shares information with others. Interestingly, a prior study on perceptions of UK cyber security professionals noted this as a major concern [13].

This study found that economic and reputational concerns were still raised regarding disclosing sensitive CSI, as this can affect stock prices or damage the reputation of the sharing enterprise or clients of the sharing entity. These perceptions were also reflected in related research [30][39, p. 1415]. In this study, these opinions were only present in relation to going public in the media, and not when sharing CSI within the cyber security community under sharing restrictions. Even though CSI often emerge from detected attacks or exploited vulnerabilities which has potential negative consequences to e.g. the undertakings' stock prices and reputation, some informants also saw positive effects in being transparent and open about encountered cyber attacks, as this could both contribute to defensive agility and resilience-, establish trust between organizations, and support future security investments in other organizations.

Around half of the respondents and several informants also acknowledged that privacy and antitrust legal concerns challenge CSIS. Even though some were concerned about sharing information that affects the privacy of customers and employees, others were more confident in that they manage to filter out such information, as it was regarded as irrelevant. Accordingly, the maturity of the undertaking might reduce the challenges related to privacy concerns.

Consequently, the analysis has shown that differentiated meanings exists within the Norwegian cyber security community regarding reputational effects of CSIS.

Cost savings and security investments As the literature suggests, this study found that CSIS contributes to decrease the uncertainty associated with cyber security investment decisions, and cost savings (Table 2.1). The analysis supported that CSIS assists decisions-makers in security investment decisions, as shared CSI provides knowledge about existing threats and vulnerabilities which can be used to develop or acquire proper protective security measures.

Cyber security personnel in private organizations were generally more negative to economic benefits stemming from CSIS engagement than personnel in public organizations. The private and public cyber security professionals had opposing opinions when they were asked to agree upon whether CSIS reduces overall cyber security costs or not. The personnel in public sector were positive to that CSIS reduces costs, whereas private employees were not. With respect to the expensiveness of establishing CSIS infrastructure, private cyber security professionals were still more negative than those in the public sector, even though the analysis did not clearly indicate a strong agreement or disagreement to it. However, the qualitative findings indicate that CSIS' contribution to reducing costs and support decision-making are dependent on the undertaking's maturity within cyber security.

Former empirical research found that cost savings was perceived as the most important incentive for engaging in CSIS [30]. A significant portion of respondents from the private sector disagreed that CSIS recuses costs, which represent a reason why some private undertakings refrain to engage in CSIS.

6.3 The usefulness of CSIS and the willingness to share

While Section 6.1 The state of CSIS in Norway discussed how CSIS was performed in Norway and Section 6.2 Perceptions on CSIS in Norway presented key findings related to the perceptions of professionals within the cyber security community, this section describes the perceived usefulness of the CSIS categories and perceptions on willingness to participate in CSIS efforts.

Usefulness - comprehensiveness versus tangibility The results from the questionnaire showed that participants generally found expertise sharing as the most useful CSIS category, whereas knowledge sharing and alerts & triggers for action were perceived second and third most useful. When examining differences between the participants' roles, the quantitative findings indicated that top and middle management perceived data sharing and alerts & triggers for action as most useful, while practitioners were more positive toward knowledge and expertise sharing. This was in direct contradiction to that of the qualitative findings: the informants in top and middle management were generally more concerned of having a broader understanding of the threat landscape, whereas practitioners were more concerned with data sharing and alerts & triggers for action. However, several top and middle managers emphasized that all categories were part of *one* process - if short on resources, they would be more selective in which incidents they focused on, rather than solely prioritizing one category over another. Practitioners, on the other hand, emphasized the face value and tangibility of especially alerts & triggers for action, which directly assisted them in protecting their undertaking.

The differences were also linked to the maturity of the organization, where focusing on more technical data (e.g. data sharing and alerts & triggers for action) was regarded as less mature than engaging in the more comprehensive exchange of knowledge and expertise. The latter was seen as a force multiplier and enabled mature organizations of making better choices both in terms of preventative measures, detection and response.

As suggested by the analysis, the participants did not agreed to what type on information they perceived as the most useful. This was also reported in former research, in which participants regarded both quantitative information (data sharing and alerts & triggers for action) and qualitative information (knowledge and expertise) as important to increase the value of CSIS [39, p. 1415].

Willingness - cost-effectiveness, automation and trust The study also explored the participants' willingness to engage in CSIS, both in term of the general willingness and whether they were more inclined to share some information over other, and to whom. As described in Section 6.1 The state of CSIS in Norway, the respondents were most willing to share information with national services, followed by cyber security organizations and to organizations similar to their own. The analysis showed that respondents from organizations in the public sector had a stronger inclination to share CSI than their private sector counterparts, and the participants in top and middle management were generally most inclined to share knowledge and expertise.

However, one key takeaway from the informants was that the willingness to share CSI was predominantly based on cost-effectiveness assessments and available resources. This finding is interesting as there were several off-the-shelf automated solutions to share data or alerts & triggers, of which several of the participants' organizations currently used such automated solutions. As discussed in the sample description, the majority of the respondents (61%) were in the private sector. Combined, these factors possibly indicate two underlying causal relationships: the proliferation of automated CSIS systems distances the top and middle management from the detailed flow of information making it almost subconscious and out of mind, and that knowledge and experience sharing is perceived as more mature - even though alerts & triggers for action was stated as the category with the highest tangibility by itself. Thus, it is possible that top and middle managers perceive the usefulness in light of feelings and non-factual perceptions, rather than what is assessed as being most cost-effective.

Furthermore, organizations' willingness to share CSI was found to be dependent on the understanding of how it benefits themselves, the sector and other external entities. The willingness to share certain information was reported to depend on trust, and whether organizations understand that sharing sensitive and valuable information often results in receiving valuable information in return. As reported in former research, trusted environments were also perceived as a prerequisite for engaging in CSIS [30] and sharing sensitive information [39, p. 1415].

6.4 Improvements to the study

During the research process, the authors experienced several areas in which the study could have been improved. One of the most notable experiences was the sampling process: Due to time restraints and what the researchers perceived as the most efficient way to sample information, it was decided not to perform a phased study in which the quantitative sampling and processing were performed before the qualitative sampling. If this had been done, the qualitative sampling could have been more directed toward elaborating the quantitative findings. This could also have led to shorter individual interview sessions, significantly reducing the time spent processing the qualitative data. With the used method, the informants were free to emphasize and elaborate on the topics *they* chose, only loosely directed by the researchers. This resulted in some interviews lasting up to three hours, with significant time spent transcribing and analyzing the data. However, the method was chosen intentionally as a measure to counteract the introduction of biases and satisficing due to the researchers' active efforts in leading the informants to answer predefined problems and experiences, which they may not perceive as important or relevant.

With regards to the questionnaire, several areas for improvement were also identified. Some were identified during the analysis by the researchers themselves, others were given by the respondents themselves in the *Feedback & comments* section of the questionnaire. This was a voluntary part of the questionnaire intended to enable the respondents in giving useful information which could improve the questionnaire itself, or aid the researchers in the following analysis. This feedback provided a more profound insight into how the questionnaire may be improved from both the researchers' and the respondents' perspective.

A major area for improving the study is to give further consideration to the use of close-ended questions. They were extensively implemented to counter response fatigue by being easy and quick to answer, while still having a relatively high degree of measurement accuracy. Shortening the questionnaire was also one of the researchers' main concern due to previously stated reasons. Despite these efforts, some respondents stated that the questionnaire was too long which strained the concentration and may have affected the integrity of the data. Also, a more comprehensive pilot with a larger sample should have been conducted before disseminating the questionnaire, as some questions should have either been voluntary (it was mandatory to answer all questions), or having a higher degree of alternatives with "not applicable" or similar characteristics. Another familiar disadvantage with close-ended questions is the loss of expressiveness. This might introduce errors as the respondent is forced to choose between an incomplete list of choices, making the respondent focus on alternatives that might not had occurred to them naturally [75, p. 114]. Research on questionnaires suggests that all closed-questions initially should be open-ended questions included in a pilot questionnaire in order to derive pertinent answer options that actually reflect the variety of answers from the population under investigation [75, p. 129]. However, this possible source of error was not sufficiently taken into account when the questionnaire was designed and tested due to time restrictions.

A more thorough and profound pilot questionnaire could also have enabled the researchers to transform some closed-ended questions into more suited open-ended alternatives. The pilot study could also have been used to ask open-ended questions to identify suited response alternatives on which to base the close-ended questions on [75, p. 116-117]. Open-ended questions were originally not included in the questionnaire in order to avoid collecting irrelevant information and reducing the overall workload by simplifying the data sets.

Additionally, several questions required a certain level of maturity and background knowledge on behalf of the respondents. Some examples of such questions were "Why did your organizations engage in CSIS" and "If your organization is not participating in any cyber security organizations, state the most relevant reason why". These questions required comprehensive knowledge on behalf of the respondent, and may have led to a lowered integrity of the results. Another possible improvement is better tailoring the questionnaire for reflecting the impact of automated CSIS technology and CSaaS. As was reflected upon in the feedback section of the questionnaire, many undertakings purchase cyber security services from either vendors or as an integrated part of cloud solutions. As a result, this could e.g. lead some respondents to answering that they did not participate in CSIS even though they did and vice versa.

Another improvement which could have been done was to further provide definitions and descriptions to part 4 - Attitudes toward CSIS. Whereas each CSIS category was adequately defined, no guidance on how to interpret e.g. "useful" was provided - it was not specified to whom the information was useful for, thus possible introducing errors as some interpreted this as the usefulness of received information, while others answered based on what they perceived most beneficial for them when *sharing*.

Even though some of the statements in the questionnaire's part 3 - *Perceptions on CSIS* were rephrased to make them more understandable for non-native English speakers, more effort could had been placed in considering translating the statements into Norwegian. This might have led to an increased response rate, as some might have refrained from participating due to language barriers. However, the researchers decided not to translate the statements to avoid introducing errors when translating the findings back into English, and to ensure a more unbiased comparison of the findings in this study and in the research of Zibak & Simpson [13][37]. Despite this, if the aim was to only examine the perceptions within the Norwegian cyber security community without any direct comparison with other countries' cyber communities, translating the questionnaire into Norwegian would be further considered.

Furthermore, as done in part 4 - Attitudes toward CSIS, explanation to the statements could have been provided in order to increase the internal validity. However, this was not done as it would have significantly increased the length of the questionnaire, increasing the risk of in response fatigue. Despite this, clarifying and exemplifying the statements should be considered if future studies on examining perceptions of cyber professionals are to be conducted. Additionally, more suited and extreme scale ranges for measuring willingness and usefulness should have been used, e.g. "useless" to "useful" and "unwilling" to "willing", in contrast to e.g. least willing - most willing.

Conclusion

This thesis examined why Norwegian organizations engage in Cyber Security Information Sharing (CSIS) by exploring how CSIS was performed in Norway, how cyber security professionals perceived it, and what affected the perceived usefulness and willingness in sharing Cyber Security Information (CSI). Previous research on the area is limited, of which most originates from theoretical research, white papers, legislation, standards, and guidelines. Additionally, almost every identified empirical research related to CSIS were conducted outside Norway, and had insufficiently representative samples based on the target population.

