UiA University of Agder

Master

Norwegian cybersecurity guidelines

A case study of Norwegian security agencies

NICOLAY BRÅTHEN LEKNES

SUPVERVISOR

Paolo Spagnoletti & Terje Gjøsæter

University of Agder, 2021
Faculty of Social Sciene
Department of Information Studies

Preface

This thesis is the final submission of the cybersecurity master program at the University of Agder (UiA), in the faculty of social science. I have been a student at the University of Agder for 5 years. My education has taught me various knowledge that I will use for the rest of my life. I want to highlight that projects do not necessarily go as planned, the ability to adjust or modify the course of action is difficult, but important.

I want to thank everyone who has contributed and made this thesis possible. Especially my supervisors at UiA, Terje Gjøsæter & Paolo Spaglonetti for valuable and explicit feedback and advice. I also want to Thank Torbjørn Kveberg from Forsvarets Forskningsinsitutt for external guidance & motivation through the thesis.

In addition, I want to thank all the respondents from security authorities in Norway who participated and shared their valuable knowledge and experiences in the interviews.

Kristiansand, 17 of June, Nicolay Leknes

Abstract

In recent years, several countries in Europe have focused on developing their own national solutions for cybersecurity. Norwegian security authorities have also developed national guidelines to develop a common national solution to meet the ever-increasing focus on European and international regulations within cybersecurity. The study sheds light on elements related to the issue at both a national and international level and seeks to discover how national cybersecurity guidelines can emerge in the cyber landscape in the coming years.

The study was carried out as a qualitative method using a case study in Norwegian security authorities. In addition, interviews from security agencies in Norway and document analysis of published documents have been used to obtain empirical data in the thesis.

Keywords: National guidelines, Cybersecurity framework, Cybersecurity regulation, Certification

Terms & Abbreviations

The terminology in the field can vary depending on the variety of reasons, a clarification of the common terms referred to in the thesis are needed.

- **Cybersecurtiy framework** = A general guideline or recipe for implementation developed by a company or organisation.
- **National guidelines** = Advice developed my national security organisations or authorities.
- **International cybersecurity frameworks** = International acknowledged cybersecurity branch framework

All of the quotes in the findings chapter(4) of this thesis is translated from Norwegian and will not be elaborated further in the text. However, quotes that are translated from other parts of the thesis will be highlighted as translated to the given language.

Contents

List of Figures

Chapter 1

Introduction

The threat landscape for cyberspace is rapidly evolving, and in the light of the corona pandemic outbreak of 2019, there have been new adaptive ways for threat actors to find vulnerabilities (ENISA, 2020). The threat landscape is not constant and tends to vary across sectors, countries & continents. A trend during the pandemic has been to expose government institutions to gain information or leverage that can be used or exposed at a later stage for political advantage (Interpol, 2020). As the landscape is constantly changing, there is a demand for effective standardised tools, guidelines, and frameworks to cope with rapid change. This thesis will study how the national security agencies in Norway have developed their own set of guidelines to be deployed in the Norwegian market. This thesis will provide a systematic literature review that presents theories of different approaches to implementing security frameworks and guidelines, both at a national and international level. Empirical data will also be presented from interviews & documents from national security authorities from Norway.

1.1 Motivation

Norway is one of the most digitized nations in the world and benefits from economic growth through more efficient public systems & services compared to other developed countries (European Commision, 2020)(Norsk senter for informasjonssikring, 2016). Norway has also been the leading actor in proposing national cybersecurity guidelines from a historical perspective, as it was the first was country to propose a national cybersecurity strategy in 2003 (Norwegian Ministeries, 2019). However, the rapid increase of digitalisation in Norwegian organisations have also lead to an economic loss. Up to 19 millions NOK each year are lost or stolen from Norwegian society due to the increase of cyberattacks, making digitalisation less profitable (Norsk senter for informasjonssikring, 2016). In addition, politically motivated attacks are also increasing as the government and the public sector digitalize. An example is the attack on the Norwegian Parliament, Stortinget, in the autumn of 2020 when Russian hackers infiltrated end users (Regjeringen, 2020). In order to defend against the rapid increase of cyberattacks, the government of Norway has provided frameworks and guidelines to ensure that critical digital infrastructure is defended (Norwegian Ministeries, 2019).

> "In order to achieve the best possible protection, Norway is dependent on cooperation both nationally and internationally. In the digital area, there is a need for increased national coordination in terms of security and support of Norwegian interests in the further development of international practice and regulations in cyberspace" (Utenriksdepartementet, 2017).
> -Erna Solberg, Prime minister of Norway (Translated from Norwegian)

The government has motions for a long-term plan and frameworks for strategic communication & cooperation between organisations that will provide strong security for critical national functions. In order to provide such cooperation, inspiration from other international standardized frameworks should be included (National Security Agency, 2021).

Norway is also looking for external cooperation and inspiration in Europe.
As (Utenriksdepartementet, 2017) states, the European Union Agency for Cybersecurity (ENISA), is an important factor of influence by how security is being practised in Norway. Implementing the EU's Network and Information Security Directive (NIS) & (ENISA)'s cybersecurity act will effectively increase security awareness and incident response coordination between European countries. As well as implementing a common certification scheme that can be used to enforce laws & regulations (Utenriksdepartementet, 2017)(National Security Agency, 2020b).

1.2 Research Question

The thesis aims to broaden the insight of cybersecurity frameworks. In a more specific scope, this thesis will highlight the topic focusing on national cybersecurity guidelines. The topic of national guidelines is interesting and relevant, as further research is needed on national cybersecurity frameworks and guidelines (Syafrizal, Selamat, & Zakaria, 2020). A case study with a sample of Norwegian security agencies was investigated to discover more about the topic, as future research is needed to find out how to supplement or improve the development and management of cybersecurity (van Eeten, 2017). It is interesting to determine how "established" international cybersecurity frameworks are deployed and further developed into more comprehensive cybersecurity guideline. As details regarding the relationship between international cybersecurity frameworks and national cybersecurity guidelines are yet to be uncovered, the thesis will be focusing on answering the following research questions:

> **Research question**
> Why are countries such as Norway developing their own national cybersecurity guidelines instead of implementing cybersecurity frameworks?

1.3 What is a cybersecurity guideline?

Before further elaborating on what a cybersecurity guideline may consist of, clarifying the terminology is needed. The term "cybersecurity guideline" may have different meanings depending on various reasons. In this context, cybersecurity guideline will be referred to as a set of recommendations or endorsement to conduct cybersecurity. Further, will national cybersecurity guidelines be used when national governments or security agencies issue the recommendations within a country. The term "cybersecurity frameworks" will be used to address acknowledged branch standards, with examples such as Center for Internet Security (CIS), National Institute of Standards and Technology (NIST) or International Organization for Standardization (ISO).

1.4 Contribution

This study has looked into the challenges and benefits of implementing a more comprehensive national cybersecurity guideline in Norway. The thesis will shed light on key aspects of cybersecurity frameworks or guidelines, which is a central focus for many European countries. This thesis further opens up for research to focus on national cybersecurity guidelines within a sector, private or public, and shed light on the issues surrounding guidelines for cloud storage and regulations in Norway.

1.5 Thesis structure

Chapter 2 will present a literature review based on national cybersecurity guidelines. Chapter 3 shows the research design & methodology for the thesis. Chapter 4 will present findings from the empirical data, interviews & document analysis. Chapter 5 will discuss the findings together with the theory from chapter 2. Chapter 6 will present a conclusion of the study. Chapter 7 will elaborate on the limitation of the study, and chapter 8 will propose further work. Attachment related to the study is further included in the appendix. Appendix A contains more figures related to the literature search. In appendix B, there is an attachment of the interview guide. Appendix C presents the consent form given to the interview participants. A visual representation of the structure is shown in figure 1.1.

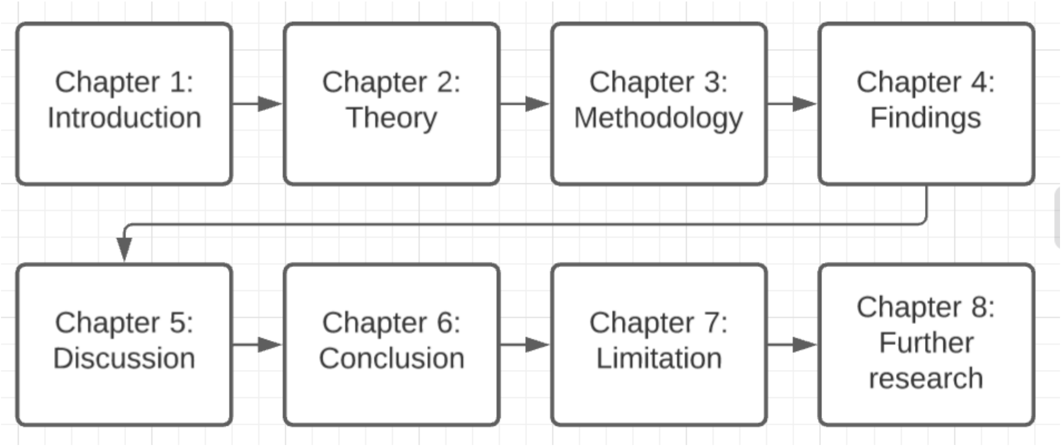


Figure 1.1: Thesis structure

Chapter 2

Theory

The following sub-sections provide insight into the recent literature in the topics. The topics in this chapter have been selected to the best of my ability to highlight themes and subjects related to the research question. The themes within the literature review are categorised into subsections that are found within the topic. Furthermore, the literature that is presented will be compared with empirical findings in Chapter 6.

2.1 The literature review

A literature review is a process to find and evaluate existing work from authors and researchers in a method that can be verified and validated later (Fink, 2019). Conducting the review was useful to discover relevant theories & themes related to the research problem. In addition, the literature created the foundation for the interview questions. The review highlights relevant literature on the topic and finds research gaps and limitations within earlier studies.

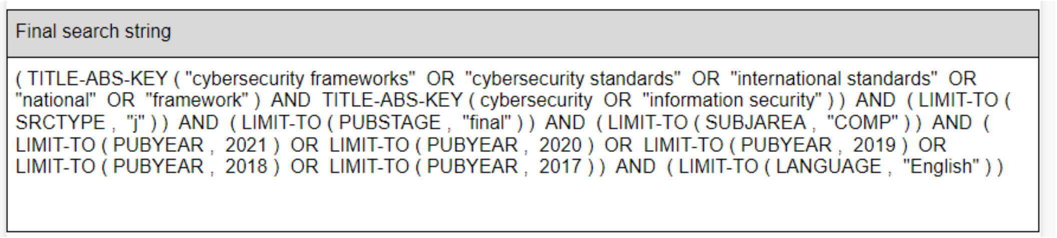
2.1.1 Review outline

There has been a general focus on the underlying topics that can answer the research question. This review has includes articles that examine other countries implementation of national cybersecurity guideline at a country level & cybersecurity framework in an overall perspective. These articles are included to look for similarities and to be able to compare execution and procedures against Norway's implementation of cybersecurity guidelines. The review below will present a range of topics that may directly or indirectly answer different aspects of the research question.

2.1.2 Database & search

One of the first steps in conducting a literature review was to find a trustworthy scientific search database. As several different databases represent different genres, choosing the correct database can be a crucial element for enhancing the quality of the review (Fink, 2019).

Scopus was chosen as a database to find relevant topics within the field. Scopus gathers data from multiple publishers together as an index database, making the searches less time consuming & reduces the chance of missing important information.



Final search string

```
( TITLE-ABS-KEY ( "cybersecurity frameworks"  OR  "cybersecurity standards"  OR  "international standards"  OR
"national"  OR  "framework" )  AND  TITLE-ABS-KEY ( cybersecurity  OR  "information security" ) )  AND  ( LIMIT-TO (
SRCTYPE ,  "j" ) )  AND  ( LIMIT-TO ( PUBSTAGE ,  "final" ) )  AND  ( LIMIT-TO ( SUBJAREA ,  "COMP" ) )  AND  (
LIMIT-TO ( PUBYEAR ,  2021 )  OR  LIMIT-TO ( PUBYEAR ,  2020 )  OR  LIMIT-TO ( PUBYEAR ,  2019 )  OR
LIMIT-TO ( PUBYEAR ,  2018 )  OR  LIMIT-TO ( PUBYEAR ,  2017 ) )  AND  ( LIMIT-TO ( LANGUAGE ,  "English" ) )
```

Figure 2.1: Final search string on Scopus

Searching for "security frameworks" on Scopus will yield over 65.000 results making it ineffective to deal with. To narrow results, I included keywords & synonyms that may relate to answering the research questions. To combine relevant search keywords, Boolean operators were used. Boolean operations can both be used to narrow the searches by using 'AND' or widen the search using 'OR'. There is a fine balance between being too specific and vague in searches. Specific search terms can lead to tunnel vision and bias. Search terms that are too vague will result in articles out of scope and make the review difficult. There are methods to validate the balance of the searches. Inspecting other research articles on the topic and looking for relevant keywords is one of those methods (Fink, 2019). The keywords used were inspired by the research problem but adjusted to the scope of external research papers. The search string is documented in 2.1

2.1.3 Practical screening & exclusion criteria

To narrow the results, a practical screening was conducted. Excluding through a practical screen is primarily a practical reason, hence the name, as it removes unwanted articles and increases the effectiveness of the review (Fink, 2019). To efficiently narrow down articles, a systematic approach of exclusion was conducted. Filtering articles by language, year, quality & category. The process is further illustrated in 2.2.

Keywords
To narrow the subject into the scope of the research questions, relevant keywords were chosen to find relevant articles.

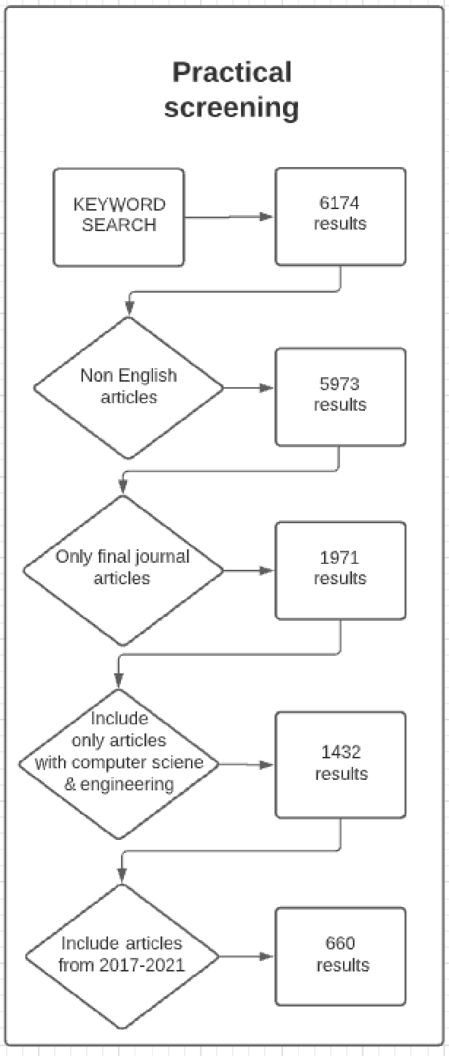

Practical screening
KEYWORD SEARCH
6174 results
Non English articles
5973 results
Only final journal articles
1971 results
Include only articles with computer sciene & engineering
1432 results
Include articles from 2017-2021
660 results

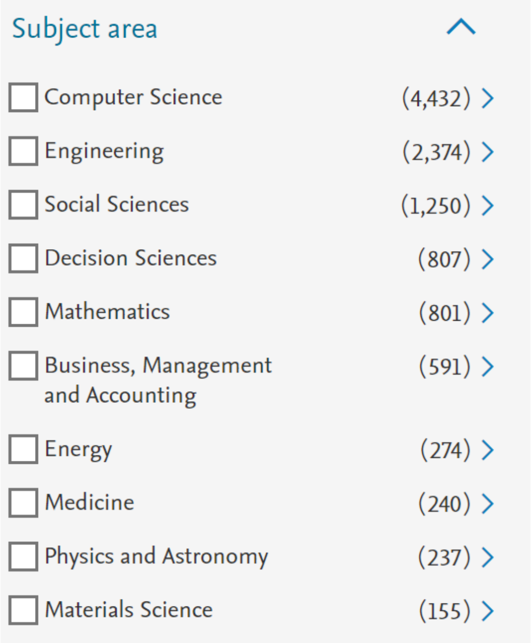
Figure 2.2: Practical Screening

Language
To understand the depth of the articles, only English written articles were included.

Year
Since the topic is rapidly evolving, with laws & regulations every year, articles from previous dates than 2017 would not be included in the review. This was only to secure recent articles that would include relevant information.

Quality
Everything except final journal articles was excluded.

Category
A final exclusion criteria was chosen based on the search topic, as Scopus filters categories into groups. Only articles that were related to computer science & engineering were included. The themes that are available in Scopus are represented in the table. 2.3



Subject area

□ Computer Science	(4,432)
□ Engineering	(2,374)
□ Social Sciences	(1,250)
□ Decision Sciences	(807)
□ Mathematics	(801)
□ Business, Management and Accounting	(591)
□ Energy	(274)
□ Medicine	(240)
□ Physics and Astronomy	(237)
□ Materials Science	(155)

Figure 2.3: Categories on Scopus

Once the practical screening was conducted, 660 articles were left for a quality review, as shown in the bottom of 2.2. The next step was only to include relevant articles. This step was conducted by further excluding articles by title, keywords & abstract. Relevant articles were included and given a grading from 0-5 of relevance towards the research question. A total of 15 articles were included in the final review, as shown in 2.4.