The thesis used a mixed methods approach to achieve triangulation and elaboration on the perceptions of Norwegian cyber security practitioners, middle and top managers from a representative sample of the Norwegian cyber security community. The vast majority of organizations were already engaged in CSIS. This thesis found that private and public organizations had varied reasons for engaging in CSIS: Whereas public organizations engaged in CSIS both due to superior requirements and regulations, and to develop or maintain relationships with government agencies, their private counterparts mainly participated in order to gain access to the Cyber Security Information (CSI) of similar undertakings as their own. The underlying factors leading to CSIS were found to be robust and heavily influenced by a sense of mutual benefit toward increasing each participating individual undertakings' security posture, and a willingness to contribute to national security.

As also found in prior research, the mutual exchange of CSI was found to give organizations access to information which otherwise would have been unavailable, effectively enabling the individual organizations and the cyber security community as a whole in increasing their security posture.

The Norwegian authorities were heavily criticized in a number of areas: the national services' dissemination of low-value information due to perceived oversanitization, over-classification and insufficient timeliness, the current Norwegian Sector Response Entities (SRE) model which was perceived to contribute to increasing the shortage of skilled cyber security personnel by decentralizing and duplicating functions, and a lack of harmonization in the Fundamental National Functions (FNF) classification process across ministries. Due to the aforementioned critique of the national services, bottom-up sharing and horizontal sharing among similar organizations were assessed as the prevailing reason for why CSIS is assessed to improve national security, rather than the information sharing efforts from the national services.

Several challenges regarding the implementation of the Security Act and SRE model were identified. Even though the the study revealed general positive perceptions on the Security Act and the SRE model, most perceived that the current practice was sub-optimal compared to the intent of the Security Act and the creation of Norwegian National Cyber Security Centre (NCSC). Specific challenges were raised regarding the decentralized FNF identification process, lack of competency in certain ministries, lack of supervision from both National Security Authority (NSA) and the ministries, and the lack or insufficient prioritization of undertakings in cyber security matters. The uncertainty related to how NSA and NCSC prioritize their support to the different sectors and undertakings had a disincentivizing effect on some informants in sharing CSI with NCSC, in favor of focusing their cyber security resources on strengthening themselves. Additionally, almost all informants in undertakings subjected to the Security Act and with security clearances, did not perceive that being subjected led to greater access to information. This was mainly due to a perceived reluctance of NCSC in sharing classified or sensitive information.

The findings also indicate that the structure and hierarchy of the Norwegian cyber security community involving NCSC and SREs leads to ineffective lines of communication, which challenge the timeliness and distribution of CSIS. The large variety of communication channels combined with a lack of common guidelines and routines in which channels to use when engaging in CSIS efforts, were perceived as challenges toward information sharing, and supported the perceived difficulties of both interoperability and automation in information sharing communities. Consequently, this study argues that uncertainties related to the Security Act and insufficient guidance from NSA and NCSC undermine CSIS in the Norwegian cyber security community. Additionally, NSA and NCSC were also perceived as not having a clear task and purpose, as well as striving to be *the* focal coordinating entity toward the national services, even in matters in which they were not the best suited entity to be so. This resulted in a loss of confidence and perceived relevance for informants in higher management echelons in particular.

However, the SRE model itself was highly acclaimed, to a degree where sectors not having an government-appointed SRE created their own SRE equivalents. The most valued function of SREs was the collation, processing and dissemination of sector-specific assessments, aiding subordinated undertakings in enhancing their security posture.

The study also revealed a strong positive perception regarding the importance of trust and interpersonal relationships in facilitating information sharing. Even though these relationships had several negative connotations, e.g. vulnerabilities through creating dependencies on individuals and unnecessary sharing restrictions through the use of TLP:RED, making it difficult to establish institutional knowledge and common utilization of shared information, they were also regarded as highly beneficial. They were perceived to make the recipient better equipped to make better assessments, even though the information could not be used directly in further reporting or shared with other colleagues due to sharing restrictions. Additionally, personal relationships were perceived to be more cost-efficient and less resource-demanding to establish than formal structures, while often being perceived as the first stepping stone toward a formalized agreement between two undertakings.

Even though CSIS was perceived to combat cyber security skills shortage and reducing duplicated information handling, a significant concern was found related to a shortage of cyber security analyst with the required skills to actually handle shared CSI. Both SREs and competing recruiting efforts between employers were mentioned as a challenge resulting in inadequate staffing within the Norwegian cyber security community. The current SRE model was perceived to increase the shortage, as it drains available applicable personnel from both national services and the undertakings themselves. Ultimately, this challenge may undermine the collective national cyber security posture in Norway. Retaining cyber security personnel in enterprises and centralizing the sector specific capacities in NSA were proposed as solutions to counter the personnel shortage, as these two entities were assessed to have the largest need for enterprise- and sector-specific competency and capacity. This solution would also likely result in improved cross-sectoral effectiveness and cooperation, as they would utilize the same information system, be co-located and have the necessary security clearances. The other key factor contributing to a lack of experienced cyber personnel in Norway was competition between employers, resulting in frequent personnel rotation across organizations as well as difficulties in hiring sufficiently skilled personnel.

This study also examined which CSIS category was perceived as most useful, in addition to the Norwegian cyber security community's willingness to share CSI. Interestingly, the quantitative and qualitative findings contradicted each other - whereas the quantitative results indicated that top and middle managers perceived the arguably more technical information categories (data sharing and alerts & triggers for action) as most useful, the practitioners preferred the more comprehensive categories (knowledge and expertise sharing). The preferences were opposite in the qualitative results - possibly indicating sampling errors. In the qualitative findings, top and middle managers were more concerned in having a broader understanding of the threat landscape, whereas practitioners found data sharing and alerts & triggers for action as most useful due to their tangibility and face value.

With regards to the willingness to share CSI, organizations in the public sector had a stronger inclination to share CSI than their private counterparts. The willingness to participate in CSIS was predominantly based on cost-effectiveness assessments and only limited by available resources, as all participants were highly positive in participating in CSIS to the extent they were able to.

7.1 Recommendations

Even though this thesis is descriptive and was not aimed at presenting normative recommendations, the basis for providing certain recommendations was evident in the presented findings. These recommendations should be regarded as a basis on which further consideration should be placed before initiating implementations.

Increasing the degree of transparency between NCSC and SREs As the findings indicated a strong preference for over-classified information over over-sanitized information, the researchers' recommend that NSA to a larger extent invite representatives with adequate formalities (e.g. security clearances and authorizations) from the SREs in discussions on preliminary assessments and unfinished analyses. In this way, a mutually beneficial cooperation may take place between the NSA, other national services and the SREs. While the SRE representatives would gain a broader access to relevant and timely information, the NSA would benefit from utilizing the representatives' sector-specific knowledge, enabling the national services in providing assessments and measures with greater effectiveness and accuracy. This would also avoid increasing the existing shortage of cyber security personnel. Additionally, the recommended measure would also contribute in increasing the speed in which trust between private and private organizations, and the national services develop, thus indirectly enhancing the national security posture.

Formalization of agreements This study revealed both strong positive and some negative aspects regarding the importance and dependency on trust and interpersonal relationships in facilitating information sharing. The researchers recommend that undertakings prioritize the formalization of information sharing agreements, as this would counteract challenges related to information sharing restrictions, such as the use of TLP:RED, in addition to possibly reducing challenges in sharing data sets containing personal data. Formalized agreements would also enable increased cooperation and building of trust between undertakings.

Homogenization of personnel present in NCSC The current perception of Norwegian cyber security personnel is that NCSC is not working as intended, partly due to the different expectations of the personnel present in the centre. The researchers assess that the perception of NCSC and undertakings' willingness to prioritize cooperation would greatly increase by implementing the following actions:

1. stating the intent and purpose of NCSC, in addition to what kind of interaction is expected between NCSC and present undertakings,
2. providing requirements for participants' personnel category and skills required, and
3. increasing cooperation and transparency in ongoing incidents and cases.

Endorsement and consolidation of existing communication channels To counteract the proliferation of extensive and unmanageable communication channels, the NSA and NCSC should endorse and consolidate existing communication channels. It would also help ensure that the information which is relevant to certain undertakings, actually reaches them. Additionally, requirements for e.g. the confidence and degree of processing of shared information could be stated, increasing the degree of tangibility and usefulness of information shared. By this, the general flow of CSI would be easier to manage and utilize, especially for undertakings which are less mature in cyber security.

7.2 Future work

The researchers intends this study to serve as an initial step in examining and improving CSIS within the Norwegian cyber security community. During the data collection several interesting considerations related to CSIS were brought up by the informants. However, due to limitations in scope and extent of this thesis, several of these aspects related to CSIS where not further examined. With this in mind, the researchers nominate four additional directions for future research on CSIS in Norway:

Effectiveness and quality of CSIS Even though this thesis found that Norwegian organizations were highly positive toward engaging in CSIS, it did not measure the de facto effectiveness and impact of CSIS. Even though CSIS is perceived as beneficial, it is highly relevant to examine whether and to what extent CSIS qualitatively improves the security posture of undertakings. The researchers propose that future studies develop tools of measurement and performs tests on organizations both prior to and after CSIS efforts are implemented. Research on this topic is also expected to provide specific recommendations regarding implementation of solutions and measures with the highest cost-efficiency, least prerequisites etc. to aid decision makers in improving their cyber security posture.

Cultural influence on CSIS The researchers propose that future research should be performed to examine the cultural influence on CSIS. As every individual organization has its own unique culture and naturally is expected to influence all matters of business, it is highly relevant to examine how different organizational cultures influence the organizations' and individual cyber security professionals' attitudes and engagement in CSIS. Cultures in both private and public organizations, as well as in national services should be examined. A proposed aim for this research would be to disclose properties of those cultures positively contributing to CSIS and properties of cultures that obstruct or hinders CSIS. Such findings may be utilized in several aspects: from security managers to both recruit employees that matches the cultural properties, streamlining and enhancing positive traits when developing and maintaining the organizational culture in cyber security communities, or to establish more effective CSIS partnerships.

Organizations refraining from engaging in CSIS Based on the quantitative findings, some of the organizations did not engage in CSIS efforts. The underlying reasons why some organizations refrain from engaging in CSIS were not examined in this study, even though the study did not deliberately exclude non-participants in CSIS. Future research should target sampling among those organizations not participating in CSIS to identify underlying disincentivizing factors, which could lead to targeted efforts from e.g. national services in order to promote CSIS.

Board of directors and C-level management attitudes toward CSIS As this thesis was limited to examining perceptions and attitudes of cyber security professionals (including Chief Security Officer or Chief Information Security Officer), perceptions of decision makers not directly involved in CSIS (e.g board of directors and C-level management) toward CSIS were not examined. Theoretical literature also propose that lack of top management endorsement poses a challenge toward CSIS (Table 2.1). As the understanding and attitudes of this personnel directly impacts an undertakings' cyber security efforts through e.g. allocation of resources, future research should be conducted to examine such personnel's understanding and perceptions of CSIS.

Bibliography

[1] E. Luiijf and A. Kernkamp, *Sharing Cyber Security Information*. Mar. 31, 2015. DOI: 10.13140/RG.2.1.4321.7442.

[2] Forsvarsdepartementet. “NOU 2016: 19,” Regjeringen.no. Publisher: regjeringen.no. (Oct. 12, 2016), [Online]. Available: https://www.regjeringen.no/no/dokumenter/nou-2016-19/id2515424/ (visited on 07/19/2022).