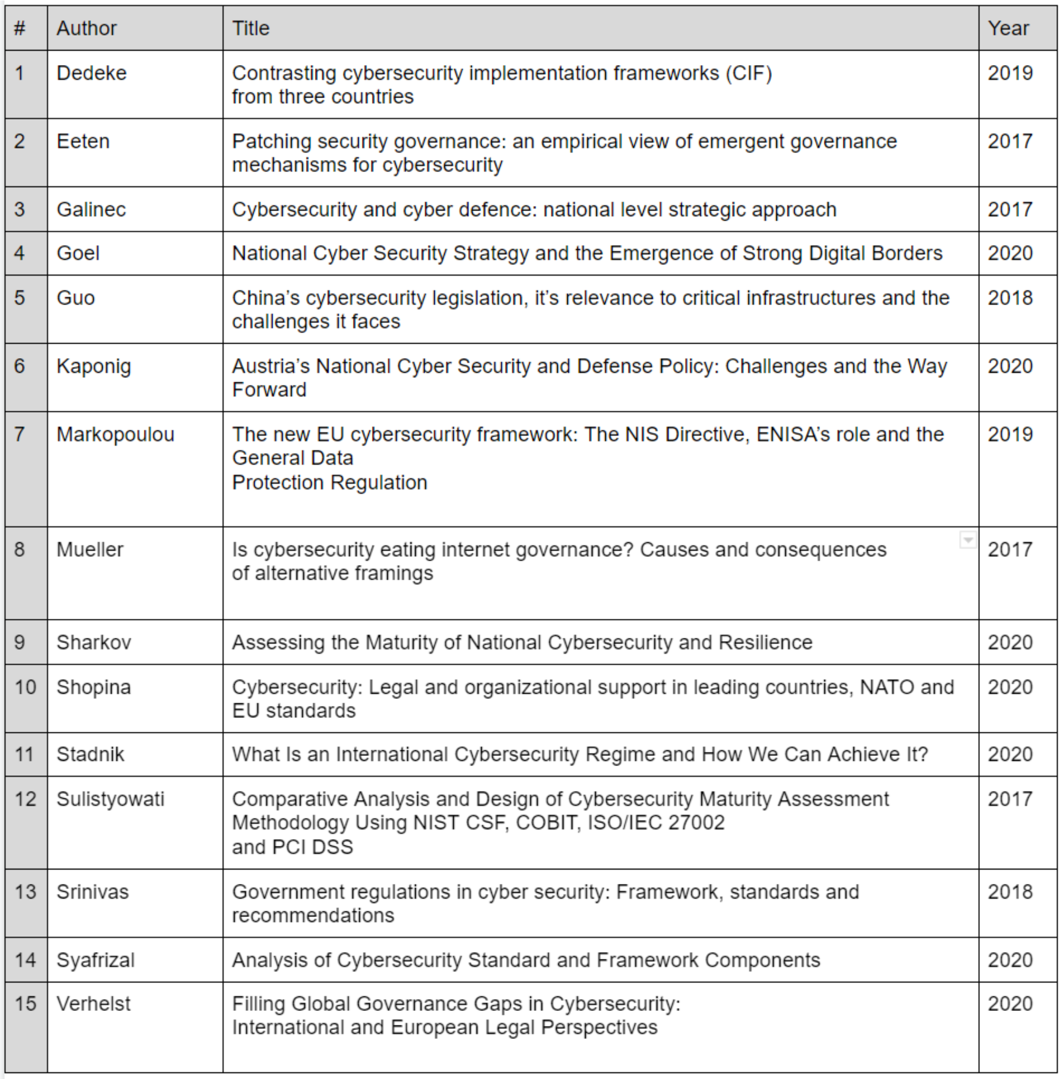
2.1.4 Conceptual matrix

The conceptual matrix is a visual representation of relevant themes found in the literature review. The literature is reproduced by themes or codes that can be generalised across multiple relevant subjects through the literature and presented in the order as followed in the matrix 2.5. The themes that are presented will further be elaborated as sub-themes below in this chapter. Further is a table to present emerging sub-themes created as visualised in 2.6 to establish the connections between the topics.

2.2 Review findings

2.2.1 Cybersecurity frameworks

Several conceptual frameworks in the field of cybersecurity propose a best practice model. The framework shed light on different agendas and purposes in the context of cybersecurity. Several attempts have been conducted to combine the cybersecurity frameworks in recent years (Sulistyowati, Handayani, & Suryanto, 2020). Combining the frameworks can lead to different terminologies, norms and cultural differences as the international branch frameworks are developed by nations and non-profit organisations from countries around the

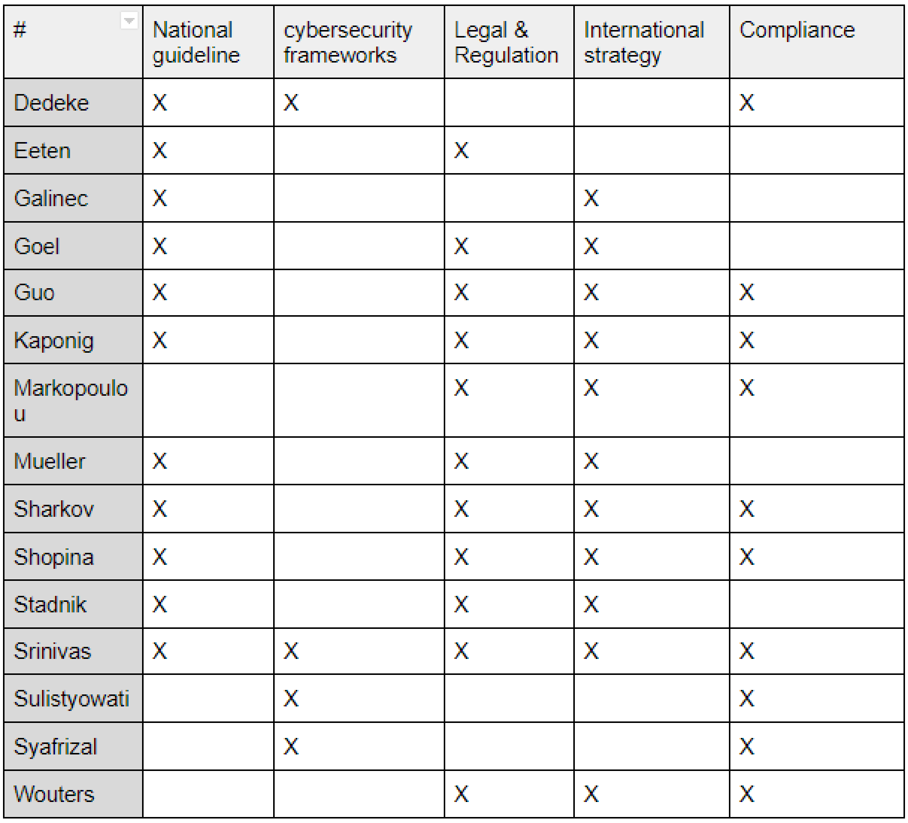


#	Author	Title	Year
1	Dedeke	Contrasting cybersecurity implementation frameworks (CIF) from three countries	2019
2	Eeten	Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity	2017
3	Galinec	Cybersecurity and cyber defence: national level strategic approach	2017
4	Goel	National Cyber Security Strategy and the Emergence of Strong Digital Borders	2020
5	Guo	China's cybersecurity legislation, it's relevance to critical infrastructures and the challenges it faces	2018
6	Kaponig	Austria's National Cyber Security and Defense Policy: Challenges and the Way Forward	2020
7	Markopoulou	The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation	2019
8	Mueller	Is cybersecurity eating internet governance? Causes and consequences of alternative framings	2017
9	Sharkov	Assessing the Maturity of National Cybersecurity and Resilience	2020
10	Shopina	Cybersecurity: Legal and organizational support in leading countries, NATO and EU standards	2020
11	Stadnik	What Is an International Cybersecurity Regime and How We Can Achieve It?	2020
12	Sulistyowati	Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS	2017
13	Srinivas	Government regulations in cyber security: Framework, standards and recommendations	2018
14	Syafrizal	Analysis of Cybersecurity Standard and Framework Components	2020
15	Verhelst	Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives	2020

Figure 2.4: Literature Findings

globe. Nations or companies that try to implement a best practice framework or guideline should consider the possibility that variations may apply depending on how the cybersecurity framework is interpreted. As mentioned earlier, the combination process has been carried out by several researcher in the field. (Sulistyowati et al., 2020) attempts to combine several of the established cybersecurity frameworks into a best practice framework. Figure 2.8 displays the overlapping of the different international cybersecurity framework and is collected from (Sulistyowati et al., 2020) article.

The reasoning for developing such comparison models is that one of the essential steps to enhance an organisation's cybersecurity would be finding the optimal cybersecurity framework. Cybersecurity frameworks consist of different technical specifications, laws & policies organisations should implement (Syafrizal et al., 2020). The complexity of variations in the cyber domains makes it difficult to recommend one particular cybersecurity framework. The tendencies are that there are being developed different cybersecurity frameworks for different sectors, industries and purposes (Syafrizal et al., 2020). The increasing number of cybersecurity frameworks are being established to comply with different requirements and legal



#	National guideline	cybersecurity frameworks	Legal & Regulation	International strategy	Compliance
Dedeke	X	X			X
Eeten	X		X		
Galinec	X			X	
Goel	X		X	X	
Guo	X		X	X	X
Kaponig	X		X	X	X
Markopoulou			X	X	X
Mueller	X		X	X	
Sharkov	X		X	X	X
Shopina	X		X	X	X
Stadnik	X		X	X	
Srinivas	X	X	X	X	X
Sulistyowati		X			X
Syafrizal		X			X
Wouters			X	X	X

Figure 2.5: Conceptual Matrix

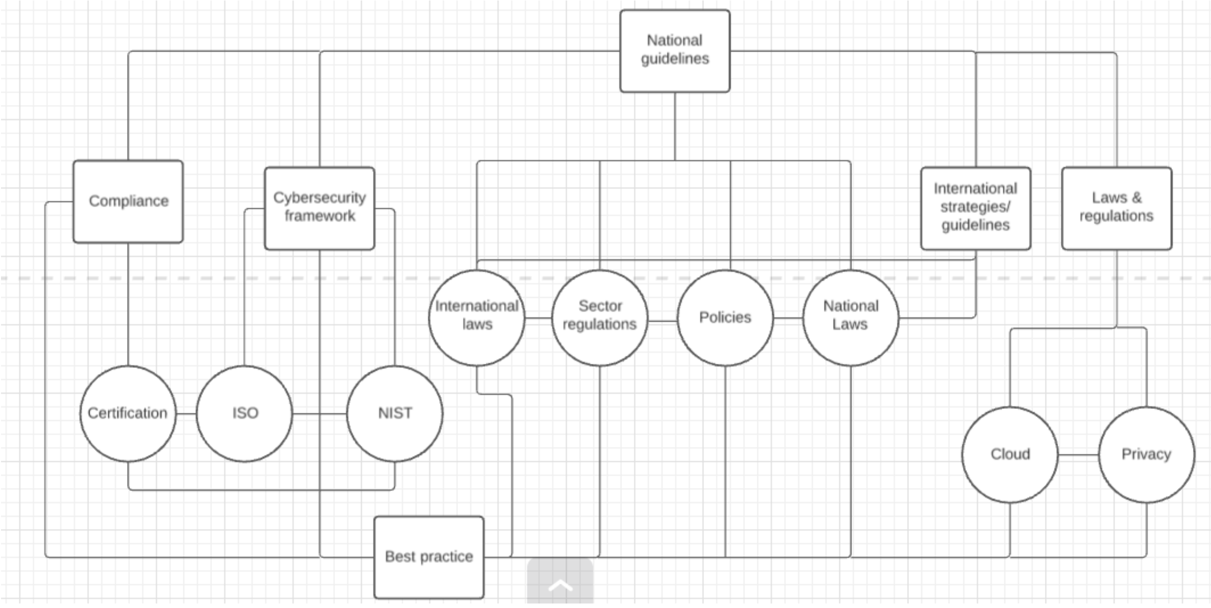
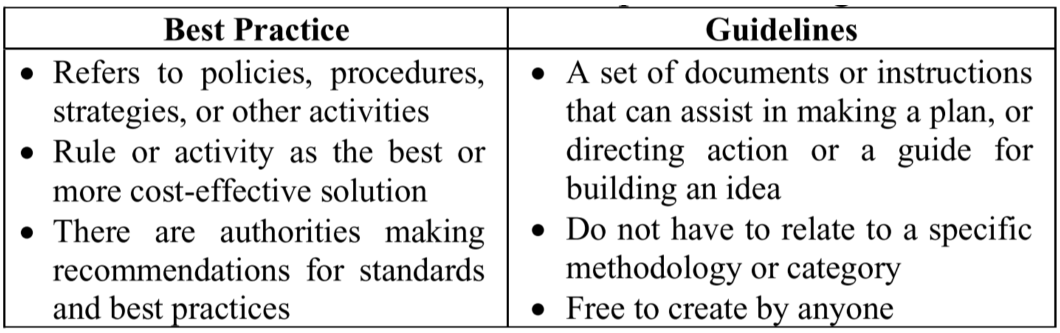


Figure 2.6: Emerging themes

obligations that emerge from the industries & sectors (Markopoulou, Papakonstantinou, & de Hert, 2019). In an ocean of different cybersecurity frameworks, companies may struggle to find the best practice cybersecurity framework for their situations and environment. Taking bits and pieces of several cybersecurity frameworks and customizing them towards a company is considered as an optimal solution. (Syafrizal et al., 2020) found that There are over 30 acknowledged industry cybersecurity frameworks in the literature. Combining several of



Best Practice	Guidelines
• Refers to policies, procedures, strategies, or other activities • Rule or activity as the best or more cost-effective solution • There are authorities making recommendations for standards and best practices	• A set of documents or instructions that can assist in making a plan, or directing action or a guide for building an idea • Do not have to relate to a specific methodology or category • Free to create by anyone

Figure 2.7: Difference between best practice & guideline
(Syafrizal et al., 2020)

these frameworks will cover many of the essential security components as visualised in 2.9

The terminology in cybersecurity can be confusing and divergent for various reasons as guidelines, frameworks best practice are often used interchangeably. Nevertheless, some differences can be pointed out to distinguish the distinctions. (Syafrizal et al., 2020) Proposes a model to explain the terminology with best practices & guidelines, as shown in the figure 2.7. He points out that one of the major differences in the terminology is that best practice and standardisation are often used by established organisations or government institutions. In contrast, are guidelines seen as general overall instructions that can be applied and developed by anyone (Syafrizal et al., 2020).

Companies must strive to find the best cybersecurity framework for their business. This can often be through sectors or relevant industry-standard of cybersecurity frameworks, as this is often where there are common regulations. Sector-based cybersecurity frameworks will continue to emerge in the coming years, as mandatory needs and obligations have to be met, especially related to companies focusing on critical infrastructure and safety. In addition, these frameworks will have to comply with national or international legal and regulatory frameworks in constant development (van Eeten, 2017).

As mentioned earlier, cybersecurity frameworks are often developed for different purposes and will also yield different security elements. None of the international cybersecurity frameworks covers all aspects of cybersecurity elements. Most cybersecurity frameworks are often very general in their form, but have several sub-domains specific to their goals and cover a smaller area of the security landscape. Of the 19 cybersecurity frameworks that (Syafrizal et al., 2020) present, will none of the frameworks cover all areas. The tendency is that most frameworks cover just a few areas. For example, NIST CSF is the framework that covers most components elements of cybersecurity, but this framework only covers a total of 11 elements of the 18 presented in the model.

A summary of some of the well-known and established cybersecurity frameworks will be presented below.

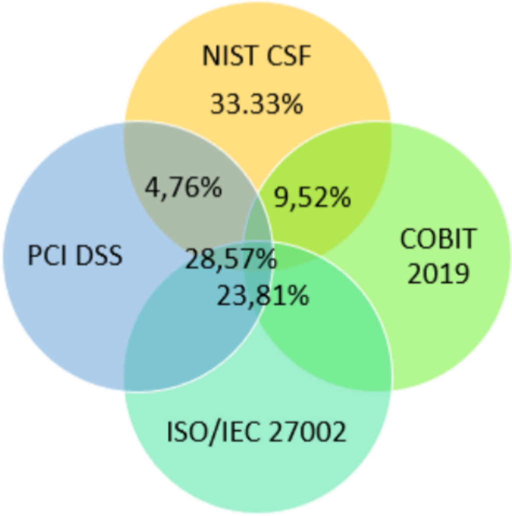


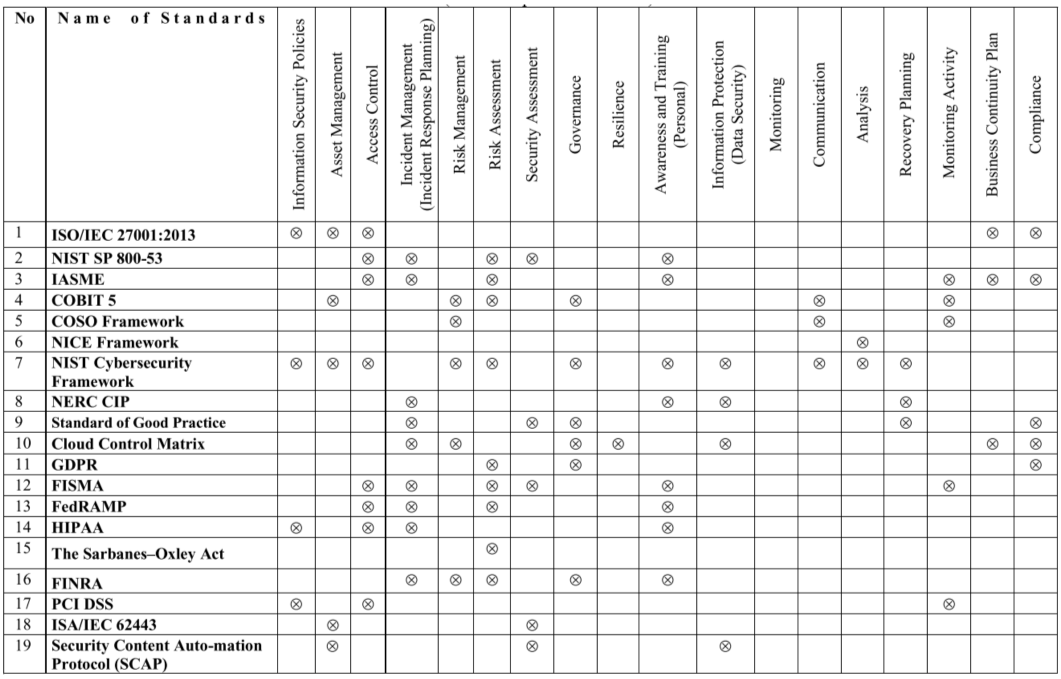
Figure 2.8: A figure of how frameworks can be combined
(Sulistyowati et al., 2020)

NIST CSF

Since as early as 1970, NIST has been established as a cybersecurity framework. It was composed by the Bureau of Standards from the USA and has been one of the leading agencies for developing state of the art cybersecurity best practices. NIST CSF is considered a cybersecurity framework rich in detail with a special focus on the technical aspects. Larger technical organisations often apply this framework. In addition, since the framework was established in the USA, several international companies that have a partnership with the United States will often have a relation to this framework to cope with American regulatory requirements (Sulistyowati et al., 2020)(Syafrizal et al., 2020).

ISO 2700 series

The ISO series is an established overall management framework but have several sub-components related to cybersecurity. The framework proposes guidelines & best practices for organisational information security, focusing on several sub-categories, divided into specific control measures related to security (Sulistyowati et al., 2020). The 27000 series has an ISO specific focus on cybersecurity, yet there is recommendations and standardisation's outside of the 27000 series, which sets requirements towards cybersecurity. The ISO 2700 series tries to establish minimum requirements that can be applied to strengthen the overall cybersecurity (Syafrizal et al., 2020). ISO is an example of a vaguer framework that is more generalised to be adapted across different sectors, as it focuses more on guidance & recommendation rather than specific requirements. This is backed up by (Dedeke & Masterson, 2019) "an ISO standard typically does not describe how the recommendations are to be implemented (Dedeke & Masterson, 2019).



No	Name of Standards	Information Security Policies	Asset Management	Access Control	Incident Management (Incident Response Planning)	Risk Management	Risk Assessment	Security Assessment	Governance	Resilience	Awareness and Training (Personal)	Information Protection (Data Security)	Monitoring	Communication	Analysis	Recovery Planning	Monitoring Activity	Business Continuity Plan	Compliance
1	ISO/IEC 27001:2013	⊗	⊗	⊗														⊗	⊗
2	NIST SP 800-53			⊗	⊗		⊗	⊗			⊗								
3	IASME			⊗	⊗		⊗				⊗						⊗	⊗	⊗
4	COBIT 5		⊗			⊗	⊗		⊗					⊗			⊗		
5	COSO Framework					⊗								⊗			⊗		
6	NICE Framework														⊗				
7	NIST Cybersecurity Framework	⊗	⊗	⊗		⊗	⊗		⊗		⊗	⊗		⊗	⊗	⊗			
8	NERC CIP				⊗						⊗	⊗				⊗			
9	Standard of Good Practice				⊗			⊗	⊗							⊗			⊗
10	Cloud Control Matrix				⊗	⊗			⊗	⊗		⊗						⊗	⊗
11	GDPR						⊗		⊗										⊗
12	FISMA			⊗	⊗		⊗	⊗			⊗						⊗		
13	FedRAMP			⊗	⊗		⊗				⊗								
14	HIPAA	⊗		⊗	⊗						⊗								
15	The Sarbanes–Oxley Act						⊗												
16	FINRA				⊗	⊗	⊗		⊗		⊗								
17	PCI DSS	⊗		⊗													⊗		
18	ISA/IEC 62443		⊗					⊗											
19	Security Content Auto-mation Protocol (SCAP)		⊗					⊗				⊗							

Figure 2.9: Component of different frameworks
(Syafrizal et al., 2020)

2.2.2 International guidelines & strategies

For a functional global market, international regulations must be compliant with national guidelines. As a result, there is a demand for closer international cooperation with cybersecurity. A broader focus towards sharing information & developing international cybersecurity strategies should be prioritized as countries develop their own national strategies and regulations (Shopina, Khomiakov, Khrystynchenko, Zhukov, & Shpenov, 2020).

The EU Commission implements specific cybersecurity regulations, certification schemes and minimum requirements for EU & EEA member nations. Therefore, developing a common European strategy that sets standards towards deliveries globally may increase diversity in the cyber landscape. However, the ability to cooperate between countries with different cultures, norms & politics may be more challenging than a country with the same ideologies (Stadnik et al., 2017).

The EU is not the only stakeholder who wants a more extensive and global cyber strategy. The North Atlantic Treaty Organisation (NATO) states that cyber defence is an important part of their defence and encouraged their member countries to develop a strong cyber defence to defend against cyber threats targeting the alliance. Cooperation between the EU & NATO was enforced in 2016 to strengthen cyber defence cooperation in Europe (Shopina et al., 2020). After the EU implemented the NIS directive, a group to help support international cooperation was created. The initial goals were to increase assistance towards

EU members with compliance and strengthen the international cooperation of cybersecurity outside of the EU (Markopoulou et al., 2019). In recent years, both the EU and the UN have tried to introduce new international strategies. EU has enforced regulations through both the NIS directive and the cybersecurity act. In contrast, the UN has been very clear that laws and regulations also apply in cyberspace and follow up with the necessary instruments if national actors violate this. Nevertheless, it can be seen that a dual strategy can lead to various geopolitical conflicts internationally, and it would be unfortunate if EU regulations were in the way for the UN to introduce global strategies (Verhelst et al., 2020).

As (Stadnik et al., 2017) emphasised, there are several factors for international cooperation in cyberspace. First, in the effort of proposing an international cyber cooperate regime, common grounds must be established. Each nation has its own set of geopolitical interests that they want to front towards international standards. "Although norms are not always codified in law, they often inspire or lead to the development of international law" (Stadnik et al., 2017). Nations have their own agenda to front norms, rules & adjust the international cooperation for international security strategies. Other "superpowers" have also been restructuring their national cybersecurity laws. With a major cultural difference towards Western countries, China has introduced the cybersecurity law, which addresses legislation and regulation related to cyber at a national level and how they should relate to the rest of the global cyber community. China has already taken measures for broader international cooperation and has signed a cyber cooperation agreement with Russia (Guo, 2018).

- "The power of a single country is far from sufficient to effectively address this challenge. Rather, we must jointly solve this problem through international cooperation" (Guo, 2018).

Digital borders The international branch standards increase the overall security by recommending guidance for the security environment by continuously improving their standardisation frameworks for the global market. In addition, regulatory agencies are being established to enforce laws & regulations on the international market and control digital borders. In 2004, ENISA was founded to raise awareness and increase a security culture in the European market.(Markopoulou et al., 2019). ENISA has since been practising recommendations towards the European member states and enforcing mandatory regulations through the NIS-directive of 2016 and the security act (Markopoulou et al., 2019).

The EU is trying to lift the overall security requirement of their member states to a minimum set of standards through regulations to ensure safe data and trade across borders EU borders. A valid concern that (Mueller, 2017) points out is that the security dilemma could occur. Continually improving the security of the EU nations will decrease the security of nations outside of the EU. A protection scheme where the EU is a closed landscape is not necessarily beneficial for a broader international strategy. More robust digital borders will to a greater extent, enable nations and the EU to regulate internet services of their choice, including monitoring data traffic that crosses the land borders and to other parts of the world (Goel, 2020).

2.2.3 National guidelines

The international governance model is seen as the overall strategy, and tendencies lean towards more independent national security guidelines that attempt to comply with the international regulations. National security guidelines and strategies are being developed rapidly, as there is regulatory enforcement to implement national strategies for the EU members through the NIS directive (Markopoulou et al., 2019).

Nations can seek help from (ENISA) who has contributed and developed the (NIS) directive for guidance and advice for national strategies (Markopoulou et al., 2019). As regulatory responsibilities increases, national security authorities stands above a broader responsibility than before where international strategies are mandatory enforced upon them (Galinec, Možnik, & Guberina, 2017). Therefore, guidelines should elaborate on the specific regulations a sector or company is affected by within the national strategies. It should also be specified whether one is covered by a wider scope of regulation, especially concerning critical infrastructure. In addition, the national guideline should say something about which frameworks are suitable for the given sector or industry standard (Srinivas, Das, & Kumar, 2019)(Galinec et al., 2017). National agencies can base their guidelines on several established security frameworks, as the international branch standard is often generalised to fit different sectors (Syafrizal et al., 2020).

There should be a greater focus on how to get both the private and public sectors to interact with each other in the national strategies. For example, instead of referring to international standards, governments security agencies should, to a greater extent, implement national guidelines that apply to them, making it easier for companies to comply with international regulations (Srinivas et al., 2019).

A valid issue is a challenge towards the established commercial branch standards and the frameworks that interest economic and geopolitical gains. Nation-state strategies would yield a significant threat to the developers of frameworks and for those who implement them. As (Mueller, 2017) states, "nation-states are one of the most prominent and serious threats to the cybersecurity of private actors" (Mueller, 2017). Further questions should be raised of how much of the private market's power should have on cybersecurity regulation through certification schemes and whether national agencies can intervene through national guidelines (Verhelst et al., 2020).

Examples of national strategies/guidelines

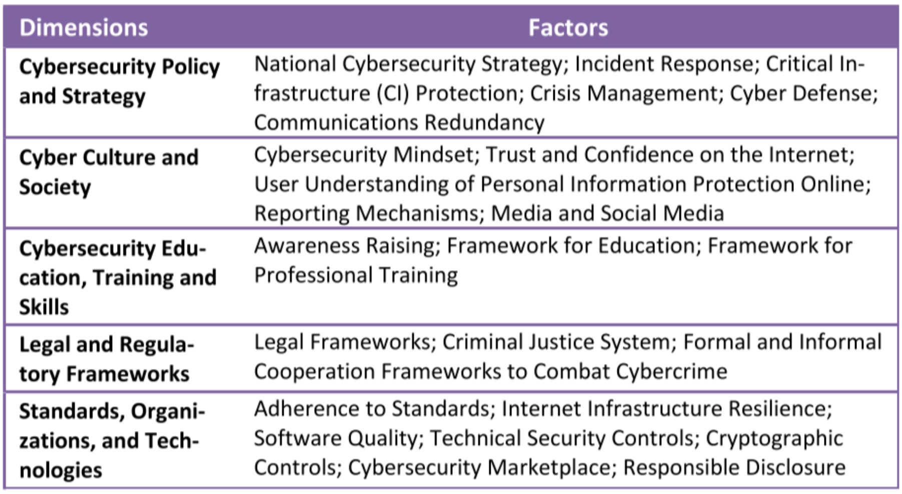
There are various examples of implementations of national security strategies around the world. Australia has tried to introduce a new cyber strategy that focuses on increasing national and international cooperation. Much of the national co-operation was about having exercises and getting the private and public sector closer together. In addition, Australia will have a special focus on bonding with the rest of the world, particularly with the EU, the UN & NATO. One of the biggest obstacles to achieving the national strategy has been compliance with the EU's NIS directive (Kaponig, 2020).

In Croatia, as in Australia, international compliance with regulations is an obstacle to implementation. However, it (Galinec et al., 2017) also highlights other aspects that need to be in place. This means working towards a more coordinated understanding of security and a thorough follow-up of the authorities in general. More consistency of cybersecurity should be prioritized, from the education of employees to the implementation of a system. The Croatian government should, to a larger extent, take the lead on cybersecurity (Galinec et al., 2017).

2.2.4 Compliance

As different frameworks are being developed for national and international use, methods to determine compliance can be measured through maturity tools and models. Maturity models can be used to assist a company in evaluating its compliance towards a given framework or guideline. (Sulistyowati et al., 2020). Implementing maturity models for companies will indicate how well the guideline or framework is compliant and compare it to other stakeholders in the same industry or sector. The same mindset can be transferred to a national level to compare how countries implement national cyber guidelines (Sharkov, 2020). Several nations have already developed a maturity tool for assessing cybersecurity through the Cybersecurity Capacity Maturity Model for Nations (CMM), developed by Global Cyber Security Capacity Center (GCSCC) (Sharkov, 2020). The concept is to create criteria and measurement tools for how cybersecurity capacity is defined across countries have common grounds for comparable basis. The model 2.10 is from the (Sharkov, 2020) article, where he presents some of the factors from the (CMM) maturity model. The model shows an example of different overall requirements and factors that must be in place in a nation.

The approach to comply with the frameworks can be achieved differently, as different frameworks require different compliance (Srinivas et al., 2019). Another method for measuring compliance with security frameworks are through security audits (Syafrizal et al., 2020). The audits are being used as an assurance of compliance, and the companies that meet the requirements are rewarded with certification of the given framework. The growing involvement of national guidelines in the market, together with the rapid increase of international



Dimensions	Factors
Cybersecurity Policy and Strategy	National Cybersecurity Strategy; Incident Response; Critical Infrastructure (CI) Protection; Crisis Management; Cyber Defense; Communications Redundancy
Cyber Culture and Society	Cybersecurity Mindset; Trust and Confidence on the Internet; User Understanding of Personal Information Protection Online; Reporting Mechanisms; Media and Social Media
Cybersecurity Education, Training and Skills	Awareness Raising; Framework for Education; Framework for Professional Training
Legal and Regulatory Frameworks	Legal Frameworks; Criminal Justice System; Formal and Informal Cooperation Frameworks to Combat Cybercrime
Standards, Organizations, and Technologies	Adherence to Standards; Internet Infrastructure Resilience; Software Quality; Technical Security Controls; Cryptographic Controls; Cybersecurity Marketplace; Responsible Disclosure

Figure 2.10: Maturity assessments for a nation, through the CMM maturity model (Sharkov, 2020)

regulations could lead to several complications to fulfill compliance. As (Syafrizal et al., 2020) states:

> Protecting organizations from cyber threats while demonstrating compliance with laws and standards is seen as extremely complex due to the difficulty on choosing the appropriate standard to be used" (Syafrizal et al., 2020).

Certification Several of the international branch standards have developed their own set of qualification schemes as certification audits. A certification is proof of compliance and can prove that companies comply with certain standards and recommendations. As more cybersecurity frameworks emerge, so does frameworks certification. Companies will have to comply with an increasing number of certifications in the market, as both regional, national international frameworks are being developed (Sharkov, 2020). The appliance of certifications requirements is different based on location. Vendors and suppliers that do not comply with the national guidelines or strategies may be taken out of service or denied a trade in the market. Hence it will require the companies to adjust and implement a minimum standard of security (van Eeten, 2017). In the EU cybersecurity act, it has become a mandatory requirement that EU member nations establish agencies or organisations that create and enforce and certifications in the country (Verhelst et al., 2020). Certification schemes that are implemented at national levels require minimums standards of vendors and deliveries. In the UK, organisations that handle critical infrastructure without being certified of the British cybersecurity standard ISO may be rejected to do business in the market (Dedeke & Masterson, 2019).

2.2.5 Policies, laws & regulations

There is a far greater degree of focus on how national guidelines and strategies are to be implemented. National security authorities should, to a greater extent, create national best practices that merge laws and regulations into national guidelines (Srinivas et al., 2019)(Galinec et al., 2017). Several countries have started this process, where critical infrastructure is strictly regulated and complies with national and international regulations. Superpowers like China, the USA & UK are already enforcing regulations in their national cybersecurity strategies. However, the compliance between several national strategies can lead to cooperation on the cross of nations. China introduced the cybersecurity law in 2017. The USA introduced Cybersecurity and Infrastructure Security Agency Act in 2018 & UK the Cyber-Attacks Regulations in 2019 (Guo, 2018)(Shopina et al., 2020). As regulations vary from the nation, there is uncertainty about which regulation should be enforced when foreign companies do business across domestic borders. A more diverse political cyber landscape could emerge if nations are to create their own sets of rules. If no consensus or agreements on key issues are established globally, one will see an increased focus on protecting national interests through laws and national strategies. There are increasing tendencies towards clearer and tighter digital borders, where data traffic is monitored more extensively to safeguard national interests. Such a tendency is undesirable and unfortunate in the long run (Goel, 2020).

> National policymakers face the challenge of striking a balance between regulation and potential chaos on the Internet while at the same time promoting freedom (Goel, 2020).

Another heated issue globally in the context of the rapid emergence of more cloud services. Several challenges are related to the data storage of these cloud services, as national strategies do not necessarily have the same preconditions(Markopoulou et al., 2019). However, laws have to be functional to a degree, and countries should be cautious of implementing additional national security requirements for foreign digital services suppliers (Markopoulou et al., 2019).

2.2.6 Summarize of the literature

The literature uncovered addresses themes related to the underlying process of national guidelines to map challenges of implementation. Developing national guidelines is considered a complex process, as several elements must be accounted for. Developing national strategies in step with the regulatory requirements like the NIS directive has set countries to develop their own national strategies and guidelines.

Chapter 3

Methodology

This section will present the research methodologies and samples that are used to conduct the empirical analysis. The reasoning for several of the choices conducted in the thesis is further described and backed up with the literature on the field. In figure 3.1 there is attached a visual representation of the master thesis process.

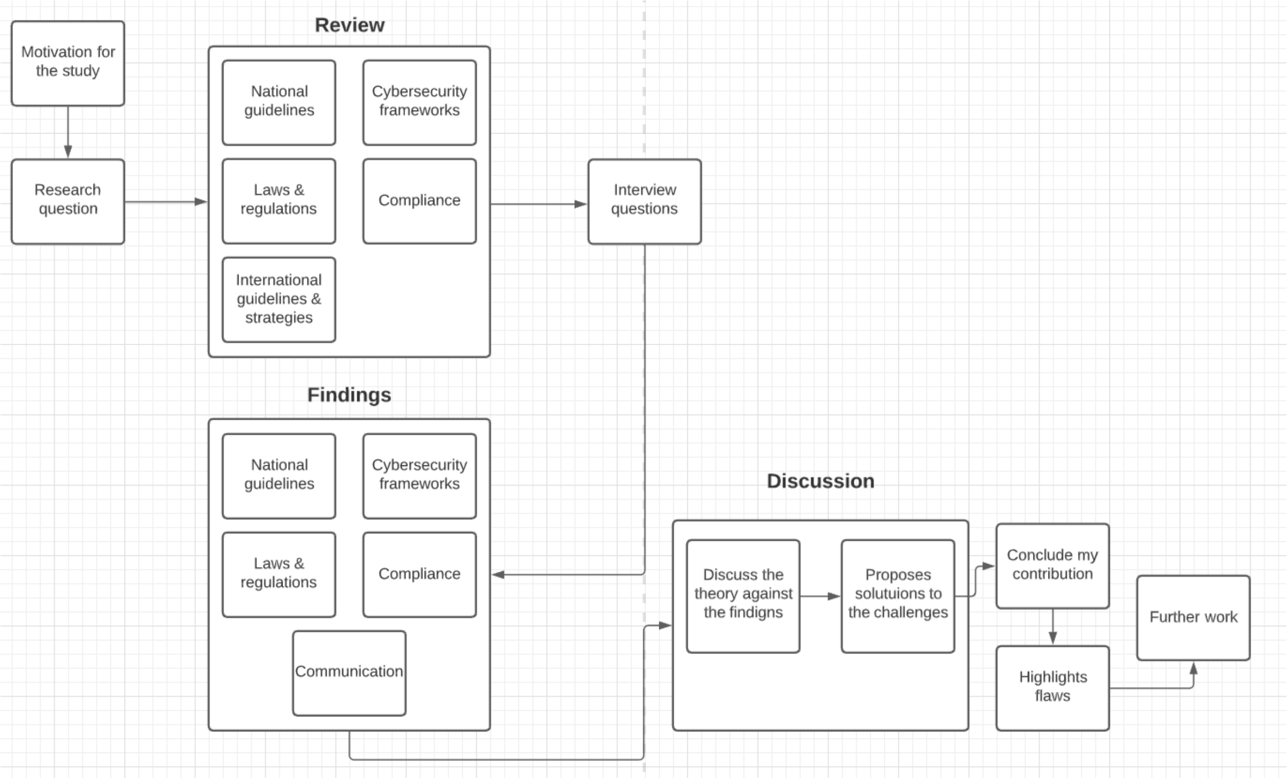


Figure 3.1: A figure of the master thesis process

3.1 Qualitative methodology

In order to answer the research question, a qualitative methodology was chosen. The qualitative collects information in a powerful way where details and behaviours come to light and where phenomenons are explained further. The methods to collect data by doing qualitative research are often highly time-consuming and require a specific research scope (Salkind Neil, 2009). The main empirical data from this study was done by conducting semi-structured interviews. In order to answer the research question, there is a need for a deeper understanding of the environment, interests & opinions surrounding the topic, which the qualitative interview can support with.