[3] NSM. “Rammeverk for håndtering av IKT-hendelser - Nasjonal sikkerhetsmyndighet,” nsm.no. (Jun. 24, 2020), [Online]. Available: https://nsm.no/regelverk-og-hjelp/andre-publikasjoner/rammeverk-for-handtering-av-ikt-hendelser/ (visited on 05/19/2022).

[4] NSM, “Digitale verdikjeder og avhengigheter,” Norwegian National Security Authority, Oslo, Risik assessment, Sep. 21, 2020. [Online]. Available: https://nsm.no/regelverk-og-hjelp/rapporter/helhetlig-digitalt-risikobilde-2020/det-digitale-risikobildet/digitale-verdikjeder-og-avhengigheter/ (visited on 08/02/2022).

[5] NSM. “Varsel om russiske trusler mot kritisk infrastruktur,” nsm.no. (Apr. 21, 2022), [Online]. Available: https://nsm.no/aktuelt/varsel-om-russiske-trusler-mot-kritisk-infrastruktur (visited on 05/07/2022).

[6] “Risiko 2022 - Økt risiko krever økt årvåkenhet,” NSM, Sandvika, Risk assessment, 2022. [Online]. Available: https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf (visited on 05/07/2022).

[7] NSM. “Sikkerhetsloven og forskrifter.” (Jun. 10, 2020), [Online]. Available: https://nsm.no/regelverk-og-hjelp/sikkerhetsloven-og-forskrifter/ (visited on 07/20/2022).

[8] “Risiko 2021 - helhetlig sikring mot sammensatte trusler,” NSM, Risk assessment, Mar. 11, 2021. [Online]. Available: https://nsm.no/aktuelt/risiko-2021-helhetlig-sikring-mot-sammensatte-trusler (visited on 05/08/2022).

[9] K. B. Sandvik, “Cyberkrig og internasjonal rett,” *Internasjonal Politikk*, vol. 71, no. 2, pp. 252–262, May 15, 2013, ISSN: 1891-1757, 0020-577X. DOI: 10.18261/ISSN1891-1757-2013-02-08. [Online]. Available: https://www.idunn.no/ip/2013/02/cyberkrig_og_internasjonal_rett (visited on 05/08/2022).

[10] R. Johnsen, "Cyberkrigføring og forsvarets operative evne," *Internasjonal Politikk*, vol. 71, no. 2, pp. 241–251, Publisher: Universitetsforlaget. DOI: 10.18261/ISSN1891-1757-2013-02-07. [Online]. Available: https://www.idunn.no/doi/10.18261/ISSN1891-1757-2013-02-07 (visited on 05/08/2022).

[11] KMD, *Digitalisering i offentlig sektor*, Brev, Publisher: regjeringen.no, Feb. 1, 2021. [Online]. Available: https://www.regjeringen.no/no/dokument/dep/kdd/andre-dokumenter/brev/utvalgte_brev/2021/digitalisering-i-offentlig-sektor/id2830849/ (visited on 05/08/2022).

[12] M. Fleming, E. Goldstein, and J. K. Roman, "Evaluating the impact of cybersecurity information sharing on cyber incidents and their consequences," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper 2418357, Mar. 31, 2014. DOI: 10.2139/ssrn.2418357. [Online]. Available: https://papers.ssrn.com/abstract=2418357 (visited on 05/27/2022).

[13] A. Zibak and A. Simpson, "Cyber threat information sharing: Perceived benefits and barriers," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, ser. ARES '19, New York, NY, USA: Association for Computing Machinery, Aug. 26, 2019, pp. 1–9, ISBN: 978-1-4503-7164-3. DOI: 10.1145/3339252.3340528. [Online]. Available: https://doi.org/10.1145/3339252.3340528 (visited on 04/05/2022).

[14] CSRIC, "Cybersecurity information sharing working group barriers report," presented at the Reliability The Communications Security and Interoperability Council, Jun. 2016, p. 9. [Online]. Available: https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG5_Info_Sharing_Report_062016.pdf.

[15] N. E. Weiss, "Legislation to facilitate cybersecurity information sharing: Economic analysis," *Economic Analysis*, p. 19,

[16] B. Woods, S. J. Perl, and B. Lindauer, "Data mining for efficient collaborative information discovery," in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, Denver Colorado USA: ACM, Oct. 12, 2015, pp. 3–12, ISBN: 978-1-4503-3822-6. DOI: 10.1145/2808128.2808130. [Online]. Available: https://dl.acm.org/doi/10.1145/2808128.2808130 (visited on 10/07/2022).

[17] D. Shackleford, "Cyber threat intelligence uses, successes and failures: The SANS 2017 CTI survey," SANS, 2017, p. 19.

[18] R. Brown and P. Stirparo, "SANS 2022 cyber threat intelligence survey," SANS, Feb. 23, 2022.

[19] L. O. Nweke and S. Wolthusen, "Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection," in *2020 12th International Conference on Cyber Conflict (CyCon)*, ISSN: 2325-5374, vol. 1300, May 2020, pp. 63–78. DOI: 10.23919/CyCon49761.2020.9131721.

[20] C. S. Johnson, M. L. Badger, D. A. Waltermire, J. Snyder, and C. Skorupka, "Guide to cyber threat information sharing," National Institute of Standards and Technology, NIST SP 800-150, Oct. 2016, NIST SP 800–150. DOI: 10.6028/NIST.SP.800-150. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf (visited on 05/06/2022).

[21] T. Kokkonen, J. Hautamäki, J. Siltanen, and T. Hämäläinen, "Model for sharing the information of cyber security situation awareness between organizations," in *2016 23rd International Conference on Telecommunications (ICT)*, May 2016, pp. 1–5. DOI: 10.1109/ICT.2016.7500406.

[22] F. B. Schneider, E. M. Sedenberg, D. K. Mulligan, and IRGC, Eds., *Public Cybersecurity and Rationalizing Information Sharing*, International Risk Governance Center (IRGC), 2016. DOI: 10.5075/epfl-irgc-264007.

[23] V. Mavroeidis and S. Bromander, "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence," in *2017 European Intelligence and Security Informatics Conference (EISIC)*, Sep. 2017, pp. 91–98. DOI: 10.1109/EISIC.2017.20.

[24] C. Sillaber, C. Sauerwein, A. Mussmann, and R. Breu, "Data quality challenges and future research directions in threat intelligence sharing practice," in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, ser. WISCS '16, New York, NY, USA: Association for Computing Machinery, 2016, pp. 65–70, ISBN: 978-1-4503-4565-1. DOI: 10.1145/2994539.2994546. [Online]. Available: https://doi.org/10.1145/2994539.2994546 (visited on 04/06/2022).

[25] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "MISP: The design and implementation of a collaborative threat intelligence sharing platform," in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, Vienna Austria: ACM, Oct. 24, 2016, pp. 49–56, ISBN: 978-1-4503-4565-1. DOI: 10.1145/2994539.2994542. [Online]. Available: https://dl.acm.org/doi/10.1145/2994539.2994542 (visited on 10/28/2022).

[26] S. Murdoch and N. Leaver, "Anonymity vs. trust in cyber-security collaboration," in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, ser. WISCS '15, New York, NY, USA: Association for Computing Machinery, 2015, pp. 27–29, ISBN: 978-1-4503-3822-6. DOI: 10.1145/2808128.2808134. [Online]. Available: https://doi.org/10.1145/2808128.2808134 (visited on 04/12/2022).

[27] A. Mohaisen, O. Al-Ibrahim, C. Kamhoua, K. Kwiat, and L. Njilla, "Rethinking information sharing for threat intelligence," in *Proceedings of the fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies - HotWeb '17*, San Jose, California: ACM Press, 2017, pp. 1–7, ISBN: 978-1-4503-5527-8. DOI: 10.1145/3132465.3132468. [Online]. Available:

http://dl.acm.org/citation.cfm?doid=3132465.3132468 (visited on 10/28/2022).

[28] R. Garrido-Pelaz, L. González-Manzano, and S. Pastrana, "Shall we collaborate?: A model to analyse the benefits of information sharing," in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, Vienna Austria: ACM, Oct. 24, 2016, pp. 15–24, ISBN: 978-1-4503-4565-1. DOI: 10.1145/2994539.2994543. [Online]. Available: https://dl.acm.org/doi/10.1145/2994539.2994543 (visited on 04/08/2022).

[29] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions," *Computers & Security*, vol. 87, p. 101 589, Nov-19 Nov. 2019, Number: Nov-19 Publisher: Elsevier, ISSN: 01674048. DOI: 10.1016/j.cose.2019.101589. [Online]. Available: https://doi.org/10.1016/j.cose.2019.101589 (visited on 04/11/2022).

[30] N. Robinson and E. Disley, "Incentives and barriers to information sharing," ENISA, Report/Study, 2010. [Online]. Available: https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing (visited on 04/06/2022).

[31] L. A. Gordon, M. P. Loeb, and W. Lucyshyn, "Sharing information on computer systems security: An economic analysis," *Journal of Accounting and Public Policy*, vol. 22, no. 6, pp. 461–485, Nov. 2003, ISSN: 02784254. DOI: 10.1016/j.jaccpubpol.2003.09.001. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0278425403000632 (visited on 10/07/2022).

[32] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "The impact of information sharing on cybersecurity underinvestment: A real options perspective," *Journal of Accounting and Public Policy*, vol. 34, no. 5, pp. 509–519, Sep. 1, 2015, ISSN: 0278-4254. DOI: 10.1016/j.jaccpubpol.2015.05.001. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0278425415000423 (visited on 10/07/2022).

[33] M. Lee and J. Lee, "The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet," *Information Systems Frontiers - ISF*, vol. 12, Apr. 1, 2012. DOI: 10.1007/s10796-010-9253-1.

[34] E. Gal-Or, "The economic incentives for sharing security information," *Information Systems Research*, vol. 16, no. 2, pp. 186–208, 2005, Publisher: INFORMS, ISSN: 1047-7047. [Online]. Available: https://www.jstor.org/stable/23015911 (visited on 05/06/2022).

[35] K. E. Eichensehr, "Articles public-private cybersecurity," *Texas Law Review*, vol. 95, p. 72,

[36] K. H. Wilson, "Sharing securely within government: Best practices for facilitating interagency data science," p. 8, 2017.

[37] A. Zibak and A. Simpson, "Towards better understanding of cyber security information sharing," in *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, Jun. 2019, pp. 1–8. DOI: 10.1109/CyberSA.2019.8899697.

[38] B. A. Jackson, "How do we know what information sharing is really worth?: Exploring methodologies to measure the value of information sharing and fusion efforts," RAND Corporation, Jun. 18, 2014. [Online]. Available: https://www.rand.org/pubs/research_reports/RR380.html (visited on 04/07/2022).

[39] C. Sillaber, C. Sauerwein, A. Mussmann, and R. Breu, "Towards a maturity model for inter-organizational cyber threat intelligence sharing: A case study of stakeholders' expectations and willingness to share," presented at the Multikonferenz Wirtschaftsinformatik 2018 (MKWI '18), pp. 1409–1420.

[40] A. Brilingaitė, L. Bukauskas, A. Juozapavičius, and E. Kutka, "Overcoming information-sharing challenges in cyber defence exercises," *Journal of Cybersecurity*, vol. 8, Jan. 28, 2022. DOI: 10.1093/cybsec/tyac001.

[41] A. Zibak, C. Sauerwein, and A. C. Simpson, "Threat intelligence quality dimensions for research and practice," *Digital Threats: Research and Practice*, Aug. 26, 2021, Just Accepted, ISSN: 2692-1626. DOI: 10.1145/3484202. [Online]. Available: https://doi.org/10.1145/3484202 (visited on 05/04/2022).

[42] M. G. Jaatun, L. Bodsberg, T. O. Grøtan, and M. Elisabeth Gaup Moe, "An empirical study of CERT capacity in the north sea," in *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Jun. 2020, pp. 1–8. DOI: 10.1109/CyberSecurity49315.2020.9138865.

[43] JD, *Instructions for the ministries' work with civil protection and emergency preparedness*, Publisher: regjeringen.no, Sep. 1, 2017. [Online]. Available: https://www.regjeringen.no/en/dokumenter/instructions-for-the-ministries-work-with-civil-protection-and-emergency-preparedness/id2569693/ (visited on 07/26/2022).

[44] NSM. "Nasjonale sikkerhetsinteresser - Nasjonal sikkerhetsmyndighet." (Jan. 12, 2021), [Online]. Available: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnleggende-nasjonale-funksjoner-gnf/nasjonale-sikkerhetsinteresser/ (visited on 07/26/2022).

[45] JD, *Act relating to national security (security act) - lovdata*, Jan. 1, 2019. [Online]. Available: https://lovdata.no/dokument/NLE/lov/2018-06-01-24#KAPITTEL_1 (visited on 07/20/2022).

[46] DHS. “National critical functions - an evolved lens for critical infrastructure security and resilience,” cisa.gov. (Apr. 30, 2019), [Online]. Available: https://www.cisa.gov/sites/default/files/publications/national-critical-functions-overview-508.pdf (visited on 07/22/2022).

[47] CPNI. “Critical national infrastructure | CPNI,” Critical National Infrastructure. (Apr. 20, 2021), [Online]. Available: https://www.cpni.gov.uk/critical-national-infrastructure-0 (visited on 07/22/2022).

[48] NSM. “Nasjonalt cybersikkerhetssenter.” (May 14, 2020), [Online]. Available: https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/ (visited on 07/25/2022).

[49] U. K. Cabinet Office. “Public summary of sector security and resilience plans,” www.gov.uk/government/organisations/cabinet-office. (Jan. 12, 2017), [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/678927/Public_Summary_of_Sector_Security_and_Resilience_Plans_2017__FINAL_pdf___002_.pdf (visited on 07/21/2022).

[50] N. C. S. Centre. “CNI hub,” NCSC.gov.uk. (Jul. 21, 2022), [Online]. Available: https://www.ncsc.gov.uk/section/private-sector-cni/cni (visited on 07/21/2022).

[51] NSM. “Grunnleggende nasjonale funksjoner.” (May 28, 2020), [Online]. Available: https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-i-departementenes-identifisering-av-grunnleggende-nasjonale-funksjoner/grunnleggende-nasjonale-funksjoner/ (visited on 07/19/2022).

[52] NSM. “Veiledere og håndbøker til sikkerhetsloven.” (Jun. 2, 2020), [Online]. Available: https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/ (visited on 07/20/2022).

[53] NSM, *Håndbok i klassifisering*. [Online]. Available: https://nsm.no/getfile.php/136443-1619007576/Filer/Dokumenter/Veiledere/H%C3%A5ndbok%20i%20klassifisering%20%283%29.pdf (visited on 07/26/2022).

[54] S. Gajek, M. Lees, and C. Jansen, “IIoT and cyber-resilience,” *AI & SOCIETY*, vol. 36, no. 3, pp. 725–735, Sep. 1, 2021, ISSN: 1435-5655. DOI: 10.1007/s00146-020-01023-w. [Online]. Available: https://doi.org/10.1007/s00146-020-01023-w (visited on 07/27/2022).

[55] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer security incident handling guide : Recommendations of the national institute of standards and technology,” National Institute of Standards and Technology, NIST SP 800-61r2, Aug. 2012, NIST SP 800–61r2. DOI: 10.6028/NIST.SP.800-61r2. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (visited on 05/06/2022).

[56] NSM. “Veileder i verdivurdering av informasjon,” Veiledere og håndbøker til sikkerhetsloven. (Jun. 3, 2020), [Online]. Available: https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-i-verdivurdering-av-informasjon/innledning-1/ (visited on 08/21/2022).

[57] NSM. “Spørsmål og svar om klarering.” (Jul. 2, 2020), [Online]. Available: https://nsm.no/fagomrader/personellsikkerhet/sikkerhetsklarering/sporsmal-og-svar-om-klarering/ (visited on 11/21/2022).

[58] Regjeringen, “Prop. 1 S (2015–2016) - For budsjettåret 2016 under Forsvarsdepartementet,” The Norwegian Government, Jul. 10, 2015, p. 172. [Online]. Available: https://www.regjeringen.no/contentassets/10336d68c60e42bcb37d92a27b33 no/pdfs/prp201520160001_fddddpdfs.pdf (visited on 08/21/2022).

[59] FIRST, *Traffic light protocol (TLP) version 2.0*, Jan. 8, 2022. [Online]. Available: https://www.first.org/tlp (visited on 08/15/2022).

[60] Chatham House. “Chatham house rule,” chathamhouse.org. (), [Online]. Available: https://www.chathamhouse.org/about-us/chatham-house-rule (visited on 08/21/2022).

[61] EOS-utvalget. “EOS-utvalget,” EOS-utvalget. (), [Online]. Available: https://eos-utvalget.no/ (visited on 10/14/2022).

[62] JD and FD, “National Cyber Security Strategy for Norway,” Norwegian Ministeries, Oslo, Strategy, Jan. 30, 2019. [Online]. Available: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf (visited on 10/14/2022).

[63] *Prop. 97 L (2015–2016) Endringer i sikkerhetsloven (reduksjon av antall klareringsmyndigheter mv.)* Publisher: regjeringen.no, Apr. 15, 2016. [Online]. Available: https://www.regjeringen.no/no/dokumenter/prop.-97-l-20152016/id2483258/ (visited on 07/20/2022).

[64] E. Moyle. “CERT vs. CSIRT vs. SOC: What’s the difference?” TechTarget SearchSecurity. (Mar. 2021), [Online]. Available: https://www.techtarget.com/searchsecurity/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference (visited on 10/16/2022).

[65] CISA. “Defining computer security incident response teams | CISA.” (Jan. 24, 2007), [Online]. Available: https://www.cisa.gov/uscert/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams (visited on 10/16/2022).

[66] A. Harsch, S. Idler, and S. Thurner, “Assuming a state of compromise: A best practise approach for SMEs on incident response management,” in *2014 Eighth International Conference on IT Security Incident Management & IT Forensics*, May 2014, pp. 76–84. DOI: 10.1109/IMF.2014.13.

[67] ENISA. "Information sharing and analysis centers (ISACs)," European Union Agency for Cybersecurity (ENISA). (), [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing (visited on 10/16/2022).

[68] Telenor, "Digital Sikkerhet 2020 - de lange linjene," Telenor, Fornebu, Trusselrapport, Jun. 23, 2020. [Online]. Available: https://www.telenor.no/om/digital-sikkerhet/ (visited on 05/15/2022).

[69] JD, "Samfunnsikkerhet - Meld. St. 29 (2011–2012)," Norwegian Parliament, Stortingsmelding 29, Jun. 15, 2012, Publisher: regjeringen.no. [Online]. Available: https://www.regjeringen.no/no/dokumenter/meld-st-29-20112012/id685578/ (visited on 10/14/2022).

[70] JD and FD, "Tiltaksoversikt til nasjonal strategi for digital sikkerhet," Norwegian Ministeries, Oslo, Strategy, Jan. 30, 2019, p. 40. [Online]. Available: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/tiltaksoversikt---nasjonal-strategi-for-digital-sikkerhet.pdf.

[71] C. G. Thomas, *Research Methodology and Scientific Writing*. Springer Nature, Feb. 24, 2021, 620 pp., Google-Books-ID: UBwgEAAAQBAJ, ISBN: 978-3-030-64865-7.

[72] M. Amundsen and F. C. Sunde, "Master thesis project description - the impact of cyber security information sharing and its effect on national security," NTNU, Oslo, May 27, 2022.

[73] P. D. Leedy and J. E. Ormrod, *Practical Research: Planning and Design*, 11th. Essex, England: Pearson, 2016. [Online]. Available: http://www.jstor.org/stable/1318509?origin=crossref (visited on 05/27/2022).

[74] B. C. Choi and A. W. Pak, "A catalog of biases in questionnaires," *Preventing Chronic Disease*, vol. 2, no. 1, A13, Dec. 15, 2004, ISSN: 1545-1151. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1323316/ (visited on 05/25/2022).

[75] A. N. Oppenheim, *Questionnaire design, interviewing, and attitude measurement*, New ed. London ; New York : New York: Pinter Publishers ; Distributed exclusively in the USA and Canada by St. Martin's Press, 1992, 303 pp., ISBN: 978-1-85567-043-3 978-1-85567-044-0.

[76] L. R. Harris and G. T. Brown, "Mixing interview and questionnaire methods: Practical problems in aligning data," Publisher: University of Massachusetts Amherst. DOI: 10.7275/959J-KY83. [Online]. Available: https://scholarworks.umass.edu/pare/vol15/iss1/1/ (visited on 09/05/2022).

[77] A. Fontana and J. H. Frey, "The interview: From structured questions to negotiated text," in *Handbook of qualitative research*, vol. 2, 6 vols., Sage, 2000, pp. 656–672.

[78] D. Silverman, "Analyzing talk and text," *Handbook of qualitative research*, vol. 2, no. 0, pp. 821–834, 2000.

[79] D. Silverman, *Interpreting qualitative data*, Fifth edition. London: SAGE, 2014, 489 pp., OCLC: ocn903278597, ISBN: 978-1-4462-9542-7 978-1-4462-9543-4.

[80] J. W. Creswell, *Research design: qualitative, quantitative, and mixed methods approaches*, 4th ed. Thousand Oaks: SAGE Publications, 2014, 273 pp., ISBN: 978-1-4522-2609-5 978-1-4522-2610-1.

[81] V. Garousi, M. Felderer, and M. V. Mäntylä, "Guidelines for including grey literature and conducting multivocal literature reviews in software engineering," *Information and Software Technology*, vol. 106, pp. 101–121, Feb. 1, 2019, ISSN: 0950-5849. DOI: 10.1016/j.infsof.2018.09.006. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950584918301939 (visited on 04/06/2022).

[82] J. Healey, "Challenges to sharing," Atlantic Council, 2015, pp. 2–4. [Online]. Available: https://www.jstor.org/stable/resrep03611.5 (visited on 05/25/2022).

[83] A. M. Kanca and Ş. SAĞIROĞLU, "Sharing cyber threat intelligence and collaboration," in *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*, Dec. 2021, pp. 167–172. DOI: 10.1109/ISCTURKEY53027.2021.9654328.

[84] A. Zibak and A. Simpson, "Can we evaluate the impact of cyber security information sharing?" In *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, Jun. 2018, pp. 1–2. DOI: 10.1109/CyberSA.2018.8551462.

[85] L. Dandurand and O. S. Serrano, "Towards improved cyber security information sharing," in *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, ISSN: 2325-5374, Jun. 2013, pp. 1–16.