3.2 Research design

There is no golden rule of what research design you should choose, yet some pointers should be considered. Research questions that base their form on "how" or "why" often seek to elaborate exploratory problems and be rationalised for a case study. (Yin, 2013). To answer this question, a single case study on the group of Norwegian security authorisations was conducted. A single case study can be used to highlight and contribute to the already existing theory (Yin, 2013). The interview sample, which is discussed later, may be fitted in as an extreme case or a deviation of a normal sample. As extreme case samples can represent and reveal a broader insight of a larger number of people (Yin, 2013). Instead of comparing different nations, sectors or organisations, which would have been difficult to generalise, an insight into Norwegian security as a group was chosen.

The main empirical data collection method was conducted through interviews. Interviews are considered to be one of the most important sources of empirical data when conducting qualitative research (Yin, 2013). In-depth interviews focus on getting the quantitative answers and personal behaviour, the environment, & detailed information about the meaning of the answer (Steinar Kvale, 2015).

To be a good interview listener, the interviewer should have the appropriate amount of knowledge in the field to ask follow-up questions, in the case of a semi-structured interview (Steinar Kvale, 2015). By conducting a semi-structured interview, you will have the ability to enlighten topics or questions that you do not feel fully answered. The semi-structured approach was chosen as the interview method, where interview questions are prepared in advance, as seen in the interview guide, A.1, but allows the interviewer to ask follow-up questions during the interview.

The interview guide was formed based on the research question along with the theoretical knowledge we had. There is a need for the interview questions to be translated from the research problem into relevant and broader interview questions. Asking directly about the research question may be too specific and create a bias in the form of a leaned focus. Being the interviewer, one must act as neutral as possible when conducting the interviews (Steinar Kvale, 2015). We do not want to angle the answers into a direction that pleases our interests as a researcher. The interview questions were further developed into subcategories to highlight the most important topics surrounding the research question.

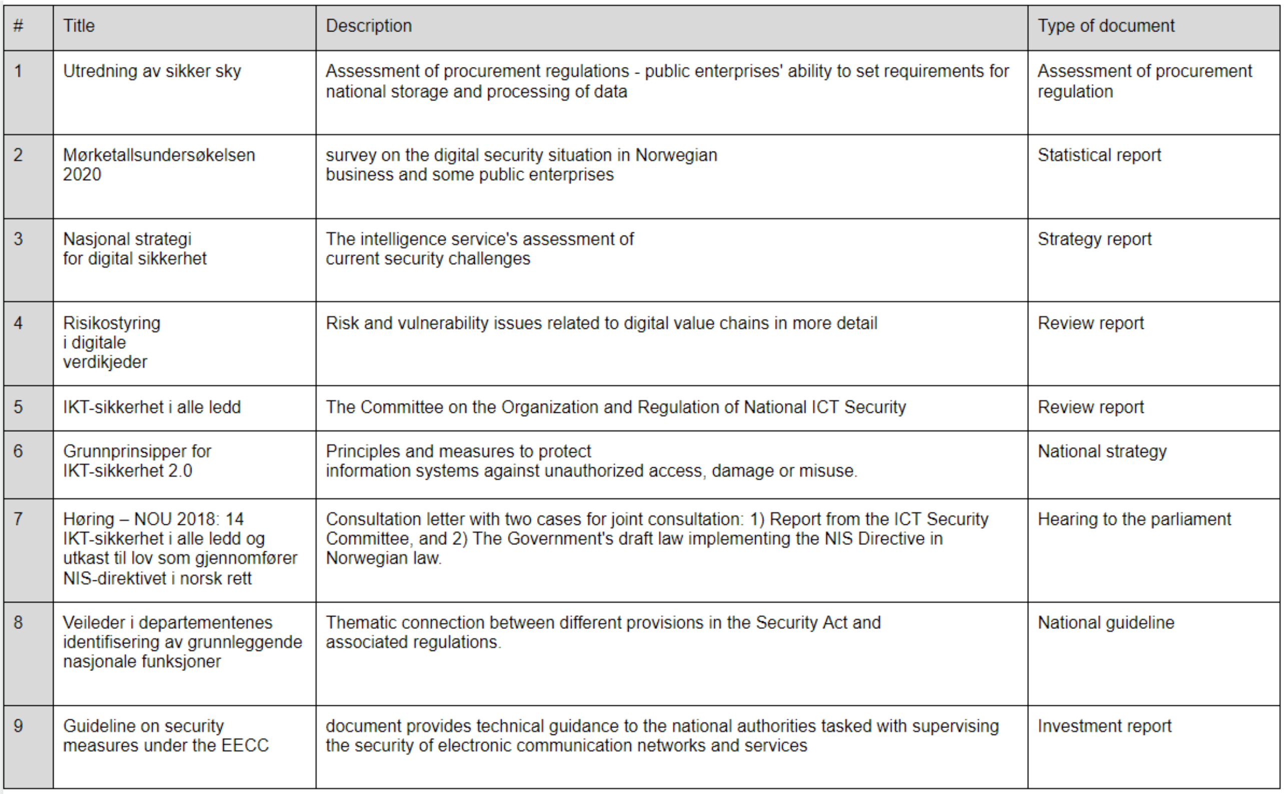
Physical restrictions applied due to the corona pandemic of 2019, resulting in all of the interviews being performed digitally. This was beneficial in a practical sense, reducing travelling, cost & time of the interviews. However, some of the effects when conducting qualitative interviews were also removed. As the interview environment is digital, there were challenges in collecting the respondent's real behaviour & expressions. The interview was recorded with a screen recording that collects the audio and video of the interview. The ability to record the audio enhanced the total interview experience, as there was no need to write down notes during the interview. We focused on creating a good conversation. The interview was later transcribed and coded into categories.

A carefully picked sample among the security authorities in Norway was chosen to gather the required empirical data. The Norwegian security agencies are spread among different sub-sectors such as private and public, nonprofit and commercial. Instead of focusing on one particular organisation that would limit the study, a broad spectrum of security agencies in Norway were selected. To participate in the study, interview respondents had to fulfil the sample criteria as a central security authority. Carefully selected respondents that were considered as "expert" agencies were chosen. A total of 8 organisations, including 8 respondents, were interviewed. To gather sufficient data in the field, all of the interviews were estimated to last 60 minutes each. (Yin, 2013) Describes such interviews as "in-depth interviews", where the interview respondents are considered experts in the field. Newer studies that use qualitative interviews describes the benefits of having fewer respondents, delegating more time to prepare and analysing the interviews(Steinar Kvale, 2015). The interview participants were presented with 25 prepared questions, as shown in B and additional follow-up questions during the interviews.

3.3 Document analysis

Interviews can be a sufficient way to collect empirical data. Document studies can be a way to validate the data that has been collected and decrease inaccuracy and bias. Only conducting one qualitative methodology is not necessarily enough, as interviews have weaknesses due to the respondent's reliability & validity.

Security agencies publish recommendations of best practices to the public domain yearly. It would be natural to include some of the documents. These reports are published regularly, and with open access on the internet, the availability of the documents was not a problem. Some of the interview respondents also recommended including some documents in the study and referred to several documents and the interviews. Reports from government committees & Risk and threat reports are some of the documents included. A visual representation of the



#	Title	Description	Type of document
1	Utredning av sikker sky	Assessment of procurement regulations - public enterprises' ability to set requirements for national storage and processing of data	Assessment of procurement regulation
2	Mørketallsundersøkelsen 2020	survey on the digital security situation in Norwegian business and some public enterprises	Statistical report
3	Nasjonal strategi for digital sikkerhet	The intelligence service's assessment of current security challenges	Strategy report
4	Risikostyring i digitale verdikjeder	Risk and vulnerability issues related to digital value chains in more detail	Review report
5	IKT-sikkerhet i alle ledd	The Committee on the Organization and Regulation of National ICT Security	Review report
6	Grunnprinsipper for IKT-sikkerhet 2.0	Principles and measures to protect information systems against unauthorized access, damage or misuse.	National strategy
7	Høring – NOU 2018: 14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet i norsk rett	Consultation letter with two cases for joint consultation: 1) Report from the ICT Security Committee, and 2) The Government's draft law implementing the NIS Directive in Norwegian law.	Hearing to the parliament
8	Veileder i departementenes identifisering av grunnleggende nasjonale funksjoner	Thematic connection between different provisions in the Security Act and associated regulations.	National guideline
9	Guideline on security measures under the EECC	document provides technical guidance to the national authorities tasked with supervising the security of electronic communication networks and services	Investment report

Figure 3.2: Documents included as supplement for the findings

documents included is presented in 3.2. Document studies also bring weaknesses, and it is important to keep in mind that the data may be bias, outdated and or considered secondary knowledge. Therefore, the document analysis is primarily used to verify the respondents' data from the interviews, including adding figures and quotes that can enhance the validity of the respondent's data.

3.4 Validation & Reliability

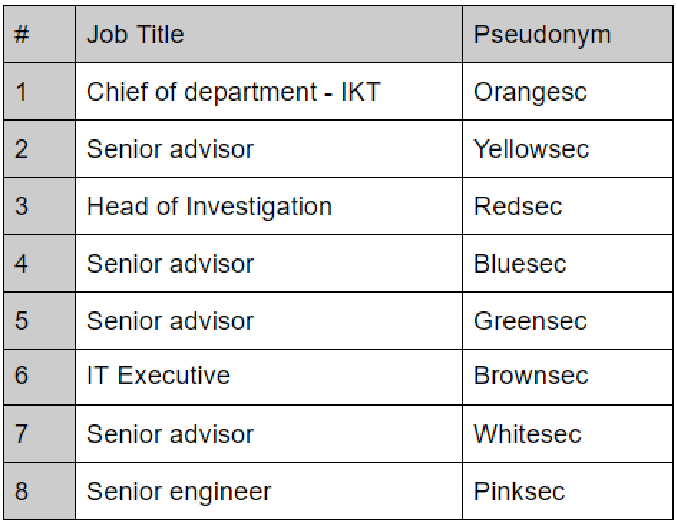
To ensure that the produced material is less biased, considerations regarding validations & reliability was important. Reliability is based on how researchers can conduct the same study repeatedly and produce the same results (Yin, 2013). Notable and major choices that could affect a reproductive study are documented to the best of my knowledge along the way.

Interview respondents may be a valid source of information, yet it is important to keep in mind that there are also biases when conducting interviews. Respondents may have problems remembering certain events, topic or giving an inaccurate representation of the given facts. The document studies were included as an empirical supplementation to validate the reliability of the interviewed data further.

3.5 Ethical challenges

There is a duty for all researchers to be able to protect the interview respondents confidentially and anonymity (Steinar Kvale, 2015). The recording, storage & transcribing should be conducted ethically. To protect the anonymity and identity of t 1

The respondents and their associated organisation, pseudonyms were being used. In addition, the draft of the thesis was sent before the final delivery to ensure that their anonymity was intact and that the findings presented in the analysis were coherent with the interview data from the interviews. A table that presents an overview of the sample is presented 3.3where the job titles and associated pseudonym are presented.



#	Job Title	Pseudonym
1	Chief of department - IKT	Orangesc
2	Senior advisor	Yellowsec
3	Head of Investigation	Redsec
4	Senior advisor	Bluesec
5	Senior advisor	Greensec
6	IT Executive	Brownsec
7	Senior advisor	Whitesec
8	Senior engineer	Pinksec

Figure 3.3: Interview sample overview

3.5.1 Consent form

Before conducting the interviews, the respondents emailed a consent form that informed them about the privacy & data collection surrounding the interview. This informed the respondents about their rights about insight into their data, the storage & how the overall data is being managed. The consent form is attached in **??**.

3.5.2 NSD

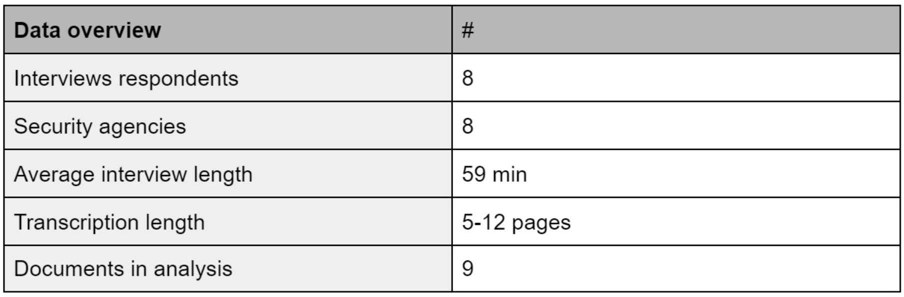
To conduct the study, an application was sent to the Norwegian centre for research to validate the sample & approve that it follows general rules of data storage and privacy of the interview respondents. The application was approved to gather general information about respondents with anonymity, meaning that the data presented in the thesis should not be able to identify individuals.

3.5.3 Storage

To ensure lawfully and ethical storage of the data guidance, terms & conditions provided by UiA & NSD was followed. The data was stored at UiA own cloud, provided by Microsoft. The process to save the files on UiA's own cloud was also approved by NSD in the research application.

3.5.4 Transcription

Once the interviews were complete, transcription of the audio files was conducted. The process of transcribing was time-consuming as each audio file contained an average of 59 minutes of recording, which resulted in several hours of transcription work for each interview. In total, each interview produced an average of text files on 5-12 pages, which resulted in a vast amount of raw text. Some statistics concerning this process is illustrated in fig 3.4.



Data overview	#
Interviews respondents	8
Security agencies	8
Average interview length	59 min
Transcription length	5-12 pages
Documents in analysis	9

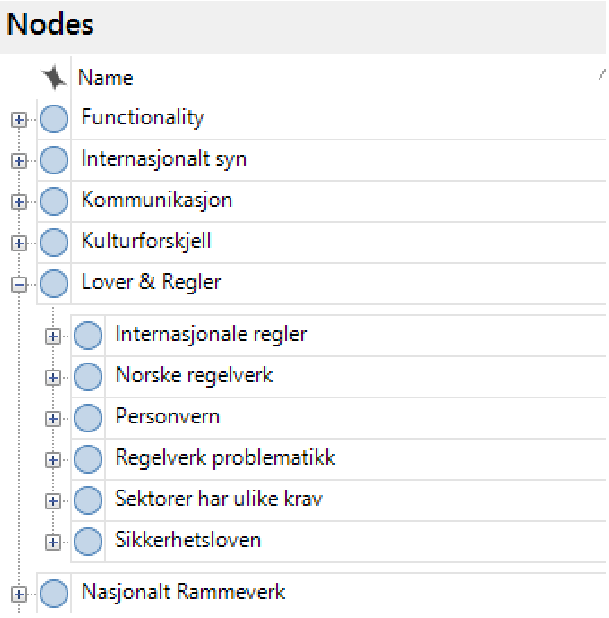
Figure 3.4: Empirical data overview

3.6 Qualitative data Coding

An important factor of qualitative analysis is coding the findings. The codes will get the essential information from the transcription and will represent the themes for the findings. D(Tjora, 2012) describes coding as one of the most important elements of qualitative analysis. Having an open mind and avoiding premature conclusions. An inductive approach where one reduces expectations of the empirical data is important. The researcher should also not be afraid to cultivate new codes, categories, or themes that enrich the empirical data. The results from the empirical finding, which are presented in chapter 5, reveals that the empirical data has discovered several new themes that were not anticipated from included theory chapter of the study.

3.6.1 Groups of coding

The coding was based on a functional sorting-based approach where main themes and sub-themes were structured to reproduce empirical findings more easily. Nvivo 12, which was



Nodes

Name

- Functionality
- Internasjonalt syn
- Kommunikasjon
- Kulturforskjell
- Lover & Regler
  - Internasjonale regler
  - Norske regelverk
  - Personvern
  - Regelverk problematikk
  - Sektorer har ulike krav
  - Sikkerhetsloven
- Nasjonalt Rammeverk

Figure 3.5: Snapshot of computer software used for coding

the software used to analyze the data, categorizes the codes into structured subgroups, as shown in figure 3.5. This way of analyzing makes it easier to go back to a later point in the analysis to confirm various arguments and statements. Nvivo12 also has several features that make it easier both practically and visually. One feature that I have chosen to include is the word cloud. The illustration presents the themes in the codes based on how often the words are repeated. Words with less than 6 letters were excluded to avoid conjunctions. The word cloud is shown in 3.6.