[86] F. Skopik, G. Settanni, and R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing," *Computers & Security*, vol. 60, pp. 154–176, Jul. 1, 2016, ISSN: 0167-4048. DOI: 10.1016/j.cose.2016.04.003. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404816300347 (visited on 04/06/2022).

[87] S. Brown, J. Gommers, and O. Serrano, "From cyber security information sharing to threat management," in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, ser. WISCS '15, New York, NY, USA: Association for Computing Machinery, 2015, pp. 43–49, ISBN: 978-1-4503-3822-6. DOI: 10.1145/2808128.2808133. [Online]. Available: https://doi.org/10.1145/2808128.2808133 (visited on 04/12/2022).

[88] N. Robinson, "Information sharing for cyber-security: Evidence from europe," Asan Institute for Policy Studies, 2013. [Online]. Available: https://www.jstor.org/stable/resrep08108 (visited on 05/25/2022).

[89] S. Solak and Y. Zhuo, "Optimal policies for information sharing in information system security," *European Journal of Operational Research*, vol. 284, no. 3, pp. 934–950, Aug. 1, 2020, ISSN: 0377-2217. DOI: 10.1016/j.ejor.2019.12.016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0377221719310197 (visited on 05/25/2022).

[90] D. Mann, S. S. Shapiro, and D. Bodeau, "Bilateral analysis of information sharing efforts: Determining the expected effectiveness of information sharing efforts," in *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security - WISCS '14*, Scottsdale, Arizona, USA: ACM Press, 2014, pp. 41–50, ISBN: 978-1-4503-3151-7. DOI: 10.1145/2663876.2663880. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2663876.2663880 (visited on 04/05/2022).

[91] J. R. Gil-Garcia, T. A. Pardo, and M. K. Sutherland, "Information sharing in the regulatory context: Revisiting the concepts of cross-boundary information sharing," in *Proceedings of the 9th International Conference on Theory and Practice of Electronic Governance*, Montevideo Uruguay: ACM, Mar. 2016, pp. 346–349, ISBN: 978-1-4503-3640-6. DOI: 10.1145/2910019.2910099. [Online]. Available: https://dl.acm.org/doi/10.1145/2910019.2910099 (visited on 04/08/2022).

[92] D. S. Sayogo and J. R. Gil-Garcia, "Understanding the determinants of success in inter-organizational information sharing initiatives: Results from a national survey," in *Proceedings of the 15th Annual International Conference on Digital Government Research - dg.o '14*, Aguascalientes, Mexico: ACM Press, 2014, pp. 100–109, ISBN: 978-1-4503-2901-9. DOI: 10.1145/2612733.2612739. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2612733.2612739 (visited on 05/25/2022).

[93] P. Koepke, *Cybersecurity information sharing incentives and barriers*, Cambridge, Jun. 2017.

[94] J. Żywiołek, J. Rosak-Szyrocka, and B. Jereb, "Barriers to knowledge sharing in the field of information security," *Management Systems in Production Engineering*, vol. nr 2 (29), 2021, ISSN: 2299-0461. DOI: 10.2478/mspe-2021-0015. [Online]. Available: http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-3a4f58d5-1800-4cbe-9f25-4300d741b231 (visited on 04/08/2022).

[95] C. Wilson, "Questionnaires and surveys," in *Credible Checklists and Quality Questionnaires*, C. Wilson, Ed., Boston: Morgan Kaufmann, Jan. 1, 2013, pp. 29–79, ISBN: 978-0-12-410392-4. DOI: 10.1016/B978-0-12-410392-4.00002-7. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780124103924000027 (visited on 11/08/2022).

[96] L. R. Gay, G. E. Mills, and P. W. Airasian, *Educational research: competencies for analysis and applications*, 10th ed. Boston: Pearson, 2012, 648 pp., OCLC: ocn710045202, ISBN: 978-0-13-261317-0.

[97] SSB. "11653: Employees and jobs, by sector, contents and quarter. statbank norway," SSB. (), [Online]. Available: https://www.ssb.no/en/system/ (visited on 09/17/2022).

[98] P. Pourkhomami. "Cybersecurity as a service: The pros & cons of outsourcing cybersecurity," Managed IT Services & Technology Consulting | OSIbeyond. (Mar. 19, 2021), [Online]. Available: https://www.osibeyond.com/blog/is-cybersecurity-as-a-service-csaas-enough-for-your-company/ (visited on 09/22/2022).

[99] SSB. "Classification of standard industrial classification." (), [Online]. Available: https://www.ssb.no/en/klass/klassifikasjoner/6 (visited on 06/08/2022).

[100] SSB. "12542: Employed persons. 4th quarter, by occupation, contents and year," SSB. (), [Online]. Available: https://www.ssb.no/system/ (visited on 09/09/2022).

[101] G. Dusek, Y. Yurova, and C. P. Ruppel, "Using social media and targeted snowball sampling to survey a hard-to-reach population: A case study," *International Journal of Doctoral Studies*, vol. 10, pp. 279–299, 2015, ISSN: 1556-8881, 1556-8873. DOI: 10.28945/2296. [Online]. Available: https://www.informingscience.org/Publications/2296 (visited on 09/20/2022).

[102] Y. Baruch and B. Holtom, "Survey response rate levels and trends in organizational research," *Human Relations*, vol. 61, pp. 1139–1160, Aug. 1, 2008. DOI: 10.1177/0018726708094863.

[103] T. Johnson and L. Owens, "Survey response rate reporting in the professional literature," *2003 Proceedings of the Section on Survey Methods, American Statistical Association*, Aug. 3, 2013.

[104] S. Rogelberg and J. Stanton, "Introduction: Understanding and dealing with organizational survey nonresponse," *Organizational Research Methods*, vol. 10, pp. 195–209, Apr. 1, 2007. DOI: 10.1177/1094428106294693.

[105] D. Jobber, J. Saunders, and V.-W. Mitchell, "Prepaid monetary incentive effects on mail survey response," *Journal of Business Research*, vol. 57, pp. 347–350, Feb. 1, 2004. DOI: 10.1016/S0148-2963(02)00385-5.

[106] D. Rose, S. Sidle, and K. Griffith, "A penny for your thoughts: Monetary incentives improve response rates for company-sponsored employee surveys," *Organizational Research Methods - ORGAN RES METHODS*, vol. 10, pp. 225–240, Apr. 1, 2007. DOI: 10.1177/1094428106294687.

[107] "Nettskjema - kunnskapsbasen - NTNU," NTNU Kunnskapsbasen. (), [Online]. Available: https://i.ntnu.no/wiki/-/wiki/Norsk/Nettskjema (visited on 05/25/2022).

[108] T. Aichner, M. Gruünfelder, Oswin Maurer, and D. Jegeni, *Twenty-five years of social media: A review of social media applications and definitions from 1994 to 2019*, in *Cyberpsychology, Behavior, and Social Networking*, vol. 24, 4 vols., Mary Ann Liebert, Inc., Sep. 4, 2021. DOI: 10.1089/cyber.2020.0134. [Online]. Available: https://www.liebertpub.com/doi/epdf/10.1089/cyber.2020.0134 (visited on 09/26/2022).

[109] *LinkedIn*, in *Wikipedia*, Page Version ID: 1112411488, Sep. 26, 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=LinkedIn&oldid=1112411488 (visited on 09/26/2022).

[110] M. Silic and A. Back, "The dark side of social networking sites:understanding phishing risks," *Computers in Human Behavior*, vol. 60, pp. 35–43, Jul. 2016, ISSN: 07475632. DOI: 10.1016/j.chb.2016.02.050. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0747563216301029 (visited on 09/26/2022).

[111] F. Fornes. "Jukseliste for gode LinkedIn-innlegg," LinkedIn. (Feb. 2022), [Online]. Available: https://www.linkedin.com/feed/update/urn:li:activity:6894909441649848320/?updateEntityUrn=urn%3Ali%3Afs_feedUpdate%3A%28V2%2Curn%3Ali%3Aactivity%3A6894909441649848320%29 (visited on 09/27/2022).

[112] S. E. Stemler, "A comparison of consensus, consistency, and measurement approaches to estimating interrater reliability," Publisher: University of Massachusetts Amherst. DOI: 10.7275/96JP-XZ07. [Online]. Available: https://scholarworks.umass.edu/pare/vol9/iss1/4/ (visited on 09/23/2022).

[113] J. Brannen, "Mixing methods: The entry of qualitative and quantitative approaches into the research process," *International Journal of Social Research Methodology*, vol. 8, no. 3, pp. 173–184, Jul. 2005, ISSN: 1364-5579, 1464-5300. DOI: 10.1080/13645570500154642. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/13645570500154642 (visited on 09/09/2022).

[114] M. D. Fetters, L. A. Curry, and J. W. Creswell, "Achieving integration in mixed methods designs—principles and practices," *Health Services Research*, vol. 48, no. 6, pp. 2134–2156, 2013, _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/14
6773.12117, ISSN: 1475-6773. DOI: 10.1111/1475-6773.12117. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/1475-6773.12117 (visited on 09/23/2022).

[115] E. Kristoffersen, "Forsvarets etterretningsdoktrine (2021)," p. 57,

[116] J. Biermann, L. d. Chantal, R. Korsnes, J. Rohmer, and Uendeger, "From unstructured to structured information in military intelligence - some steps to improve information fusion," presented at the Systems, Concepts and Integration (SCI) Methods and Technologies for Defence Against Terrorism, Section: Technical Reports, London: North Atlantic Treaty Organiza-

tion (NATO), Oct. 25, 2004. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA460220 (visited on 10/02/2022).

[117] Laerd. "Understanding descriptive and inferential statistics," Laerd Statistics. (), [Online]. Available: https://statistics.laerd.com/statistical-guides/descriptive-inferential-statistics.php (visited on 11/06/2022).

[118] J. D. Brown, "Likert items and scales of measurement?" *Shiken: JALT Testing and Evaluation SIG Newsletter*, vol. 15, no. 1, pp. 10–14, Mar. 2011, ISSN: 1881-5537. [Online]. Available: https://hosted.jalt.org/test/bro_34.htm.

[119] T. O. Maguire, "Semantic differential methodology for the structuring of attitudes," *American Educational Research Journal*, vol. 10, no. 4, pp. 295–306, 1973, Publisher: [American Educational Research Association, Sage Publications, Inc.], ISSN: 0002-8312. DOI: 10.2307/1161660. [Online]. Available: https://www.jstor.org/stable/1161660 (visited on 11/09/2022).

[120] Leard. "Mean, mode and median - measures of central tendency - when to use with different types of variable and skewed distributions," statistics.laerd.com. (), [Online]. Available: https://statistics.laerd.com/statistical-guides/measures-central-tendency-mean-mode-median.php (visited on 11/09/2022).

[121] C. Michalopoulou, "Likert scales require validation before application - another cautionary tale," *Bulletin of Sociological Methodology*, vol. 134, no. 1, pp. 5–23, Apr. 1, 2017. DOI: 10.1177/0759106317693786. [Online]. Available: https://journals.sagepub.com/doi/epub/10.1177/0759106317693786 (visited on 11/14/2022).

[122] F. Ramsey and D. Schafer, *The Statistical Sleuth: A Course in Methods of Data Analysis*. Cengage Learning, May 2, 2012, 786 pp., Google-Books-ID: jfoKAAAAQBAJ, ISBN: 978-1-285-40253-6.