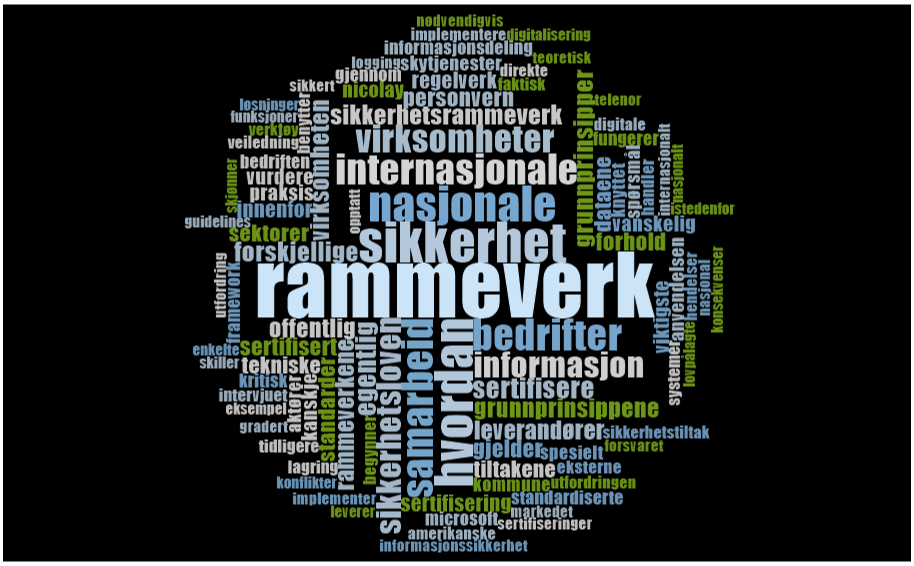


Figure 3.6: Snapshot of word cloud

3.7 Context of Norway

Norwegian security agencies are separated into sub-branches with their own set of goals and objectives. The security agencies within this sample work with different genres like privacy, critical infrastructure, & security governance. As several agencies have built up freely or mandatory cooperation between them, there are still ongoing processes of more integration of the security cooperation across different sectors (Regjeringen, 2021).

To establish a sample that can be presentable concerning the research problem of the thesis, it was important to obtain empirical data from different sources of the industry. The sample consists of several national agencies that elaborate on common national components and strategies. As (Regjeringen, 2019a) states that its important to see the context of several areas of cooperation:

> "Digital security must be seen in a holistic perspective, across sectors and levels of government, and in the context of other areas of the cooperation for social security" (Regjeringen, 2019a). (Translated from Norwegian).

The security agencies alone cannot defend against foreign threats. It is a coordination process that has to be conducted by the citizens, the private & the public sectors (Regjeringen, 2019a). Norway's further government plan is to integrate several of these agencies into strengthened cooperation. The idea is that public and private sectors can work together and share information and experiences. This is a part of the long haul digitisation strategy in the public sector from 2019-2030 in Norway (Regjeringen, 2019a). A common digital interaction between the sectors consists of legal, technical, organisational & semantic cooperation.

The digital security agencies have also made an effort for cooperation between them. In 2017 a centre for security agencies was established in Oslo. The centre had representatives from several government agencies representing the national security, organised and led by the Norwegian security authority (NSM) (NSM, n.d). These agencies may work with different goals and objectives. However, they tend to have the same vision to strengthen & maintain the overall national security.

Chapter 4

Findings

This chapter will summarize the findings from the interviews and document analysis. The findings are segmented into codes from the empirical analysis and are presented into the corresponding categories below to answer the research question. In addition, quotes from the interviews respondents and document analysis are being supplied to validate the data.

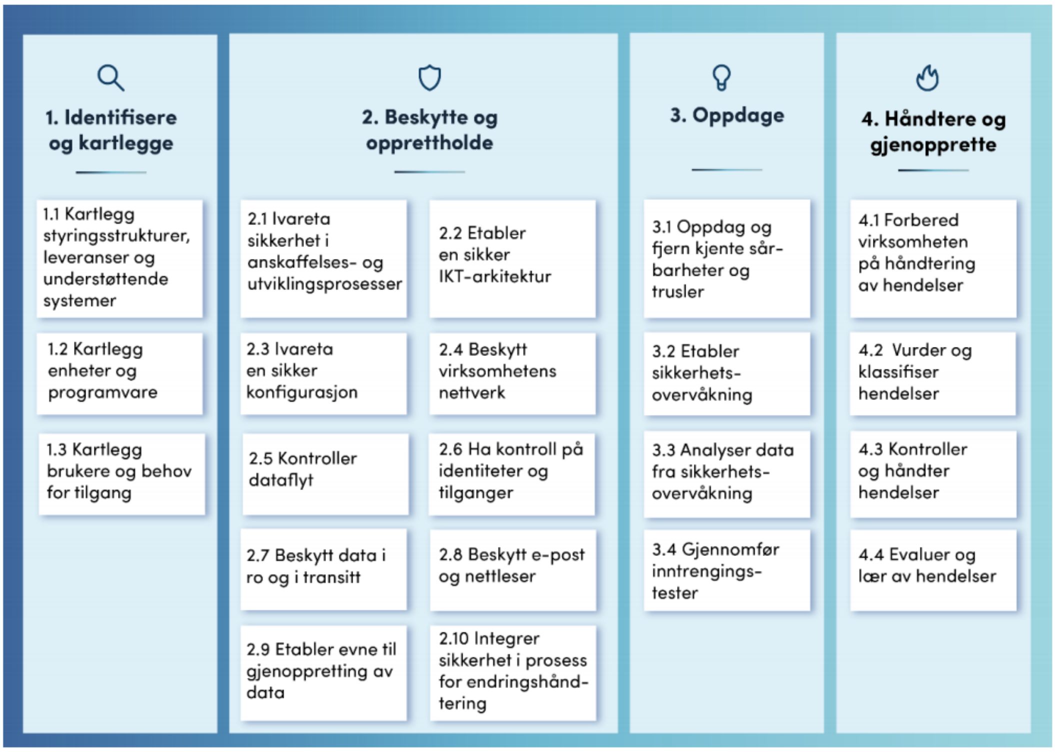
4.1 National guidelines

Several countries in Europe have already developed their own set of national guidelines in one form or another. A common factor among the national guidelines is that they base their requirements on an already existing cybersecurity framework. This is also the case for some of the Norwegian guidelines. For example, "NSMs grunnprinsipper 2.0" is based on several established cybersecurity frameworks, such as the ISO 27000 series. NSM's basic principles for ICT security are a guideline developed by NSM for how the companies in Norway can secure their information systems.

NSMs basic principles are well established in the Norwegian market. Moreover, NSM's basic principles are often used as a reference point for other Norwegian guidelines, laws and or regulations. Therefore, implementing NSM basic principles is considered good practice in Norway, even for smaller companies. NSM's basic principles 2.0 are presented in 4.1.

> "NSM's basic principles are based on international frameworks, which means that if you follow NSM's you will have a certain compliance with different international frameworks" - (Pinksec)

Crating a guideline that fits every single company is probably not possible. In Norway, there are several varieties of industries and type of businesses, both in competence, sector and



1. Identifisere og kartlegge

1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer

1.2 Kartlegg enheter og programvare

1.3 Kartlegg brukere og behov for tilgang

2. Beskytte og opprettholde

2.1 Ivareta sikkerhet i anskaffelses- og utviklingsprosesser

2.2 Etabler en sikker IKT-arkitektur

2.3 Ivareta en sikker konfigurasjon

2.4 Beskytt virksomhetens nettverk

2.5 Kontroller dataflyt

2.6 Ha kontroll på identiteter og tilganger

2.7 Beskytt data i ro og i transitt

2.8 Beskytt e-post og nettleser

2.9 Etabler evne til gjenoppretting av data

2.10 Integrer sikkerhet i prosess for endringshånd-tering

3. Oppdage

3.1 Oppdag og fjern kjente sår-barheter og trusler

3.2 Etabler sikkerhets-overvåkning

3.3 Analyser data fra sikkerhets-overvåkning

3.4 Gjennomfør inntrengings-tester

4. Håndtere og gjenopprette

4.1 Forbered virksomheten på håndtering av hendelser

4.2 Vurder og klassifiser hendelser

4.3 Kontroller og håndter hendelser

4.4 Evaluer og lær av hendelser

Figure 4.1: NSM's guidelines for Norwegian companies
(National Security Agency, 2020a)

size. Therefore, national guidelines should be carefully crafted and adjusted to fit national and international regulatory recommendations and requirements.

Norwegian companies will not necessarily have problems implementing national guidelines, but it can lead to greater problems for foreign international companies. A disadvantage of introducing national guidelines is the communication problems towards international larger companies. Norway should not risk international cooperation leaving the Norwegian market due to too strict Norwegian cybersecurity guidelines. If Norway creates mandatory regulations that affect large international suppliers, such as Microsoft, Amazon or Facebook, it is not entirely certain that they will comply, considering the size of Norway on a global basis.

> "The established suppliers have market power, and the power is very unevenly distributed. The largest companies have a budget that is much larger than Norway's total budget" (Pinksec).

The main reasoning for developing strict national guidelines are various. An argument is that the national guidelines often are more compliant with laws or regulations. Another argument is that national guidelines are developed in the native language and are easier to understand and work with, as the terminology can be understood and interpreted by additional employees. How national guidelines are implementing depends on the company that applies them. However, to a greater extent, the national guidelines should be embedded into the company culture, as "The cybersecurity guidelines are an integral part of our work procedures, they are an integral part of national security, and our entire social structure" (RedSec). National guidelines also tend to be a simplified version of a cybersecurity framework and will often yield some of the basic principles in a figurative sense and will, in many cases, be easier for less experienced employees to understand.

Another aspect of implementing national guidelines in the Norwegian context is the ongoing focus on a more collaborative public sector. Public organisations are spread among different sectors with a vast amount of expertise with different security approaches. Consequently, there is a demand for components or platforms that, to a greater extent, could enhance the focus on common guidelines related to cybersecurity in the public sector. Unfortunately, today's situation is that many organisations in the public sector deploy their own solutions instead of collaborating on common components.

> "Many develop their own solutions where, strictly speaking, common components should be used. It is everything from authentication but also the exchange of data. There is a need to put in place more national common components" (Orangesec).

The Norwegian government is addressing the issue with the development digitisation plans for more common strategies and platforms. The figure 4.2 is collected from the national strategy report of Norway that was published in 2019 and is a visual representation of strategic cooperation between different actors. There is an overall agreement that there is a need for a more common component in the nation, as (Orangesec) states:

> "In the long run, to get good and valuable digitization. There must be additional national common components in place so that you have the opportunity to reuse data to a much greater extent than what is in place today" OrangeSec.

Cooperative projects are already in motion. One of the measures in the cyber field has been to establish a common national cyber centre that brings together many key players for information sharing and experience transfer. The Norwegian national cybersecurity centre was established in November 2019 in Oslo, where stakeholders related to the field could meet physically to address ongoing issues. The cybersecurity centre has several affiliated partners, both from private companies to public organisations like municipalities. The goal is to develop a community where companies, both in the public and private sector, can ask for advice, highlight concerns and work together to resolve security issues & concerns. (NSM), the leading operator of the centre has regularity situation reports for the included partners to map out the threat landscape. Unfortunately, the centre's full potential has not been developed and exploited optimally due to physical restrictions of the coronary pandemic.

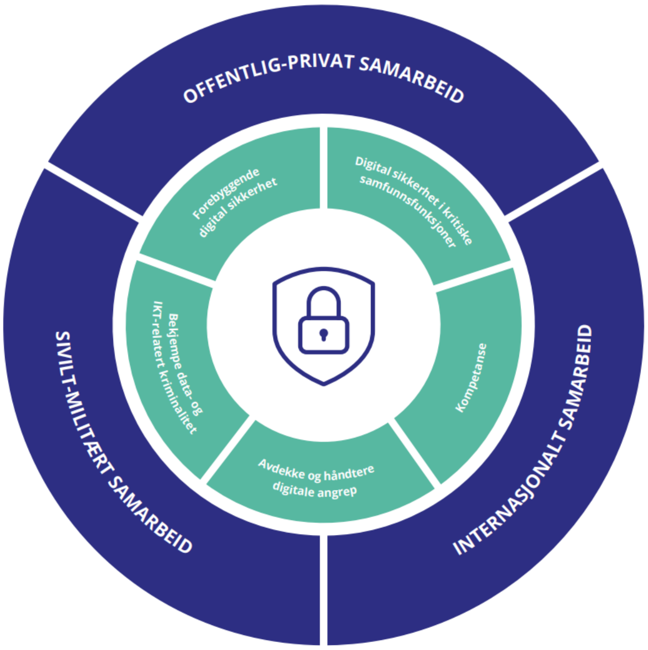

OFFENTLIG-PRIVAT SAMARBEID
Forebyggende digital sikkerhet
Digital sikkerhet i kritiske samfunnsfunksjoner
Bekjempe data- og IKT-relatert kriminalitet
Kompetanse
SIVILT-MILITÆRT SAMARBEID
INTERNASJONALT SAMARBEID
Avdekke og håndtere digitale angrep

Figure 4.2: Model of a national cooperation between military, private and public sector (Regjeringen, 2019b)

4.2 Cybersecurity frameworks

Following a cybersecurity framework can be used as an indicator to communicate quality and ensure that the companies are on the same page related to security. However, part of the challenge is that following cybersecurity frameworks is not necessarily entirely voluntary. Different sectors may require different cybersecurity frameworks, which in practice means that private commercial companies are indirectly forced to follow the requirements to compete in the market. (Orangsec) states: "private companies are indirectly forced to be able to deliver in various sectors. It is very much regulated. I have no faith in that volunteerism to certify."

Implementing a cybersecurity framework could indirectly create more paperwork & bureaucracy, yet if you adapt it correctly, it can enhance the structure and quality of the company's security in the long term. Furthermore, enabling a clear structure through a cybersecurity framework will also be efficient towards being adaptive & agile for adjustments and changes in the future, as you can always lean toward a cybersecurity framework.

As mentioned earlier, some sectors and industries have already enforced mandatory requirements towards cybersecurity frameworks, such as the requirement to be ISO certified. Various sectors even have the implementation regulated by law, for example, the financial industry. This can create a false sense of security if not followed up correctly. As (Redsec) states: "ISO & Nist contribute to a camouflage of a problem to the same extent as they contribute to addressing a problem and solving it" (Redsec)

Larger companies will have a greater extent of security experts who will understand the benefits of different frameworks and differentiate the specification and needs for the companies requirement. Norway consist of a broad spectre of small and medium-sized companies that do not necessarily have their own employees who specialize in cybersecurity. An employee who works with the economy or HR may have difficulties understanding cybersecurity frameworks. The issue related to lack of knowledge has been addressed through several consultancy companies in the market. Consultant companies will deliver and assist with the implementation of cybersecurity frameworks, often through certification schemes. This is not the case for cybersecurity guidelines, as these are often just a set of recommendations without any form of certification schemes.

4.3 Compliance

Certification may be a good solution for companies that continuously improve their overall security, as certifications often require external auditors to be certified, hence a new source of review and feedback from someone outside the company.

> To be able to give trust to customers and services, you want to be certified. We require ISO certification when we order things. Following certified schemes will give confidence to other government agencies (Brownsec).

Certifications can also be used as proof of quality. In addition, companies validated through certification schemes can use it as a sales argument and a market advantage towards their customers. However, the certification itself should not be viewed as the main goal for companies. Rather, it should be used to acquire knowledge and expertise for employees and the companies overall.

Several EU nations have ongoing discussions about implementing their own set of national certifications for their equivalent guideline. The EU already requires their nations to enforce and follow up EU regulations like the NIS-directive. However, issues related to the maintenance of each certification scheme and how it would affect the global economy arise. European deliveries can be complex. The global economy is indeed global. Finding a supplier who is fully compliant with national guidelines could be an upcoming issue. Even ENISA's report (ENISA, 2020) states that national authorities should address the issue and point out that cybersecurity frameworks may be a good idea to solve, but too strict enforcement is not recommended. Maintaining a national guideline based on one or more frameworks takes time, money & resources. National agencies that base their guidelines on cybersecurity frameworks are constantly being updated and may find themselves constantly updating the guidelines to be compliant with the cybersecurity framework.

> "Competent authorities should take into account that some (especially the large) providers may operate in several EU countries, and that it would be cumbersome

> for these providers adopt different standards in different countries. In this respect it could be useful to allow providers to use international standards, which are widely used across the EU and in this way reduce compliance costs for these providers" (ENISA, 2020).

Being certificated does not necessarily mean that a company conduct good cybersecurity. A company that is being certified could, as mention earlier, lead to an illusion of good cybersecurity if the processes of maintaining the cybersecurity framework are not being sustained properly (Bluesec). Even advise against being certified. "We do not recommend any public enterprises to certify themselves in ISO 27001 because we do not see the need" (Bluesec). The rationalization for the statement is that national guidelines are often based on ISO or NIST. That certification of cybersecurity framework is an extra and unnecessary element where resources are spent. Several of the respondents in the study recommend NSM's basic principles as a low-threshold standard that both can implement in small, medium and large businesses. NSM's basic principles are based on several cybersecurity frameworks, making this a good alternative to cybersecurity frameworks in the Norwegian market. It is also conceivable that NSM principles will eventually be baked into an overall Norwegian strategy, with mandatory enforcement, where specifically sectors and or the entire public sector set requirements for vendors. "we want to promote NSM as an approval scheme that people should use." (Brownsec).

Certification of cybersecurity frameworks or guidelines may also be seen as a barrier for several actors to compete in the market. In many cases, the private sector will indirectly be forced to take certifications to meet different requirements in different sectors regulated by law. Certifications would be less popular if they were completely free, without obligations required by sectors or companies. Unfortunately is the certification process both expensive and time-consuming. As a result, there is a tendency for companies to outsource this type of job to consulting companies which has more knowledge in the field.

4.4 Privacy, Laws & regulations

4.4.1 Sector regulations

In Norway, there are also sectors based regulations that are strictly monitored through security audits. Supervisors from the government will validate that the companies in the sector follow the requirements. The sector philosophy is heavily embedded in Norway, where each sector will have to comply with various requirements as they are affected by different laws & regulations.

An example is an energy company in Norway that produce electricity. The company will have to deal with a vast amount of questions that may affect them. The below example is just an illustration of relevant questions.

- Are we managing national security values?
- If yes, should they be graded?
- Are there any regulations from the government in this sector?
- Are we handling critical infrastructure?
- Are there any specific requirements for our vendors or customers?
- Are we following international requirements?

One of the first assessments that should be evaluated is if the company is handling data categorized as an important Norwegian property or that the data is of Norwegian geopolitical interests. If the data is not graded, the process will proceed to regulatory requirements. If no national regulatory legalisation is affecting the company through sectors or other industries, there should be an individual assessment through the NIS directive, as there are several levels of compliance on an EU level. Smaller power companies may not have the same regulatory requirements as large companies. Each company will have to assess which regulation to follow. "The biggest challenge is probably to communicate which regulations you fall under." (Redsec)

Companies that work in the energy sector must secure their digital information system to safeguard confidentiality, integrity, and accessibility. According to the digital information system's type, structure and function, it is the individual company's responsibility to plan, implement, and maintain security measures. "Some will outsource services to save large sums of money, but it is important to have security in mind as well." (Pinksec) Companies must ensure that security is either maintained or improved for companies in the energy sector to outsource services.