[123] J. F. Gubrium, J. A. Holstein, A. B. Marvasti, and K. D. McKinney, *The SAGE Handbook of Interview Research: The Complexity of the Craft*. SAGE, Feb. 14, 2012, 625 pp., Google-Books-ID: VCFsZsvZdwkC, ISBN: 978-1-4129-8164-4.

[124] J. M. Johnson and T. Rowlands, "The interpersonal dynamics of in-depth interviewing," in *The SAGE Handbook of Interview Research: The Complexity of the Craft*, 2nd ed., Google-Books-ID: VCFsZsvZdwkC, London: SAGE, Feb. 14, 2012, pp. 99–114, ISBN: 978-1-4129-8164-4.

[125] B. Saunders, J. Kitzinger, and C. Kitzinger, "Anonymising interview data: Challenges and compromise in practice," *Qualitative Research*, vol. 15, no. 5, pp. 616–632, Oct. 2015, ISSN: 1468-7941. DOI: 10.1177/1468794114550439. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4582834/ (visited on 09/12/2022).

[126] M. S. Anderson, M. A. Shaw, N. H. Steneck, E. Konkle, and T. Kamata, “Research integrity and misconduct in the academic profession,” in *Higher Education: Handbook of Theory and Research: Volume 28*, ser. Higher Education: Handbook of Theory and Research, M. B. Paulsen, Ed., Dordrecht: Springer Netherlands, 2013, pp. 217–261, ISBN: 978-94-007-5836-0. DOI: 10.1007/978-94-007-5836-0_5. [Online]. Available: https://doi.org/10.1007/978-94-007-5836-0_5 (visited on 09/12/2022).

[127] N. H. Steneck, “Fostering integrity in research: Definitions, current knowledge, and future directions,” *Science and Engineering Ethics*, vol. 12, no. 1, p. 22, 2006.

[128] D. Shaw and P. Satalkar, “Researchers’ interpretations of research integrity: A qualitative study,” *Accountability in Research*, vol. 25, no. 2, pp. 79–93, Feb. 17, 2018, ISSN: 0898-9621, 1545-5815. DOI: 10.1080/08989621.2017.1413940. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/08989621.2017.1413940 (visited on 09/12/2022).

[129] J. M. DuBois, M. Strait, and H. Walsh, “Is it time to share qualitative research data?” *Qualitative Psychology*, vol. 5, no. 3, p. 380, Publisher: US: Educational Publishing Foundation, ISSN: 2326-3598. DOI: 10.1037/qup0000076. [Online]. Available: https://psycnet.apa.org/fulltext/2017-12030-001.pdf (visited on 09/12/2022).

[130] B. Saunders, J. Kitzinger, and C. Kitzinger, “Participant anonymity in the internet age: From theory to practice,” *Qualitative Research in Psychology*, vol. 12, no. 2, pp. 125–137, Apr. 3, 2015, ISSN: 1478-0887. DOI: 10.1080/14780887.2014.948697. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4376240/ (visited on 09/12/2022).

[131] M. N. Marshall, “Sampling for qualitative research,” *Family Practice*, vol. 13, no. 6, pp. 522–526, Jan. 1, 1996, ISSN: 0263-2136. DOI: 10.1093/fampra/13.6.522. [Online]. Available: https://doi.org/10.1093/fampra/13.6.522 (visited on 09/12/2022).

[132] A. Tjora, *Kvalitative forskningsmetoder i praksis. 3. utgave.* 3rd ed. Oslo: Gyldendal Akademisk, Jan. 2, 2017, ISBN: 978-82-05-50096-9.

[133] C. MacDougall and E. Fudge, “Planning and recruiting the sample for focus groups and in-depth interviews,” *Qualitative Health Research*, vol. 11, no. 1, pp. 117–126, Jan. 1, 2001, Publisher: SAGE Publications Inc, ISSN: 1049-7323. DOI: 10.1177/104973201129118975. [Online]. Available: https://doi.org/10.1177/104973201129118975 (visited on 09/17/2022).

[134] Etterretningstjenesten, “Fokus 2022,” Etterretningstjenesten, Oslo, Threat assessment. [Online]. Available: https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/fokus-2022 (visited on 09/17/2022).

[135] PST, “National threat assessment 2022,” Norwegian Police Security Service, Oslo, 2022. [Online]. Available: https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2022/ (visited on 09/17/2022).

[136] J. Monforte and J. Úbeda-Colomer, "Tinkering with the two-to-one interview: Reflections on the use of two interviewers in qualitative constructionist inquiry," *Methods in Psychology*, vol. 5, p. 100 082, Dec. 1, 2021, ISSN: 2590-2601. DOI: 10.1016/j.metip.2021.100082. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2590260121000394 (visited on 09/18/2022).

[137] J. Braithwaite, "Corporate crime research: Why two interviewers are needed," *Sociology*, vol. 19, no. 1, pp. 136–138, Feb. 1, 1985, Publisher: SAGE Publications Ltd, ISSN: 0038-0385. DOI: 10.1177/0038038585019001011. [Online]. Available: https://doi.org/10.1177/0038038585019001011 (visited on 09/18/2022).

[138] H. V. Kincaid and M. Bright, "The tandem interview: A trial of the two-interviewer team," *The Public Opinion Quarterly*, vol. 21, no. 2, pp. 304–312, 1957, Publisher: [Oxford University Press, American Association for Public Opinion Research], ISSN: 0033-362X. [Online]. Available: https://www.jstor.org/stable/2746746 (visited on 09/18/2022).

[139] F. Bechhofer, B. Elliott, and D. McCrone, "Safety in numbers: On the use of multiple interviewers," *Sociology*, vol. 18, no. 1, pp. 97–100, Feb. 1, 1984, Publisher: SAGE Publications Ltd, ISSN: 0038-0385. DOI: 10.1177/003803858401800109. [Online]. Available: https://doi.org/10.1177/003803858401800109 (visited on 09/18/2022).

[140] E. Kristoffersen, "Forsvarets etterretningsdoktrine," Norwegian Armed Forces, Oslo, Jan. 3, 2021, p. 57. [Online]. Available: https://www.etterretningstjenesten.no/publikasjoner/etterretningsdoktrinen/Etterretningsdoktrine_2021_Web_LoRes_02.pdf/_/attachment/inline/633b7840-43de-42af-bb89-243d81076208:edd1367bd55a434b4489162637336d7d632d42a0/Etterretningsdoktrine_2021%20-%20Web_LoRes%2002%20(PROD).pdf (visited on 10/02/2022).

[141] M. Vaismoradi, H. Turunen, and T. Bondas, "Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study," *Nursing & Health Sciences*, vol. 15, no. 3, pp. 398–405, 2013, _eprint: https://onlinelibrary.wiley.com/do ISSN: 1442-2018. DOI: 10.1111/nhs.12048. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/nhs.12048 (visited on 09/25/2022).

[142] S. Glen. "Self-selection bias," Statistics How To. (Jul. 30, 2017), [Online]. Available: https://www.statisticshowto.com/self-selection-bias/ (visited on 12/04/2022).

[143] "Etterretningsdoktrinen," Etterretningstjenesten. (), [Online]. Available: https://www.etterretningstjenesten.no/publikasjoner/etterretningsdoktrinen (visited on 10/02/2022).

[144] NIST. "The five functions," nist.gov. Last Modified: 2021-05-12T10:06-04:00. (Apr. 12, 2018), [Online]. Available: https://www.nist.gov/cyberframework/online-learning/five-functions (visited on 11/16/2022).

Appendixes

Information on the research project

The Impact of Cyber Security Information Sharing and its Effect on National Security

In this information letter we give you information on the goals of the research project and what the project means for you.

Purpose of the project
Norwegian national security depends on the cooperation and security efforts of both public and private entities, especially those supporting fundamental national functions (FNF). This task is challenging, as these FNFs span across different sectors, whereas CERTs and security hubs are mainly organized per sector or government ministries. The challenge is further complicated as most public and private entities have long, complex supply chains, spanning across national borders.

Despite the increasing interest in national security and collaboration between public and private entities, there is a lack of empirical research measuring security personnel's understanding and attitude towards information sharing and its relation to ensuring national security in Norway. This includes both cyber security information sharing (CSIS) efforts, and perceived benefits and challenges with CSIS.

This survey is part of a master thesis intended to examine whether CSIS efforts contribute to improved national security in Norway. The project will give an understanding of how CSIS is performed in Norway, as well as how it is perceived by the Norwegian cyber security community. Additionally, empirical research on whether the perceived value of CSIS efforts outweigh the cost, and whether the current cyber security regime is sufficient for both private enterprises and governmental strategic services is examined.

The overarching research question of the thesis is as follows: "Does cyber security information sharing efforts contribute to improved national security in Norway?", which is further divided into the following sub-questions to enable a more profound insight.

> **RQ1:** Are there any benefits of a joint national approach for coordinating and implementing CSIS versus a private and decentralized approach?
> **RQ2:** How is CSIS performed in Norway, and how is it perceived amongst security personnel and stakeholders?
> **RQ3:** Does the perceived value of information sharing efforts outweigh the perceived cost within the Norwegian CSIS community?
>> RQ3-1: Perceived benefits and challenges of CSIS
>> RQ3-2: Perceived usefulness of CSIS efforts
>> RQ3-3: Perceived willingness to engage in CSIS efforts

The goal of this questionnaire is to answer RQ2 and RQ3.

Institution responsible for the project
The department of Information Security and Communication Technology at NTNU is responsible for the project.

Why are you being asked to participate?

You have received this questionnaire as you are either a professional or stakeholder within the Norwegian cyber security community. The dissemination is based on the structure of supply chains supporting certain fundamental national functions, surveying both relevant sub-entities within the supply chains and the national cyber communities in which the chains end. We, the researchers, have presented this questionnaire to our acquaintances within the cyber security domain, but we only know a fraction of all we would like to participate in the survey.

For further dissemination, we rely on referral sampling, also known as "snowballing". We would highly appreciate if you forwarded this questionnaire to other relevant personnel within the Norwegian cyber security community, both in the private and public sector.

To ensure the validity of the research project, we aim at over 100 respondents, so please recommend and forward it to others.

What does participation involve for you?

This questionnaire is one of three data collection methods used in the thesis. If you choose to take part in the project, this will involve that you fill out an online questionnaire, taking approximately 15-20 minutes. The survey includes questions on your perception of CSIS and benefits and challenges related to CSIS; usefulness of CSIS efforts and your willingness to engage in CSIS efforts.

With regards to the questionnaire, no personal data is to be collected and you will not be identifiable from the submitted data. All data stored will be in accordance with NTNU policies and is to be deleted after the completion for the thesis. Additionally, only we, the researchers, will have access to the submitted data.

Participation is voluntary and you may protest

Participation in the project is voluntary. If you chose to participate, you can withdraw your consent at any time without giving a reason. As all participants are non-identifiable in the submitted data, we rely on your cooperation in identifying your submitted data. All your data will subsequently be deleted. There will be no negative consequences for you if you chose not to participate or later decide to withdraw.

Your personal privacy – how we will store and use your personal data

We will only use your data for the intents and purposes stated in this information letter. We treat all data confidentially and in accordance with personal data legislature (GDPR, Norwegian Personal Data Act and The Act on ethics and integrity in research).

You will not be identifiable in the collected data or in the finalized thesis.

All data will be stored in accordance with NTNU privacy and security policies and other legislature. The raw data is to be deleted after the completion and submittance of the thesis. Additionally, only we, the researchers, will have access to the submitted data.