4.4.2 Privacy

In the last several years, almost everyone has heard the term (GDPR), which stands for general data protection regulation. The GDPR elaborates nothing more than general privacy recommendations. Companies should ensure sufficient security when processing personal data and that you use a risk-based approach and making sure that it is sufficient. A positive remark is that GDPR is considered overall guidance of how you should implement and will correspond well with other requirements and are often not in conflict with anything related to other laws or regulations. The conflict between national guidelines and GDPR is not an issue, as is developed by the companies own risk assessments.

> "GDPR does not say much about how to secure the systems. It says a lot about assessments you should make in terms of personal information. They say that you should secure it adequately, but not so much about what to do and how to secure it (Yellowsec).

Companies could be fined with regulatory fees if the minimum requirements of GDPR are not followed adequately. The EU sets mandatory requirements for what each European country must have in place for security and privacy.

Norway, which is not a part of the EU, still have to follow much of the same regulations through the partnership under the EEA Agreement. A nation that are members of the EU OR EEA partnership must follow the basic rules for cybersecurity, such as European sector regulation, GDPR & NIS Directive. These rules set the guidelines for how to develop further national rules and guidelines. National guidelines cannot exceed the EU's regulations, except for classified national information. This means that, in principle, it is not possible to set up regulations that prevent ungraded data from entering EU countries. Further, this means that companies that deal with classified information can seek to find shortcuts, like grade classified information that necessarily is not. As (RedSec) states: "It is easier to grade something classified than to assess whether it should be graded, and then it is by definition unavailable" (Translated from Norwegian)

The EU is an area that must be taken into account, but one must also consider whether the other superpowers from Asia & America will cooperate when developing national guidelines. To establish national cybersecurity guidelines, there must be clear lines as to whether international regulations will affect the national guideline. To further develop national guidelines, broader cooperation must be established between foreign countries where compliance at an international level must be met. For example, Norway's guidelines on privacy are more or less suggestion & advice where each company has to decide if they comply with the enforced regulations.

4.4.3 Cloud storage

During the corona pandemic outbreak of 2019, many companies had to move over to a cloud-based system in one way or another. Employees had to work from home, and cloud-based solutions were unavoidable. The corona situation led to home offices becoming the new norm in society. A concern was that the companies were not ready for this transition and that cloud services became a major challenge and risk vulnerability for several companies.

Companies have to assess the risk and consider if the cloud provider is trustworthy. Sometimes the security related to the hardware is forgotten. Everything related to IT will eventually end up in a physical object.

There are several benefits with cloud services, one factor is money, but another is the dynamic cloud allocation of resources. Small and medium-sized companies will often have the benefits of outsourcing data to the cloud as a cost-related issue. However, they will also get benefits from cloud provider cybersecurity at the same time. The sheer security of your data can often be better-taken care of by Microsoft or another giant supplier. Data centres in Norway store data for foreign companies, such as Microsoft, which could create a misdirection for Norwegian companies. It is a grey area that Norwegian public companies stores sensitive data in the cloud. Data that crosses national borders should have strict demands towards the third party supplier that access and handles them. "Microsoft Norway may be asked to provide all the data they have about a given customer, even if the data is stored at one of the new Norwegian data centres" (OrangeSec). American authorities can extract sensitive information from Norwegian citizens through American companies operating in Norway, as USA security legislation will be enforced even in Norway.

In 2020, the area caught fire, as US authorities could retrieve data stored within the EU. Thus, the United States can extract information within the EU domain without having to follow the legislation set by the EU. The case became known through the Schrems II judgment, and the result was that the EU regulations were not considered valid. The reasoning for the results is that American authorities have a great and intrusive opportunity to demand information from their companies located in the EU. The uncertainty at the EU level makes it difficult to develop national guidelines for cloud storage before new regulations exist between the EU and the USA. An assessment of cloud storage was conducted in 2017 to establish how Norwegian assets can be stored in cloud services. (NSM) concluded that for cloud services to be a secure way to store low-grade data, the data centres must be located in Norway. (*Vurdering av anskaffelsesregelverket - offentlige virksomheters mulighet til a stille krav til nasjonal lagring og behandling av data*, n.d.)

> To move forward on a national level, it is important to put in place an agreement between the EU and the US that regulates privacy so that you can safely use American suppliers because today, you can not really do that (Orangsec).

In comparison, Norway is different, where a court and judicial review are required to gain access to data for individual users and sensitive information. There are incentives for regulation that addresses the issue of data stored locally and across national borders. "USA's security legislation is so intrusive that they can request the disclosure of data without the customer being notified" (Orangesec).

The security act specifically sets regulations for critical infrastructure and is considered a part of the Norwegian government assets and should not be outsourced to a third party without further assessments. The same recommendation should be applied regardless of whether a company are affected by the security act or not. The companies should make a risk assessment that the data is safely stored and that the employees have the right competence to access the decision.

Many of the important functions that carry Norway may already be in the cloud through telecom and energy. NATO have international requirements towards their member states that restrict this action. However, a grey area still needs to be clarified towards assets that are being considered as critical assets or not. Therefore, the Norwegian authorities will not completely advise against using the cloud. However, rather advise the companies to be careful.

> We can not say to companies, do not use cloud services because they are dangerous, but we can say use cloud, but be careful, think carefully before you expose services, because it is very much good with the cloud (Yellowsec).

4.5 Communication

In recent years a growing focus has been on collaborating, sharing and communication across different sectors. Also, international cooperation has been in focus across European countries as more nations develop their own sets of national cybersecurity centres. Therefore, the willingness to share the exposure of an incident should have a larger focus. As for how it happened and the results of the initial attack, to learn from the incident. However, the sharing culture should have a fine balance of how much to share, especially when outsourcing essential data. "On both sides, we do not want to reveal the vulnerabilities, but at the same time, we want to work together, to find that balance" (Brownsec).

An ongoing discussion is whenever cyber incidents should be shared on a broader spectre to coordinate guidance between sectors and companies and advise and guide national security agencies and governments. "We are happy to compete on products, but we will work together on cybersecurity" (GreenSec). National authorities should have some requirements towards incident sharing when the attacks are certain, especially when dealing with important national assets like critical infrastructure. (NSM) in Norway have already developed its own guidelines and advice for handling critical infrastructure as a supplement for the basic NSM principles.

It is up to each company to share security incidents with the authorities or other security agencies. As shown in the figure 4.3 from mørketallsundersokelen 2020, most companies do not necessarily share their incidents with security institutions. Companies that share cyberattacks or incident with the public are often praised for their openness to the community and willingness to share. However, there is a negative effect of sharing the information of a cyber incident. Sharing can lead to the embarrassment of weak security and damage

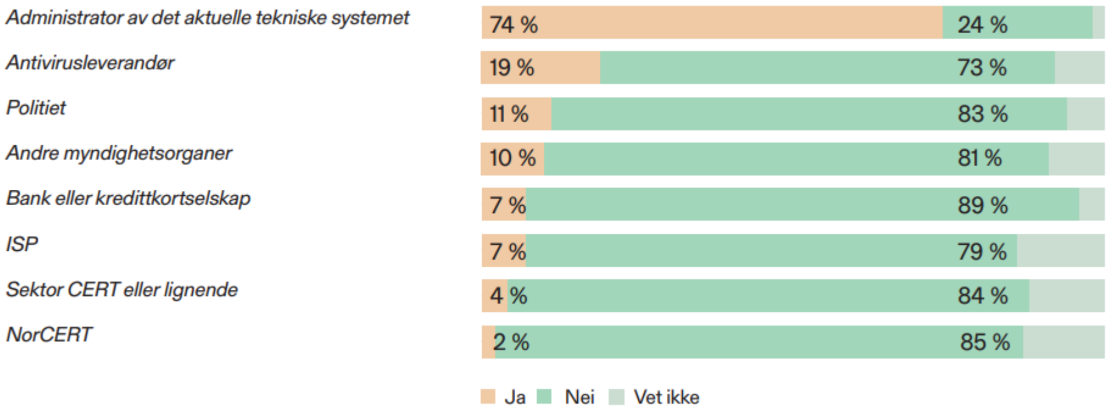


Figure 4.3: Statistic on incidents reported
(Noringslivets sikkerhets- rad, 2020)

the company's reputation, leading to a loss of value, for example, through a decline in the stock market. As (Redsec) states, "Information is the most important asset businesses have, both in the public and private sector" (Redsec). Therefore, companies should find a balance between openness and confidentiality.

> "An eternal discussion is to access information and be able to share it in more forums than where they are shared. Openness is important, but when an incident occurs, handling is priority one." (Greensec).

4.5.1 Terminology

Another issue has been that the security agencies are using various terminologies. For example, an agency can recommend measures to strengthen ICT security while addressing digital security issues. Technically skilled employees may not struggle with this issue as they may pragmatically look at security. However, leaders, HR and economics can have a hard time in a jungle of different terminologies. "Why do we use different terms? This is also the case in the legislation, and it is a challenge" (Redsec). Even the Norwegian law uses different terminology when addressing security, which can create problems for those who make laws, apply and interpret them. Therefore, one idea is to introduce a common language, which goes across sectors and industries, preferably baked into national guidelines.

4.5.2 Public & Private sector

Efficient optimisation could occur by implementing solutions into the national guidelines across sectors, both private and public. Platforms or solutions that will enable more automated processes are in demand. It has previously been a silo-based mindset where your system is your responsibility. There is a greater desire for a common digital platform and interaction across systems, especially in the public sector.

Some of the security agencies are closely working together with NSM to share exchange information when incidents occur. A similar agency or system could have been beneficial in the private sector for a better trust relationship between the companies. However, as long as there are major differences between the public and the private sector, a common guideline for both public and private companies may be difficult to develop. "the private sector has a mindset of profit, what costs the least, They are not necessarily very concerned with the security, as it is the bottom line that counts." (Orangesec). In addition, the diversity of interests makes a common national strategy difficult to implement across sectors.

4.5.3 Cultural differences

Cultural differences could affect how security is perceived, both at the local, regional, and national level. There are large differences in the experience and adoption of different security measures within Norway. A small municipality like Østre Toten would not have the same security measures and experience as a larger one like Oslo. Nordic countries conduct more or less the same measures when it comes to security. Sweden has even adapted some of the Norwegian security measures of NSM 2.0 guidelines in its security law. However, there seem to be cultural differences between Norway and Sweden. "Some Swedish organizations can have a culture that fosters stricter compliance with instructions than Norwegians" (Bluesec). Looking at other countries, Norwegian culture is more similar to other Nordic countries when compared to countries in Asia and even in the United Kingdoms (UK). The focus on a top-down approach is more prioritized in the UK than in Nordic countries, as decisions often are conducted higher up in the hierarchy.

4.5.4 Software & Tools

A topic that is needed to address is the equipment that different companies are using. Some elements of the national recommendations can be as simple as removing the default password from a device. Companies invest in software's to catch ongoing threat through logging analytic software to increase the overall security. Many companies may be good with logging tools, where a systematic approach are being applied towards the analytic part of it. There are recommendations in NSM guidance's to apply logging tools, but the employees do not necessarily use the software as they are intended to or lack knowledge. Companies will log a vast amount of data but will not necessarily analyse it and find out exactly what has happened before it is too late. "If you are unable to find out what happened after an incident, you will not be able to detect the thing that happens along the way." (Yellowsec).

4.5.5 Functionality

Security and functionality are often considered contradictions. Mandatory laws or regulations should be assessed thoroughly before being implemented to reduce the risk that they hinder or obscure the functionality of a system. If you implement a guideline that leads to set additional requirements so employees do not get their job done, you have laid out poor security. "When building minimum requirements, you will have to think very carefully about implementing recommendations or specific requirements" (Bluesec). Implementing a cybersecurity framework that interferes too much is not suitable for anyone. The frameworks must be implemented with the perspective of those who will use them. General recommendations through national cybersecurity guidelines instead of mandatory requirements can be more feasible for several companies.

> "Some may feel that the security measures are too restrictive, so you have to change the process so that the employees work tasks become effective even if you implement security measures, you can not think unilateral security." (Bluesec).

The developers of security guidelines should consider the variety of the appliance it can have on a company. Creating a guideline that sets minimum requirements can affect how the company perceive cybersecurity itself. Cybersecurity measures that conflict with other systems or measures that are too restrictive for the employees can be perceived as a barrier. Creating too low minimum requirements could create poor security for certain companies. There will be cases where the guidelines are misunderstood and implemented poorly, and there will be cases where guidelines are overextended due to the company's size. An example is the Norwegian Parliament building, Stortinget. Two-factor authentication is just being rolled out in the parliament building. However, some employees see this as a barrier and that the security is slowing down their efficiency. Companies should try to find the balance between functionality and security in the best possible way. Companies will have to access risks and accept that not everything is perfectly secure.giode

Chapter 5

Discussion

This chapter will discuss some of the essential empirical findings and the theory from the literature review. Additionally, the chapter will explain why the data being discussed is relevant to the context and how it can be interpreted in the research field.

5.1 National guidelines

As described in the findings, there is an increasing trend internationally to develop national guidelines. The findings are coherent with the main features in theory, as national security strategies and guidelines are being developed rapidly in the European market, focusing on national strategies and guidelines. (Markopoulou et al., 2019)

The reasons for the development are caused by several underlying elements, such as increasing demand for better overall digital communication across the nation. Rules, regulations and certification schemes that emphasize national values and interests are especially in focus. Norway has put in place several viable solutions praised by the security community, and several processes have been initiated to increase collaboration across sectors, especially in the public sector. The argument is coherent by theories (Srinivas et al., 2019) that there should be guidelines that elaborate on a specific sector or industry standards. In practice, this means that national guidelines could, to a greater extent, be implemented to fit different sectors and industries, as international frameworks often are general in their form and not necessarily adjusted to local or national conditions or environments. (Verhelst et al., 2020) It also points out that private actors have a significant role in the industry and that national guidelines can reduce the private actors market influence regarding cybersecurity guidelines and strategies. In the findings, some respondents also pointed out that the cybersecurity guidelines were purely chosen because of the expertise of third parties.

As described in the findings, there is an increasing trend internationally to develop national guidelines. The reasons for the development are caused by several underlying elements, such as increasing demand for better overall digital communication across the nation. Rules, reg-

ulations and certification schemes that emphasize national values and interests are especially in focus. Norway has put in place several viable solutions praised by the security community, and several processes have been initiated to increase collaboration across sectors, especially in the public sector.

5.2 Cybersecurity framework

The findings show that implementing a cybersecurity framework could cause challenges as there are risks involved when implementing an international cybersecurity framework such as ISO. International cybersecurity frameworks could be a resource for more documentation and bureaucracy, as ISO requires a heavy process of coordination and compliance after its initial implementation. ISO is considered a minimum standard of good practice, as ISO focuses on general aspects of cybersecurity. ISO is also flexible in its form, as it can be generalised across nations around the world (Syafrizal et al., 2020). The findings reflect that the sectors may have implemented an international cybersecurity framework, such as ISO, but do not necessarily use it for the initial purpose. Cybersecurity frameworks should be implemented to enhance a company's security and not only satisfy the market requirements. In addition, the findings show that employees could have difficulties in understanding comprehensive international cybersecurity frameworks. As the respondents have reported in the findings, there is a divided distance between theory and practice, as ISO is not practised after its purpose. A solution could be implementing national guidelines, as ISO can be considered too complex or too expensive for smaller organisations where knowledge and expertise related to cybersecurity are not on the agenda.

5.3 Compliance

A company that does not comply with regulatory requirements within a sector can be frozen out of the market due to the requirements of certain cybersecurity frameworks, such as ISO or NIST. (van Eeten, 2017) However, it can be challenging to face regulation, laws policies and comply efficiently with a cybersecurity framework.(Syafrizal et al., 2020)
There is a nuance between theory and practice, as the findings show that you are often required to be certified to comply with international cybersecurity frameworks. However, several of the actors do not recommend certifications schemes, especially when addressing the public sector, as certification is not necessarily coherent with the good practice of cybersecurity. Instead, the vast majority have either used cybersecurity frameworks because the market requires it. Still, in practice, it turns out that it can be "superficial", and perhaps it would be a good solution to introduce national guidelines instead. Given this argument, it is conceivable that there would be an opportunity to certify it in the Norwegian market.

5.4 Policies, laws & regulations

In the findings, one will see a two-way discussion where there is a conflict between national guidelines and international regulations. The reason is that nations within the EU are bound to follow the EU's regulations at an international level before they can develop their own set of national guidelines. As the theory describes, several of the "superpowers" have already established their own sets of national guidelines to protect national interests. (Goel, 2020) Further describes that this rearmament could lead to an increased national focus and political conflicts and that a further division of the cyber landscape could emerge. Norway should, to the best of its ability, comply with EU and international law. Unlike the United States or China, which may have greater freedom to act on the political cyber landscape. Nevertheless, it may be appropriate for Norway to develop its own national guidelines to comply with Norwegian laws, rules and policies, and safeguard Norwegian national interests, while at the same time following the EU and international regulations.

The same also applies concerning data storage which is further mentioned in the findings. There is currently a great deal of uncertainty about whether data storage can occur across national borders and how international law enforces these.

It raises further questions about whether data stored in Norway can actually be retrieved from Norway and or within the EU's borders is legal and what consequences this entails. Laws have to be functional to a degree, and countries should be cautious of implementing additional national security requirements for foreign digital services suppliers (Markopoulou et al., 2019).

The question of whether national guidelines should be required by law and or certified is difficult to answer. Some see certification as positive and quality-enhancing, while others view certification schemes as completely unnecessary and wasting money on bureaucracy. Nevertheless, there are tendencies towards more comprehensive requirements for certain companies at a national level (Dedeke & Masterson, 2019). A proposal is to make deliveries to the public sector with mandatory minimum requirement baked into national guidelines like NSM basic principles 2.0. A possible effect may be an indirect regulation towards the private sector. In this way, one does not create more direct rules towards the market but greater demands for vendors and raises the quality of the delivery to the public sector. Questions should be further raised related to the power private sectors already have in the market through being the framework provider for most of the market (Verhelst et al., 2020). Further, it will be interesting to see the development of the private market if certifications of national guidelines become the new norm instead of implementing cybersecurity frameworks. If such regulation will occur, which can completely or partially replace the cybersecurity framework, one will most likely face opposition from the private market due to a significant loss of market value.

A simplified figure has been created to illustrate a possible delivery chain towards the public sector in Norway, as shown in the figure 5.1. Security guidelines developed by the government or security agencies are often based on non-profit and serves only to enhance the cybersecurity knowledge for the nation. A non-profit mandatory enforced national guideline may put companies that specialise in certifying cybersecurity frameworks, especially the consulting industry, in jeopardy (Mueller, 2017).