What will happen to your personal data at the end of the research project?

The planned end date of the project is in December 2022. All submitted data will be deleted at the end of the project. The findings and correlations between the collection methods will however be accessible through the thesis.

Your rights

No participants will be identifiable in the collected data and finalized thesis. However, if you have concerns that you in fact are identifiable, you have the right to:

- protest,
- access your submitted personal data,
- correct personal data about you,
- delete personal data about you, and,
- submit a complaint to the Norwegian Data Protection Services regarding the processing of your personal data.

What gives us the right to process your data?
We will process your data as the project is assessed to be in the public interest, but you are able to withdraw if you no longer wish to participate.

Based on an agreement with the department of Information Security and Communication Technology at NTNU, Norwegian Data Protection Services has assessed that the processing of personal data in this project meets requirements in data protection legislation.

If you have any questions regarding the project, or want to know more or use your rights, please contact:

- Mikkel Amundsen (student/researcher): +47 [redacted] or mikkelam@stud.ntnu.no
- Fanny Chaba Sunde (student/researcher): +47 [redacted] or fannycs@stud.ntnu.no
- Benjamin James Knox (supervisor): +47 [redacted] or benjamin.j.knox@ntnu.no
- Our Data Protection Officer Thomas Helgesen: +47 [redacted] or thomas.helgesen@ntnu.no

If you have questions about how data protection has been assessed in this project, contact:

- Data Protection Services, by email: (personverntjenester@sikt.no) or by telephone: +47 53 21 15 00.

Yours sincerely,

Benjamin James Knox	*Fanny Chaba Sunde*	*Mikkel Amundsen*
(Supervisor)	Researcher/student	Researcher/Student

Information on the research project

The Impact of Cyber Security Information Sharing and its Effect on National Security

In this information letter we give you information on the goals of the research project and what the project means for you.

Purpose of the project
Norwegian national security depends on the cooperation and security efforts of both public and private entities, especially those supporting fundamental national functions (FNF). This task is challenging, as these FNFs span across different sectors, whereas CERTs and security hubs are mainly organized per sector or government ministries. The challenge is further complicated as most public and private entities have long, complex supply chains, spanning across international borders.

Despite the increasing interest in national security and collaboration between public and private entities, there is a lack of empirical research measuring security personnel's understanding and attitude towards information sharing and its relation to ensuring national security in Norway. This includes both cyber security information sharing (CSIS) efforts, and perceived benefits and challenges with CSIS.

This in-depth interview is part of a master thesis intended to examine whether cyber security information sharing efforts contribute to improved national security in Norway. The project will give an understanding of how CSIS is performed in Norway, as well as how it is perceived by the Norwegian cyber security community. Additionally, empirical research on whether the perceived value of CSIS efforts outweigh the cost, and whether the current cyber security regime is sufficient for both private enterprises and governmental strategic services is examined.

The overarching research question of the thesis is as follows: "Does cyber security information sharing efforts contribute to improved national security in Norway?", which is further divided into the following sub questions:

> **RQ1:** Are there any benefits of a joint national approach for coordinating and implementing CSIS versus a private and decentralized approach?
> **RQ2:** How is CSIS performed in Norway, and how is it perceived amongst security personnel and stakeholders?
> **RQ3:** Does the perceived value of information sharing efforts outweigh the perceived cost within the Norwegian CSIS community?
> > RQ3-1: Perceived benefits and challenges of CSIS
> > RQ3-2: Perceived usefulness of CSIS efforts
> > RQ3-3: Perceived willingness to engage in CSIS efforts

Institution responsible for the project
The department of Information Security and Communication Technology at NTNU is responsible for the project.

Why are you asked to participate?
We want you to participate in an in-depth interview as you are employed either in a leadership or

management position either within the Norwegian cyber security community or in an organization supporting a fundamental national function which utilizes cyber security information.

Between 10 and 15 interview objects have been asked to participate in this study. You, and the other participants have been selected on the following criteria; 1) your position and experience, 2) you work in an organization which is part of a supply chain supporting Norwegian fundamental national functions, 3) your organizations´ domain according to PMESII[1]. By interviewing multiple private and public entities with different places in supply chain hierarchies, any common findings are expected to be scientifically sound as they are cross-referenced and compared to each other to avoid intra-organizational attitudes and bias.

To find and select interview objects, we are both proactively approaching relevant organizations and individuals, relying on us, the researchers, in identifying suited objects; the organizations we reach out to identifying relevant interview objects within their ranks; or interview objects recommending other relevant interview objects.

What does participation involve for you?
The in-depth interviews is one of three data collection methods used in the thesis. If you choose to take part in the project, this will involve you participating in an in-depth interview taking approximately 1-2 hours, depending on your inputs. The in-depth interview includes questions on your general experience and perception of CSIS; benefits and challenges related to CSIS; usefulness of CSIS efforts and your willingness to engage in CSIS efforts.

The information will be recorded via a tape recorder, which is then transcribed and stored in a text format. To mitigate biases,

Participation is voluntary
Participation in the project is voluntary. If you chose to participate, you may withdraw your consent at any time without giving a reason. All information about you will then be deleted. There will be no negative consequences for you if you chose not to participate or later decide to withdraw.

A major concern to us is your ability and willingness to speak freely, truthfully and disclose all relevant perceptions. To ensure this, you are anonymized thoroughly. In the final paper, the interview object mass is descried in general and submitted data is not linked to any individual anonymized object.

Your personal privacy – how we will store and use your personal data
We will only use your data for the intents and purposes stated in this information letter. We treat all data confidentially and in accordance with personal data legislature (GDPR, Norwegian Personal Data Act and The Act on ethics and integrity in research).

You will not be identifiable in the final thesis. During processing and analysis, your name and contact details will be kept separate from the content data and stored in a separate physical format. Only we, the researchers, will be able to link your data to you as an individual.

All data will be stored in accordance with NTNU privacy and security policies and other legislature. The raw data is to be deleted after the completion and submittance of the thesis. Additionally, only we, the researchers, will have access to the submitted data.

[1] PMESII is used as a structured approach to ensure that the data collected through in-depth interviews has as high viability as possible and to ensure nuanced and accurate depiction of perceptions on Norwegian CSIS. PMESII includes the following factors: political, military, economic, social, infrastructure and information.

What will happen to your personal data at the end of the research project?
The planned end date of the project is in December. All personal data, including the recordings and transcriptions, will be deleted at the end of the project. The findings and correlations between the collection methods will however be accessible through the thesis.

Your rights
No interview objects are intended to be identifiable in the analyzed results. To ensure anonymity and our commitments to you, you will be sent all parts of the thesis in which your data is included prior to finishing the project or opt out if you do not want to receive the final draft. If you discover or have concerns that you in fact are identifiable, you have the right to:

- protest,
- access your submitted personal data,
- correct personal data about you,
- delete personal data about you, and,
- submit a complaint to the Norwegian Data Protection Services regarding the processing of your personal data.

What gives us the right to process your data?
We will process your personal data based on your consent.

Based on an agreement with the department of Information Security and Communication Technology at NTNU, Norwegian Data Protection Services has assessed that the processing of personal data in this project meets requirements in data protection legislation.

If you have any questions regarding the project, or want to know more or use your rights, please contact:

- Mikkel Amundsen (student/researcher): +47 [redacted] or mikkelam@stud.ntnu.no
- Fanny Chaba Sunde (student/researcher): +47 [redacted] or fannycs@stud.ntnu.no
- Benjamin James Knox (supervisor): +47 [redacted] or benjamin.j.knox@ntnu.no
- Our Data Protection Officer Thomas Helgesen: +47 [redacted] or thomas.helgesen@ntnu.no

If you have questions about how data protection has been assessed in this project, contact:

- Data Protection Services, by email: (personverntjenester@sikt.no) or by telephone: +47 53 21 15 00.

Yours sincerely,

Benjamin James Knox	*Fanny Chaba Sunde*	*Mikkel Amundsen*
(Supervisor)	Researcher/student	Researcher/Student

Consent form

I have received and understood information about the project “The Impact of Cyber Security Information Sharing and its Effect on National Security” and have been given the opportunity to ask questions. I give consent to participate in an in-depth interview.

I give consent for my personal data to be processed until the end of the project.

(Signed by participant, date)

Questionnaire

Perceived attitudes on Cyber Security Information Sharing within the Norwegian cyber community

Thank you for participating in the survey! Before you start the survey, we would like to explain the term Cyber Security Information Sharing (CSIS).

CSIS is understood as sharing of any information that can help an organization identify, assess, monitor, and respond to cyber threats. CSIS includes sharing of vulnerabilities as well as cyber threat intelligence/information (CTI), such as indicators of compromise (IOCs); tactics, techniques, and procedures (TTPs) used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents.

This survey will normally take between 10-15 min to complete.

Part 1 – Context

Q1: Which sector is your organization within?

- □ Private
- □ Public

Q2: Do you work in a cyber security information sharing organization?

By "Cyber Security Organization", we mean organizations which have cyber security as one of its primary tasks. Examples of such organizations are ISAC, CERT, CSIRT, SOC, etc.

- □ Yes
- □ No

Q3: Which of these categories best describe your organization's primary activity?[1]

We are after which sector your enterprise is part of; e.g. if you are part of a cyber security entity within the railway, choose "Transportation and storage"; or if you are working within or for a financial institution, choose "Finance and insurance". If you do not identify yourself with any of the provided options, select the most suited option.

- □ Agriculture, forestry, and fishing
- □ Mining and quarring
- □ Manufacturing
- □ Electricity, gas, steam, and air conditioning supply
- □ Water supply; sewerage, waste management and remediation
- □ Construction
- □ Wholesale and retail trade
- □ Transportation and storage
- □ Accommodation and food services
- □ Information and communication
- □ Finance and insurance
- □ Real estate
- □ Professional (consultatory), scientific, and technical activities
- □ Administrative and support services
- □ Public administration and defense; compulsory social security
- □ Education
- □ Human health and social work

[1] https://www.ssb.no/klass/klassifikasjoner/6

□ Arts, entertainment, and recreation
□ Other service activities

Q4: Which of these options best represents the number of employees working in your organization?

□ < 50
□ 50-249
□ 250-1000
□ > 1000

Q5: Do you have at least 1 year of working experience in cyber security?

□ Yes
□ No

Q6: How many years of professional experience do you have in cyber security?

□ < 2 years
□ 2-5 years
□ > 5 years

Q7: What is your role in your organization?

□ Top management
□ Middle management
□ Practitioner

Part 2 – CSIS in Norway

For this section, we are interested in your relationship with the organizations you share cyber security information with.

Q8: Is your organization currently involved in cyber security information sharing?

□ Yes
□ No

Q9: Which internal factor led to your organization's engagement in cyber security information sharing?

First, we ask you for the main or most relevant internal factor for engaging in information sharing, while external factors are covered next.

□ Access to government agencies
□ Access to other companies and their cyber security information
□ Access to expertise and knowledge
□ Access to professional networks
□ Unknown
□ My organization does not share cyber security information
□ Other:___________

Q10: Which external factor led to your organization's engagement in cyber security information sharing?

Select the most relevant alternative

□ Geopolitical context and security situation
□ Own or similar organizations targeted by cyber criminals
□ Requirements from superior organization, laws or regulations
□ Unknown
□ My organization does not share cyber security information
□ Other:___________

Q11: To whom does your organization share cyber security information with?

You may select more than one alternative

- □ Cyber security information sharing organizations (e.g. ISAC, CERT, CSIRT, SOC, etc.)
- □ National services (e.g. NSM/NCSC, PST, NC3, FCKS, etc.)
- □ Horizontally (to similar organizations as your own)
- □ Top-down (from cyber security information sharing organizations or national services to subordinated organizations)
- □ My organization does not share cyber security information

Q12: Does your organization pay for membership in any cyber security information sharing organizations (e.g. ISAC, CERT, CSIRT, SOC, etc.)?

- □ Yes
- □ No

Q13: If your organization is not participating in any cyber security information sharing organizations (e.g. ISAC, CERT, CSIRT, SOC, etc.), state the most relevant reason why:

- □ My organization is a member of a cyber security information sharing organization
- □ Cost of membership
- □ Lack of information quality, utility or value
- □ Inability or lack of resources to manage additional information processing
- □ Too time-consuming
- □ Other:______________

Part 3 – Perceptions on CSIS

Q14: How strongly do you agree or disagree with the following statements?
1 (strongly disagree) to 7 (strongly agree).

S1: Cyber security information sharing contributes to enhancing the national security posture and situational awareness
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S2: Cyber security information sharing contributes to enhancing organizations' security posture and situational awareness
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S3: Threat actors are deterred by cyber security information sharing among organizations
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S4: Cyber security information sharing supports incident response efforts
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S5: Cyber security information sharing contributes to breach detection and recovery
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S6: Sharing of cyber security information reduces duplicate information handling
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S7: Cyber security information sharing strengthens and expands professional networks
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S8: Cyber security information sharing validates and complements other sources of information
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S9: Cyber security information sharing enhances defensive agility and resilience
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S10: Cyber security information sharing helps in combating cyber security skills shortage
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S11: Cyber security information sharing reduces overall cyber security costs
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S12: Cyber security information sharing supports security investment decisions
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S13: Cyber security information sharing strengthens relationship with government agencies
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S14: Standardization issues hinder cyber security information sharing
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S15: Inconsistent definitions and terminology undermine efficient cyber security information sharing
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S16: It is difficult to determine the accuracy and quality of shared cyber security information
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S17: It is difficult to ensure the timeliness of shared cyber security information
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S18: The interoperability and automation of cyber security information sharing are difficult to achieve
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S19: Cyber security information sharing results in redundant and irrelevant data
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S20: There is a shortage of analysts with the skills required to handle shared cyber security information
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S21: It is difficult to trust the other participants in cyber security information sharing efforts
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S22: Free riding will hinder cyber security information sharing efforts
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S23: Setting up the cyber security information sharing infrastructure is expensive and drains resources
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S24: Cyber security information sharing reduces clients' confidence in the organization that shares information with others
This question is intended to measure whether sharing of clients' data, vulnerabilities, etc. reduce their confidence in the organization sharing it

□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S25: Government over-classification undermine effective cyber security information sharing

□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S26: Privacy and antitrust legal concerns hinder cyber security information sharing
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

S27: Inconsistent legal frameworks undermine cyber security information sharing
□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

Part 4 – Attitudes toward cyber security information sharing

The questions in Part 4 are based on four different categories of CSIS defined in the following questions.

Definitions of information sharing categories:

- **Data sharing** aims to give a receiving organization a more complete picture of the nature of a cyber security threat, incident or vulnerability. The main goal of this type of sharing is to inform a decision or assessment or to increase the chance of a successful detection of, triage of, and response to, cyber threats. Such information can be shared in e.g. intelligence reports.

- ***Alerts and triggers for action** aims to direct the receiving organization to an unknown threat or vulnerability, and often bring to attention the need for decisions of the receiving organizations did not know prior to the alert. In this category, timeliness is more important than the degree of data processing and confidence in assessments.*

- ***Knowledge sharing** is not intended to share immediate or time-sensitive information, but aims to build a common pool of knowledge, advisories and lessons learned across different organizations. This may be done through post-breach reports, case studies or intelligence and security products provided by security vendors, national organizations or security organizations.*

- ***Expertise sharing** aims to bring together individuals from separate organizations to exchange and apply multidisciplinary expertise to tackle common security issues or challenges. In contrast to knowledge sharing, expertise sharing brings people and their expertise together either physically or digitally.*

Q15: How often does your organization participate in the following information sharing categories?

S1: Data sharing
Data sharing aims to give a receiving organization a more complete picture of the nature of a cyber security threat, incident or vulnerability. The main goal of this type of sharing is to inform a decision or assessment or to increase the chance of a successful detection of, triage of, and response to, cyber threats. Such information can be shared in e.g. intelligence reports.

□ Daily
□ Weekly
□ Monthly
□ Quarterly
□ Semi-annually
□ Annually
□ Not applicable

S2: Alerts & Triggers for action

Alerts and triggers for action aims to direct the receiving organization to an unknown threat or vulnerability, and often bring to attention the need for decisions of the receiving organizations did not know prior to the alert. In this category, timeliness is more important than the degree of data processing and confidence in assessments.

□ Daily
□ Weekly
□ Monthly
□ Quarterly
□ Semi-annually
□ Annually
□ Not applicable

S3: Knowledge sharing
Knowledge sharing is not intended to share immediate or time-sensitive information, but aims to build a common pool of knowledge, advisories and lessons learned across different organizations. This may be done through post-breach reports, case studies or intelligence and security products provided by security vendors, national organizations or security organizations.

□ Daily
□ Weekly
□ Monthly
□ Quarterly
□ Semi-annually
□ Annually
□ Not applicable

S4: Expertise sharing
Expertise sharing aims to bring together individuals from separate organizations to exchange and apply multidisciplinary expertise to tackle common security issues or challenges. In contrast to knowledge sharing, expertise sharing brings people and their expertise together either physically or digitally.

□ Daily
□ Weekly
□ Monthly
□ Quarterly
□ Semi-annually
□ Annually
□ Not applicable

Q16: How useful do you find the following information sharing categories?
1 (not useful) to 5 (very useful)

S28: Data sharing
□ 1 □ 2 □ 3 □ 4 □ 5

S29: Alerts & Triggers for action
□ 1 □ 2 □ 3 □ 4 □ 5

S30: Knowledge sharing
□ 1 □ 2 □ 3 □ 4 □ 5

S31: Expertise sharing
□ 1 □ 2 □ 3 □ 4 □ 5

Q17: Which of the information sharing categories do you assess as most useful?

- □ Data sharing
- □ Alerts & Triggers for action
- □ Knowledge sharing
- □ Expertise sharing

Q18: Which of the information sharing categories do you assess as least useful?

- □ Data sharing
- □ Alerts & Triggers for action
- □ Knowledge sharing
- □ Expertise sharing

Q19: Which organizations do you receive the most useful cyber security information from?

- □ Cyber security information sharing organizations (e.g. ISAC, CERT, CSIRT, SOC, etc.)
- □ National services (e.g. NSM/NCSC, PST, NC3, FCKS, etc.)
- □ Similar organizations as your own
- □ Not applicable

Q20: How willing are you to engage in the following information sharing categories?
1 (least willing) to 5 (most willing)

S5: Data sharing
□ 1 □ 2 □ 3 □ 4 □ 5

S6: Alerts & Triggers for action
□ 1 □ 2 □ 3 □ 4 □ 5

S7: Knowledge sharing
□ 1 □ 2 □ 3 □ 4 □ 5

S8: Expertise sharing
□ 1 □ 2 □ 3 □ 4 □ 5

Q21: Which of the information sharing categories are you most willing to engage in?

- □ Data sharing
- □ Alerts & Triggers for action
- □ Knowledge sharing
- □ Expertise sharing

Q22: Which of the information sharing categories are you least willing to engage in?

- □ Data sharing
- □ Alerts & Triggers for action
- □ Knowledge sharing
- □ Expertise sharing

Q23: Which organizations is your organization most willing to share information with?

- □ Cyber security information sharing organizations (e.g. ISAC, CERT, CSIRT, SOC, etc.)
- □ National services (e.g. NSM/NCSC, PST, NC3, FCKS, etc.)
- □ Similar organizations as your own
- □ Not applicable

Feedback & Comments
This part is **voluntary.** However, if you have any feedback and comments regarding the questionnaire, feel free to answer the questions below.

Do you have any feedback that can improve the questionnaire?

Do you have any comments that may help us in analyzing the data?

Interview guide for in-depth interviews

The Impact of Cyber Security Information Sharing and Its Effect on National Security

Introduction

- a. Introduction of the interviewer
  - i. Name, experience
- b. Aim of the thesis
- c. Quick talk-through on anonymity measures
- d. Obtain consent from the interview object (IO) – sign Information Letter.

Part 1: Context of Interview Object

1. Previous experience
   - a. Where, what position, how long?
2. Current work
   - a. Information on the organization
     - i. Private/public
     - ii. Type of organization (business. security organization, national service)
     - iii. Sector (primary activity) [Note: According to predefined options, interviewers give their assessment]
     - iv. Are you part of an information sharing partnership/security sharing organization?
   - b. Position (top/middle manager and/or specific)
   - c. Describe your current work and responsibilities
   - d. Years of professional experience in cyber security
   - e. Describe your organization
     - i. What do you do?
     - ii. Describe your organization in relation to FNF
       - 1. If not knowledge of FNF, describe your organization´s role in relation to national security

Part 2: CSIS in Norway

- 1) How do you define CSIS?
- 2) Why did your organization enter CSIS partnerships, and why are you still engaging in it?
  - a) If not, why?
- 3) Who do you share information with, and why?

Part 3: Perceptions on CSIS

- 1) Which benefits and challenges do you see related to CSIS in Norway? What is good and what is challenging?
  - a) Both related to vertical (security organizations, national services, subscribing organizations), horizontally (other similar businesses)
- 2) What is your impression related to cooperation and information sharing both between businesses, from national services to your organization and to and from security information sharing organizations?

Part 4: Attitudes toward CSIS

- 1) Introduction to categories of information sharing:

i) ***Data sharing*** aims to give a receiving organization a more complete picture of the nature of a cyber security threat, incident, or vulnerability. The main goal of this type of sharing is to inform a decision or assessment or to increase the chance of a successful detection of, triage of, and response to, cyber threats. Such information can be shared in e.g. intelligence reports.

ii) *Alerts* ***& Triggers for action*** aims to direct the receiving organization to an unknown threat or vulnerability, and often bring to attention the need for decisions of the receiving organizations did not know prior to the alert. In this category, timeliness is more important than the degree of data processing and confidence in assessments.

iii) ***Knowledge sharing*** is not intended to share immediate or time-sensitive information, but aims to build a common pool of knowledge, advisories and lessons learned across different organizations. This may be done through post-breach reports, case studies or intelligence and security products provided by security vendors, national organizations or security organizations.

iv) ***Expertise sharing*** aims to bring together individuals from separate organizations to exchange and apply multidisciplinary expertise to tackle common security issues or challenges. In contrast to knowledge sharing, expertise sharing brings people and their expertise together either physically or digitally.

2) Which type of information do you share the most? Why?
   a) Usefulness and willingness?
3) Which type of information do you share the least? Why?
   a) Both usefulness and willingness?
4) Do you have any concerns related to sharing some types of information over others?
5) Who are you most and least willing to share information with? Why?

NTNU

Kunnskap for en bedre verden