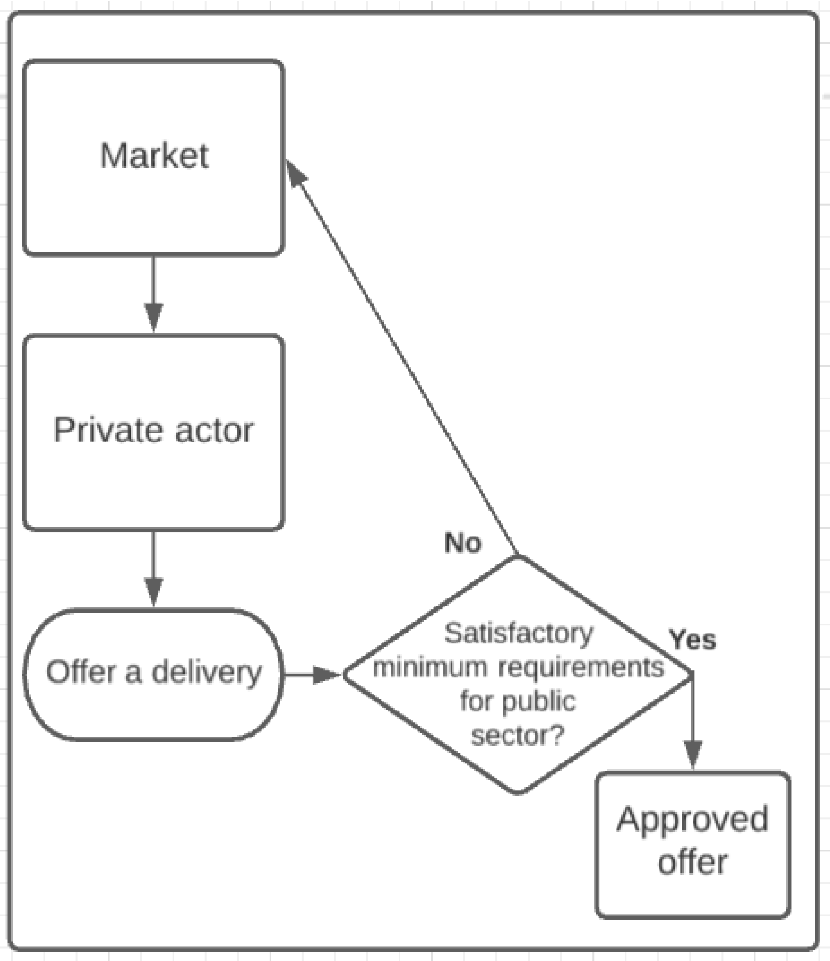


Figure 5.1: A simplified Proposal for minimum requirements towards the public sector

An ongoing issue is whether the national guidelines will shed light on the challenge of privacy in the global market. Today, there are large gaps and grey areas for both outsourcing of data and preservation of privacy. Digital development is almost exclusively in the direction of the cloud, which means that national values will be outsourced to third-party companies to a greater extent. National regulations regarding data storage outside Norway must be further improved and accessed. For example, it is a grey area whether data stored in Norway, while owned by a foreign company, is of Norwegian property. The EU commission must follow up on the privacy issues where data is extracted from third-party countries before EU countries can develop their set of national guidelines to a greater extent.

In Norway, the industry and the sector landscape are of high priority. Various regulations and laws across sectors and industries make one particular national guideline harder to establish. The guidelines should be established to enhance the general recommendation for companies and the nation's best cybersecurity interests while complying with national, European and international laws & regulations.

What will be important is to recommend guidelines that set minimum requirements for national values to a greater extent. Companies, such as those that process data with critical infrastructure, directly and indirectly, should to a greater extent be mandatory enforced minimum requirements, such as NSM 2.0 basic principles. As of now, there are many regulations across different domains that not necessarily are compliant with each other. A new national guideline would be to merge legislative regulations together with enhanced security requirements. Companies in Norway today may struggle when conducting cybersecurity assessments. An example of a simplified legislative assessment is illustrated in 5.2. The table tries to illustrate that the assessment can be complex and that it can be difficult to get an overview of which regulations companies must consider.

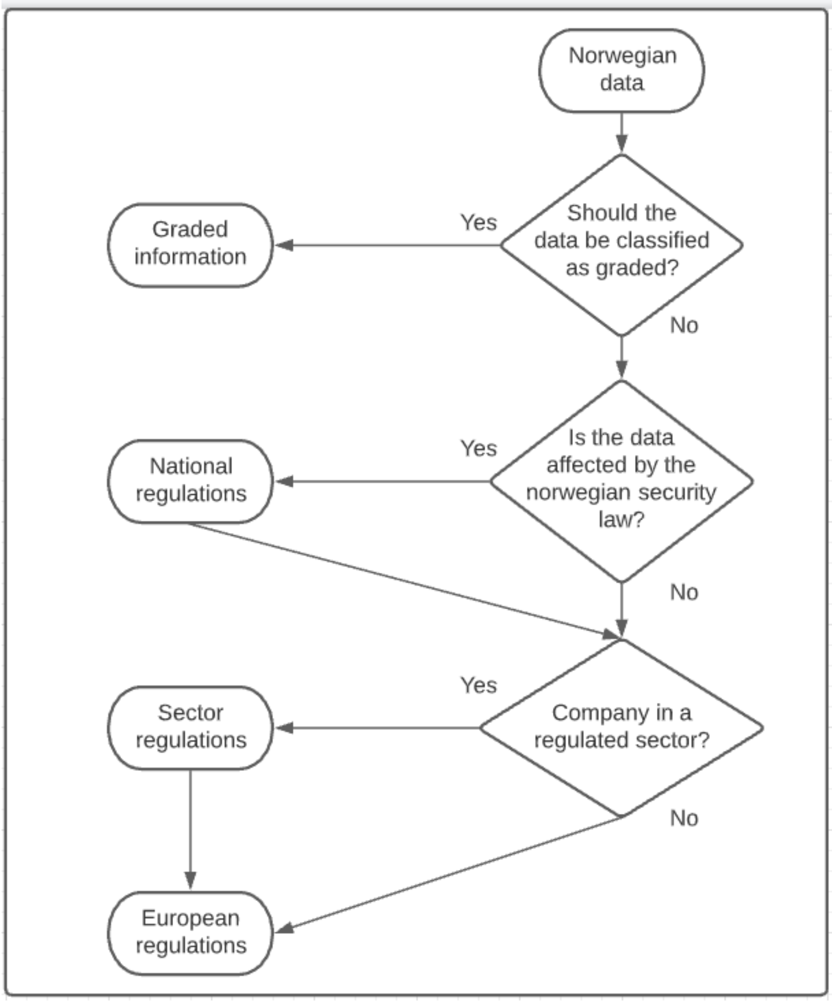

Norwegian data
Should the data be classified as graded?
Yes
Graded information
No
Is the data affected by the norwegian security law?
Yes
National regulations
No
Company in a regulated sector?
Yes
Sector regulations
No
European regulations

Figure 5.2: How data that are affected by law & regulation could look like

5.4.1 International cybersecurity frameworks as a baseline

The international frameworks are often generalised but good. The frameworks focus on gaining a common understanding globally of how to develop appropriate solutions that can be enforced everywhere. It is also up to each country to be able to adopt the cybersecurity frameworks efficiently. Nations can implement several of the cybersecurity frameworks as a baseline for their national guidelines. Combining several of the frameworks can be beneficial for a best practice approach (Sulistyowati et al., 2020). However, complying with and following up each framework towards a common national strategy can be difficult to implement, as each cybersecurity framework are regularly updated.

The development of national guidelines can be seen in connection with the increased development of regulations in the EU. as the EU is constantly trying to lift and increase their member states overall security requirements. EU specifically requires each member state to develop their own set of national standards to meet the EU level compliance (Markopoulou et al., 2019). Therefore, even though Norway is not part of the EU, they are affected by the EAA and comply with the EU's regulatory requirements.

5.4.2 Communication

A positive remark with developing a more comprehensive national guideline would be a broader understanding of communication across different industries, especially as there are cultural differences in implementing various security measures. Cybersecurity frameworks use different terminologies, which means that some companies may face communication challenges in their work. A national guideline with a simplified common language will see positive ripple effects across sectors, both where IT personnel and ordinary employees will understand each other. Cultural differences are embedded in the cybersecurity frameworks. An employee in cybersecurity in China would not necessarily have the same precondition as an employee in Norway, and vice versa, as different cybersecurity frameworks will yield different division of responsibilities among the employees.

5.4.3 Different agendas for implementation

The reasoning for implementing a cybersecurity framework has proven to be incredibly complex. It can be anything from cultural differences, own preferences, knowledge and or expertise of certain frameworks, or that the company is affected by laws and regulations requiring the company to use a specific framework. Although in the study, it has been shown that there can be many reasons why companies use different frameworks, in the figure 5.3below, I have tried to show various elements which can be underlying causes and that those who are represented in the study and the figure most likely only touch the tip of the iceberg.

> We could, in principle, choose ISO, we could choose NSM, we could choose NIST, it would be a matter of taste, But it would have been nice to follow a framework that consists of best practices (Brownsec).

The main reason for actually implementing a cybersecurity framework is to strengthen security, but choosing the appropriate is not necessarily about what is most secure. Cybersecurity frameworks are chosen based on terminologies, accessibility and functionally. The vast majority in the private sector implement cybersecurity frameworks to keep up with the market. This attitude is not necessarily favourable, as the focus is on a completely different than security. However, it will be interesting to see if the authorities in Norway and the national security agency introduce some additional national guidelines that are either regulated in the form of laws or indirectly enforced by requirements in certification schemes.

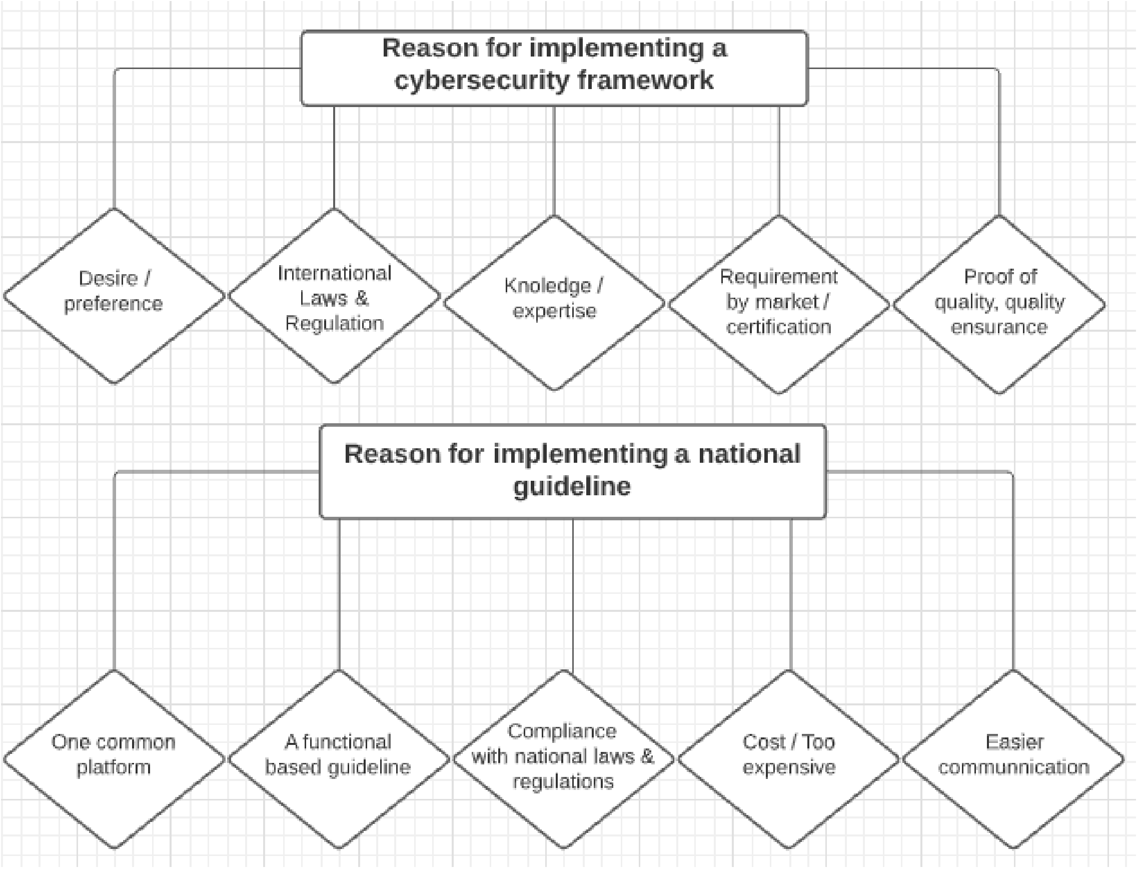

Reason for implementing a cybersecurity framework
Desire / preference
International Laws & Regulation
Knoledge / expertise
Requirement by market / certification
Proof of quality, quality ensurance
Reason for implementing a national guideline
One common platform
A functional based guideline
Compliance with national laws & regulations
Cost / Too expensive
Easier communnication

Figure 5.3: Reasoning for implementing

Chapter 6

Conclusion

The rapid development of digitisation has led to questions of how to handle national values. The thesis points to many different elements that can impact both for and against a national solution and guidelines. To the best of my ability, I have chosen to include the most important topics that can shed light on the related challenges and tried to answer the research questions as presented below

Common digital solutions and common national security guidelines have become a focus area for several countries. The EU facilitates a focus on increasing digital security by introducing requirements for the EU states. Some of the NIS-directive and the security ACT requirements are enforced as the states have to develop national guidelines and certification schemes that can be compliant with the European regulations.

Challenges are yet to be solved, as ongoing conflicts with privacy and data storage towards cloud services across third-party countries must be in place. The solution should be implemented at the EU level before the problem can be solved nationally and embedded into a national cybersecurity guideline.

Why are countries such as Norway developing their own national cybersecurity guidelines instead of implementing cybersecurity frameworks?

With the thesis special focus on Norway, there is a clear desire to facilitate more common components at a national level that can strengthen communication across sectors and industries. There are already examples of sectors & industries that have based their laws and regulations on national guidelines. These national guidelines are often developed with inspiration from international cybersecurity frameworks. Several of the respondents from the case study point out that communication challenges across sectors should be addressed further. There is a need for a greater common digital strategy with hybrid components that are suitable for universal solutions, which must be in place in order to develop a more comprehensive national guideline. Private actors must also have a role either directly or indirectly through statutory certification schemes towards the public sector.

Chapter 7

Limitation

The master's thesis has been challenging and rewarding and is by no means perfect. In this chapter, I will address the challenges and limitations that have influenced the study.

7.1 The process

Planning the process to conduct a master thesis started in October 2020, choosing a topic and finding an interesting subject that required additional research. I got in contact with several stakeholders who were interested in discovering new data on the field. In November, I contacted the Norwegian armed forces and the related science environment, Forsvarets forskningsinstitutt (FFI). In the next couple of months, we planned and prepared the case to look at the Norwegian armed forces implementation of international cybersecurity frameworks. Unfortunately, as late as the middle of Mars 2021, the sample discovered that they could not conduct interviews, which resulted in a major setback for the thesis. To solve the challenge, I had to readjust quickly. I restructured the thesis and found a new sample with the same theme. Unfortunately, this challenge has meant that there has been less time than desired for the final project.

7.2 Sample

Following the same challenges mentioned above, the selection group is also slightly affected by the restructuring process. Still, I was lucky and got a lot and positive response on the second sample selection. Nevertheless, I would like to point out that 8 interview subjects are often considered small for some studies, although it is augmented in the method chapter. In addition, the agencies were being handpicked to find respondents that could represent as "experts" or informants on the field. However, what is considered an expert sample is a weakness in itself since it is subjective to a certain degree.

7.3 Theoretical implications

In the literature review, a systematic search was carried out to the best of my ability, where the most relevant articles related to my research question were included. Nevertheless, it is important to point out that there are weaknesses in the review. Several aspects could have been done differently. For example, additional databases could have been included, and the searches could have been broader, with different keywords or synonyms. Additionally, the year span articles could have been included to include older articles, as of 2017-2021 may seem too short and can be considered bias.

The literature review has an overall focus that addresses various topics related to the research question. This means that there are not necessarily so many contradictions in the literature and the findings, as the findings tend to go more specifically into certain areas of the topic. These assessments are taken into account with both the scope and the time limitation of the thesis.

7.4 Methodology

One of the arguments of conducting qualitative interviews was to perceive the interview participants and absorb the situations and environment around the respondent to establish meta-data. Unfortunately, due to the corona pandemic of 2019, restrictions applied and made it impossible to conduct physical interviews. Instead, the interviews were conducted through a digital call and streaming service, which is considered a barrier to fully understanding the findings' depth.

Chapter 8

Further Research

In the thesis, central themes surround national cybersecurity strategies in general and with a particular case of Norway has been discussed. Further research should consider going into detail on specific sub-themes that are presented in the thesis. An example with a sub-focus that emerge from this thesis can focus directly on, for example, the private sector role and power of establishing national guidelines. There would further be interesting to get additional quantitative data in one particular field, sector or industry in Norway to see if the study can be adapted and generalised. Further research is also to be discovered on how national guidelines, in general, are developed to comply with regulatory requirements at an international level. Further studies could also seek to generalise several countries of EU nations as a group and look for similarities across nations compared to a broader international focus.

References

Dedeke, A., & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks (cif) from three countries. *Information & Computer Security*.

ENISA. (2020). *Guideline on security measures under the eecc.* Retrieved from `https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc/at_download/fullReport`

ENISA. (2020). *The year in review.* Retrieved from `https://www.enisa.europa.eu/publications/year-in-review/at_download/fullReport`

European Commision. (2020). *Digital economy and society index (desi) 2020.* Retrieved from `https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=67086`

Fink, A. (2019). *Conducting research literature reviews: From the internet to paper.* Sage publications.

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, *58*(3), 273–286.

Goel, S. (2020). National cyber security strategy and the emergence of strong digital borders. *Connections*, *19*(1), 73–86.

Guo, M. (2018). China's cybersecurity legislation, it's relevance to critical infrastructures and the challenges it faces. *International Journal of Critical Infrastructure Protection*, *22*, 139–149.

Interpol. (2020). *Interpol report shows alarming rate of cyberattacks during covid-19.* Retrieved from `https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf`

Kaponig, H. (2020). Austria's national cyber security and defense policy. *Connections*, *19*(1), 21–37.

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new eu cybersecurity framework: The nis directive, enisa's role and the general data protection regulation. *Computer Law & Security Review*, *35*(6), 105336.

Mueller, M. (2017, 07). Is cybersecurity eating internet governance? causes and consequences of alternative framings. *Digital Policy, Regulation and Governance*, *19*, 00-00. doi: 10.1108/DPRG-05-2017-0025

National Security Agency. (2020a). *Grunnprinsipper for ikt-sikkerhet versjon 2.0.* Retrieved from `https://nsm.no/getfile.php/133735-1592917067/Demo/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf`

National Security Agency. (2020b). *Helhetlig digitalt risikobilde 2020.* Retrieved from https://nsm.no/getfile.php/134468-1604926904/Demo/Dokumenter/Rapporter/NSM_IKT-risikobilde_2020_enkeltside.pdf

National Security Agency. (2021). *Risiko 2021.* Retrieved from https://nsm.no/getfile.php/136419-1616673370/Demo/Dokumenter/Rapporter/NSM_Risiko_2021_web_enkeltside_1203.pdf

Noringslivets sikkerhets- rad. (2020). *Morketallsundersokelsen 2020.* Retrieved from https://www.nsr-org.no/uploads/documents/Publikasjoner/Morketalls-2020-web.pdf

Norsk senter for informasjonssikring. (2016). *The norwegian cyber security culture.* Retrieved from https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf

Norwegian Ministeries. (2019). *National cyber security strategy for norway.* Retrieved from https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf

NSM. (n.d). *Historien om nsm.* Retrieved from https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/

Regjeringen. (2019a). *En digital offentlig sektor.* Retrieved from https://www.regjeringen.no/contentassets/db9bf2bf10594ab88a470db40da0d10f/no/word/digitaliseringsstategien.docx

Regjeringen. (2019b). *Nasjonal strategi for digital sikkerhet.* Retrieved from https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

Regjeringen. (2020). *The data breach at the storting.* Retrieved from https://www.regjeringen.no/en/aktuelt/datainnbruddet-i-stortinget/id2770135/

Regjeringen. (2021). *Dette mener e-tjenesten, pst og nsm er truslene mot norsk sikkerhet.* Retrieved from https://www.regjeringen.no/no/aktuelt/dette-mener-e-tjenesten-pst-og-nsm-er-truslene-mot-norsk-sikkerhet/id2832393/

Salkind Neil, J. (2009). *Exploring research.* USA: Pearson International Edition.

Sharkov, G. (2020). Assessing the maturity of national cybersecurity and resilience. *Connections: The Quarterly Journal*, *19*(4), 5–24.

Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S., & Shpenov, D. (2020). Cybersecurity: Legal and organizational support in leading countries, nato and eu standards. *Journal of Security & Sustainability Issues*, *9*(3).

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188.

Stadnik, I., et al. (2017). What is an international cybersecurity regime and how we can achieve it? *Masaryk University Journal of Law and Technology*, *11*(1), 129–154.

Steinar Kvale, S. (2015). *Det kvalitative forskningsintervju.* Oslo: Gyldendal akademisk.

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020, 12). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. *JOIV : International Journal on Informatics Visualization*, *4*. doi: 10.30630/joiv.4.4.482

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security*, *12*(3), 417–432.

Tjora, A. (2012). *Kvalitative forskningsmetoder i praksis* (Vol. 2). Gyldendal akademisk Oslo.

Utenriksdepartementet. (2017). *Internasjonal cyberstrategi for norge.* Retrieved from `https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategi_web.pdf`

van Eeten, M. (2017). Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. *Digital Policy, Regulation and Governance.*

Verhelst, A., et al. (2020). Filling global governance gaps in cybersecurity: International and european legal perspectives. *International Organisations Research Journal*, *15*, 141–172.

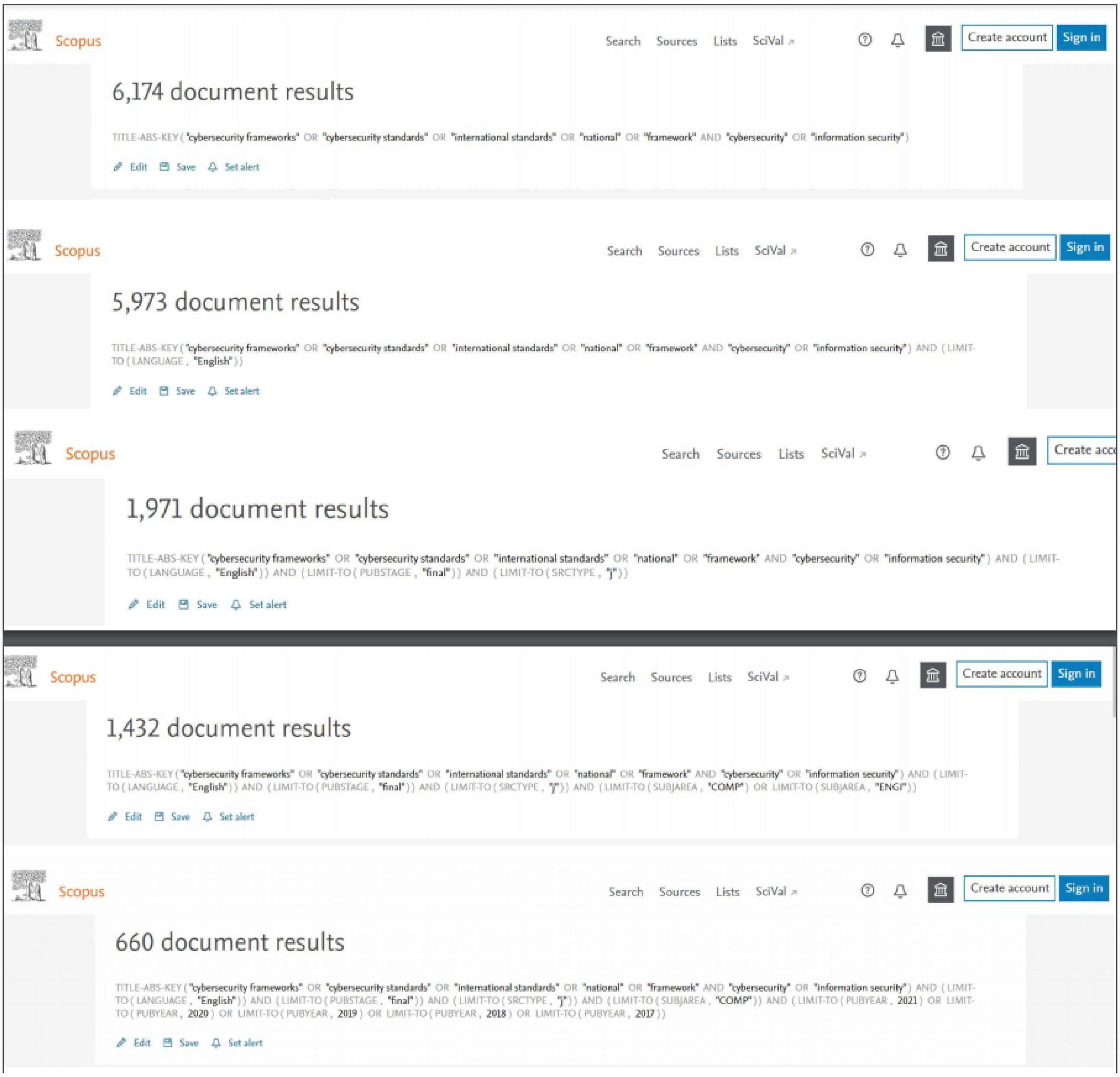
Vurdering av anskaffelsesregelverket - offentlige virksomheters mulighet til a stille krav til nasjonal lagring og behandling av data. (n.d.).

Yin, R. (2013). *Case study research: Design and methods.* SAGE Publications. Retrieved from `https://books.google.no/books?id=OgyqBAAAQBAJ`

Appendix A

Literature review search

A.1 Practical screen



6,174 document results

TITLE-ABS-KEY ("cybersecurity frameworks" OR "cybersecurity standards" OR "international standards" OR "national" OR "framework" AND "cybersecurity" OR "information security")

5,973 document results

TITLE-ABS-KEY ("cybersecurity frameworks" OR "cybersecurity standards" OR "international standards" OR "national" OR "framework" AND "cybersecurity" OR "information security") AND (LIMIT-TO (LANGUAGE , "English"))

1,971 document results

TITLE-ABS-KEY ("cybersecurity frameworks" OR "cybersecurity standards" OR "international standards" OR "national" OR "framework" AND "cybersecurity" OR "information security") AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (PUBSTAGE , "final")) AND (LIMIT-TO (SRCTYPE , "j"))

1,432 document results

TITLE-ABS-KEY ("cybersecurity frameworks" OR "cybersecurity standards" OR "international standards" OR "national" OR "framework" AND "cybersecurity" OR "information security") AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (PUBSTAGE , "final")) AND (LIMIT-TO (SRCTYPE , "j")) AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "ENGI"))

660 document results

TITLE-ABS-KEY ("cybersecurity frameworks" OR "cybersecurity standards" OR "international standards" OR "national" OR "framework" AND "cybersecurity" OR "information security") AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (PUBSTAGE , "final")) AND (LIMIT-TO (SRCTYPE , "j")) AND (LIMIT-TO (SUBJAREA , "COMP")) AND (LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018) OR LIMIT-TO (PUBYEAR , 2017))

Appendix B

Interview guide

Intervjuguide

Mitt navn er Nicolay Leknes, jeg studerer cybersikkerhet ved Universitet i Agder (UiA), hvor jeg skriver masteroppgave om nasjonale sikkerhetsveiledere. Masteroppgaven handler om anvendelsen av veiledere i praksis, med en avgrensning hvor fokuset er på nasjonale nasjonale veiledere. Jeg benytter ulike etablerte cybersikkerhetsrammeverk som teoretisk forankring for undersøkelsen, og det er viktig for meg å presisere at det ikke gjøres normative betraktninger av om det dere gjør er rett eller galt.

Oppgaven er utarbeidet med mine masterveiledere, Paolo Splaglonetti og Terje Gjøsæter fra UiA, samt med en tett oppfølging fra Torbjørn Kveberg fra FFI.

Informasjon om lagring av dataene som blir samlet inn, retningslinjer og samtykkeskjema vil bli sendt til deg i et eget dokument. Spørsmålene som blir stilt er laget basert på nyere litteratur fra fagfeltet. Hvis du av en eller annen grunn ikke vil svare på spørsmålene som blir presentert, og eller hvis du av en annen grunn vil trekke deg ut av forskningsprosjektet, kan du gjøre dette til enhver tid

Dette intervjuet er et semistrukturert intervju, der du blir bedt om å svare på forberedte spørsmål, men oppfølgingsspørsmål for utdyping av gitte spørsmål kan forekomme.

Anslått varighet for dette intervjuet er satt til ca. 1 time.
Dette intervjuet vil ta opp screen recording i form av lyd og video for transkribering.
Har du noen spørsmål før vi begynner?

Introduksjonsspørsmål

1. Hvor lenge har du jobbet i bedriften?
2. Hva er din/deres rolle i virksomheten?
3. Hvor lenge har du jobbet med arbeid knyttet mot cybersikkerhet?
4. Er du, eller noen du samarbeider med sertifisert av noen de kjente internasjonale sikkerhetsrammeverkene som f.eks ISO eller NIST?
5. Hva vil du kategorisere som et av bedriftens viktigste arbeidsoppgaver og verdier?
6. Hvordan er samarbeidet med andre interne og eksterne aktører og andre CERTer?

Nasjonale veiledere

7. Hva var er ditt forhold til nasjonale veiledere, som f.eks NSM sine grunnprinsipper?
8. Hvordan tror du sikkerhetsprinsipper i veiledere og eller rammeverk blir anvendt forskjellig fra de som lager et produkt og de som bruker det?
9. Hvordan ser dere for dere at nasjonale veiledere som NSM 2.0 kan styrke anvendelsen av rammeverk?
10. Har du noen tanker om at flere land benytter seg av egne nasjonale veiledere istedenfor å følge internasjonale sikkerhetsrammeverk?

Compliance

11. Hva vil du si skiller seg mest ut av f.eks NSM sine veiledere og andre kjente cybersikkerhet rammeverk?

12. Hva tenker du om anvendelsen av sikkerhetsveiledere i praksis, fungerer tiltakene som blir beskrevet i rammeverkene, eller er det mest teoretisk?
13. Har dere noen verktøy for å måle hvorvidt deres og eller andre rammeverk eller veiledere blir implementert på riktig måte?
14. Hva vil du peke på som en variasjon eller et avvik av implementasjon av en veiledere eller sikkerhetsrammeverk?

Internasjonalt samarbeid

15. Hva er ditt forhold til informasjonsdeling på tvers av bedrifter for å dele erfaringer o.l?
16. Hvordan tror du informasjonsdeling vil foregå på tvers av sektorer og landegrenser i tiden fremover?
17. Har du noen tanker om kulturforskjeller knyttet til implementering av veiledere og eller sikkerhetsrammeverk?

Sertifisering

18. Hva opplever du er hovedgrunnen til at bedrifter sertifiserer seg i sikkerhetsrammeverk, som f.eks ISO & NIST?
19. Hvilke fordeler og eller ulemper vil bedrifter kunne oppnå med å sertifisere seg i det norske markedet?
20. Tror du det blir aktuelt å sertifisere veiledere, som f.eks NSM grunnprinsipper?

Lover og regler

21. Har du noen tanker om datalagring av sensitiv informasjon i skyen og på tvers av landegrenser?
22. Har du noen tanker om at nasjonale veiledere blir lettere compliant med loven enn f.eks andre sikkerhetsrammeverk?
23. Har du noen kjennskap til konflikter mtp. lover og regler i internasjonale rammeverk som påvirker norske bedrifter i større grad?
24. Hva er dine tanker om lovpålagte sertifiseringer og eller implementeringer av veiledere og eller sikkerhetsrammeverk for enkelte sektorer eller bedrifter?
25. Har du noen tanker at om at internasjonale sikkerhetsrammeverk og eller nasjonale veiledere kan ha negative konsekvenser i en internasjonal kontekst?

Appendix C

Consent Form

Forespørsel om å delta i forskningsprosjekt

Standardiserte sikkerhetsrammeverk i praksis

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å se på hvordan standardiserte sikkerhetsrammverk anvendes. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Introduksjon
Mitt navn er Nicolay Leknes, jeg studerer cybersikkerhet ved Universitet i Agder (UiA), hvor jeg skriver masteroppgave om anvendelse av sikkerhetsrammeverk, med en tilnærming opp mot nasjonale sikkerhetsrammeverk. Det er viktig for meg å presisere at det ikke gjøres normative betraktninger hvorvidt bruken er rett eller galt og lignende, da dette ikke er målet med prosjektet.

Hvem er ansvarlig for forskningsprosjektet?
Oppgaven er utformet i samarbeid av mine masterveiledere i prosjektet, Paolo Spagnoletti og Terje Gjøsæter fra UiA.

Hvorfor får du spørsmål om å delta?
Masteroppgaven har behov for 5-15 respondenter med ulik tilknytning og erfaring opp mot forskjellige fagfelt som har relevant tilknytning til standardiserte rammeverk. Det kan være relevant med både teknikere, undervisningspersonell og evt. ledere for et bredt og mangfoldig perspektiv på fagfeltet.

Hva innebærer det for deg å delta?
Som følger av restriksjoner og lover knyttet til Coronaviruset, vil intervjuene bli gjennomført digitalt, via video- og ringetjenesten Zoom.

For å levere på normert tid må intervjuene gjennomføres innen 30. april i år, og gjerne før. Hvert intervju er av omlag en times varighet. Intervjuene er semi-strukturelle, som betyr at det er forberedte spørsmål, men må man være beredt på at oppfølgingsspørsmål kan forekomme for ytterligere utredning

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Dataene som blir samlet inn har ingen interesse eller intensjon om å identifisere deltakere i forskningsprosjektet. I intervjuene kommer det til å bli tatt i bruk diktafon og eller digitalt lydopptak via screen recording for transkribering. Dataene som blir innhentet vil bli analysert og presentert i masteroppgaven, disse dataene vil da være i en anonymisert fremstilling, hvorav alt innhentet rådata via screen recording og eller via diktafon vil bli slettet. All innsamling og behandling av intervjudata vil være i tråd med retningslinjene til UiA og Norsk senter for forskningsdata (NSD).

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Dataene som blir behandlet i denne studien kun være tilgjengelige for prosjektansvarlig, Paolo Spaglonetti & Terje Gjøsæter, samt jeg som student og databehandlingstjenesten Zoom.
- Videre er det også iverksatt tiltak for å sikre at ikke uvedkommende får tilgang til data under og etter intervjuene:
  -Møtelenke vil ikke deles åpent.
  -Møtet vil være passordbeskyttet.
  -Det vil bli benyttet lobby/venterom for å slippe inn riktige personer i møtet.

-Under behandlingen av vil dataene bli lagret på et SD-kort på en diktafon fra det digitale intervjuet. Så fort transkriberingen er ferdig vil dataene bli omgjort til datafunn "koder" og rådataene fra intervjuet vil bli slettet i form av at SD-kortet blir destruert.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er 10 juni 2021. All rådata vil bli destruert underveis i prosjektet, videre skal annen data fremstilt i prosjektet anonymiseres innen prosjektslutt.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitet i Agder har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:
- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Jeg vil selvfølgelig i oppgaveteksten ta ansvar for arbeidet og representasjonen av bedriften, og erkjenne at dette ikke noen offisiell beskrivelse av sikkerhetspraksis fra deres side. Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- Masterstudent, Nicolay Leknes ved Universitet i Agder, kontaktes på epost (nicoll6@uia.no), og eller på telefon: +4747207752 .
- Førsteamanuensis, Paolo Spagnoletti ved Universitet i Agder, kontaktes på epost (paolo.spagnoletti@uia.no), og eller på telefon: +393473123560.
- Vårt personvernombud: Ina Danielsen ved Universitet i Agder, kontaktes på epost (ina.danielsen@uia.no), og eller på telefon: +4738142140.

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:
- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Nicolay Leknes,
Masterstudent

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet og har fått anledning til å stille spørsmål. Jeg samtykker til:

- □ å delta i et intervju innen 30 april.

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

----
(Signert av prosjektdeltaker, dato)