Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Kristian Andre Kastet

The New Total Defence Concept: Defending the Civilian Sector Across the Conflict Spectrum

Master's thesis in Information Security
Supervisor: Benjamin James Knox
June 2022

NTNU
Norwegian University of Science and Technology

Kristian Andre Kastet

The New Total Defence Concept: Defending the Civilian Sector Across the Conflict Spectrum

Master's thesis in Information Security
Supervisor: Benjamin James Knox
June 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Abstract

An increasing number of Norwegian organizations experience cyberattacks from criminals and state actors alike. This master thesis aims to investigate the role of the new Total Defence concept in defending the civilian sector across the conflict spectrum.

The overarching research question is:

What should the new Total Defence concept's role be in defending the civilian sector in times of increasingly hostile cyber operations?

Based on a literature study focusing on different actors in Cyberspace, threat intelligence and situational awareness. The study summarizes a qualitative study into what the civilian sector needs from the state to be better prepared in Cyberspace, given the current threat environment. Moreover, what kind of support is required and how can situational awareness be improved in society.

The study reveals a need for engagement from the various actors in the new Total Defence concept in defence of the civilian sector and a role for the civilian sector to contribute back to the state.

Sammendrag

Et økende antall norske bedrifter og andre organisasjoner opplever angrep i Cyberrommet fra statlige aktører og kriminelle. Denne masteroppgaven søker å finne svar på hva som er det nye Totalforsvarets rolle i forsvaret av sivil sektor i Norge over hele konfliktspekteret.

Det overordnede forskningspørsmålet er:

Hva er det nye Totalforsvarets rolle i forsvaret av sivil sektor i en tid der man opplever et økende antall fiendtlige operasjoner i Cyberrommet?

Basert på et litteraturstudie som fokuserer på forskjellige aktører i Cyberrommet, trusseletterretning og situasjonsforståelse. Denne kvalitative studien summerer hva sivil sektor trenger fra staten for å være bedre forberedt i Cyberrommet gitt nåværende trusselnivået. Videre, hva slags støtte som er påkrevd og hvordan vi kan forbedre situasjonsforståelsen i samfunnet generelt.

Studien viser at det er nødvnedig med et engasjement fra forskjellige aktører i det nye Totalforsvaret for å kunne forbedre forsvaret av sivil sektor og en rolle for sivil sektor til å bidra tilbake til myndighetene.

Acknowledgements

Taking an education as a grown-up is undoubtedly a privilege. Attempting a master's degree does not happen in a vacuum and requires a rather extensive support system. My former boss and colleague Bjørn-Erik deserves thanks for allowing me to start on this journey and walking the extra mile to allow me time off as required to study. Also, big thanks to my former colleagues Torbjørn, Christer, Håkon, Dag, Roy, Stian, Ørjan, Øyvind and Tone for all discussions relevant or not over the years. My new boss Henrik deserves thanks for letting me have time off to finish this thesis. And a special thanks to my supervisor Ben Knox who has patiently waited for my drafts, provided invaluable guidance and has been a valuable discussion partner through this. Finally, to Christine and Kristoffer, who has patiently let me do this and quietly reminded me what is important in life when needed.

Abbreviations

CERT - *Computer Emergency Response Team, traditionally a team within an organisation that do investigations and help restore services after a cyber incident or cyberattack. Also used to describe organizations that do the same, such as KraftCERT*

CSIRT - *Computer Security Incident Response Team,traditionally a team within an organisation that do investigations and help restore services after a cyber incident or cyberattack, (Similar to a CERT). Also used to describe organizations that do the same, such as KommuneCSIRT*

IOC - *Indicator of Compromise, an indicator that a computer system or network has been breached by one or more attackers. It can be a virus file signature triggered by an Antivirus program or some other unique technical bit of information that precisely identify the attack*

NC3 - *The National Cybercrime Centre, operated by the National Criminal Investigation Service*

NorCERT -*The national, governmental CERT. Operated by NSM*

NCSC - *National Cyber Security Center, part of the National Security Authority and its mission is to be an arena for national and international cooperation within detection, handling, analysis and providing advice with respect to cyber security*

NSM - *National Security Authority, in Norwegian Nasjonal sikkerhetsmyndighet*

PPE - *Personal Protective Equipment, equipment worn to minimize exposure to hazards that could cause serious injuries or illness.*

PST - *Politiets Sikkerhetstjeneste, Norwegian police security services, has for instance counter intelligence as part of their responsibility.*

Contents

Chapter 1

Introduction

The Cold War era Total Defence concept was born out of the experiences of the Second World War (WWII) and the requirements of the Norwegian armed forces in case of a new war. In WWII, almost all the societal resources of the countries involved were used to support the war effort. If a Cold War turned hot, the scenarios required that all of the Norwegian society's resources be placed under the command of the armed forces. There was a large mobilisation force and conscription for all males. [1]. When the Cold War ended, the need for a large mobilisation force gradually disappeared. Consequently, the armed forces were gradually reduced, and many tasks that did not require military personnel were turned over to civilians. While the armed forces themselves have undergone a process and become more professionalised than the conscript mobilisation force of the Cold War.

This thesis will introduce the new Total Defence concept in Norway and how it applies to national-level cyber defence. The research problem will be described leading to the overarching research question concerning the role of the Total Defence in defending the civilian sector in times of increasingly hostile cyber operations. The methodology is presented, followed by results and analysis from

interview data. The subsidiary research questions form the frame for discussion and recommendations for action before the thesis suggests directions for future work and concludes.

1.1 The new Total Defence concept

The new Total Defence concept initially was born out of discussions on modernising the old concept starting around 2000, [2]. The Norwegian parliament started to formalise this work in the period 2003 - 2005 [3]. Since then, the concept has been evolving with the changes in the geopolitical situation and as new requirements have matured. The old total defence concept had one dimension - defence of the state in case of a military invasion from the Soviet Union. The new concept had to consider international terrorism (after 2001). The attack on the Twin Towers in New York in 2001 is the first and, so far, only time NATO's Article 5 has been used. [4]. Hybrid warfare came into sharp focus after the Russian takeover attack on Krim in 2014. However, the armed forces were interested in hybrid warfare from an earlier stage, [5]. In addition, the armed forces and the civilian sector have had an increased reliance on digitised solutions and a great number of digital platforms. This development will likely continue and accelerate if we take into consideration the fourth industrial revolution and how technology will influence and shape the world now and in the future. [6]

Some of the issues are not strictly military problems. Terrorism crosses between the military, police and the judiciary. The new Total Defence concept has had to take these issues into account, [7]. The core of the new Total Defence concept is mutual support between the armed forces and the civilian society. Central to the new concept is an enhanced security term where state and societal security and individual security are equally important. [3] Preparedness and readiness in Norway are organised according to the sectorial principle, [8] consequently, the

responsibility is currently split between 9 different governmental departments, with the justice department having the central coordinating role in peacetime. In a crisis, this will change. The department with the subject matter expertise will take the lead. In the pandemic, the Health department had the leading role for instance. In a war, the defence department will take on the leading role. The division of responsibilities is commonly referred to as the sectorial principle where the departments responsibilities continues also in a crisis [9].

The international political situation has changed dramatically over the last 25 years, from the tearing down of the Berlin wall and the end of the Cold War, through optimism that peace has come to stay, to an increasingly uncertain situation where different nation-states pursue their conflicting agendas. Causing tensions in various parts of the world, including in our northern waters. In addition to crisis and disaster situations where the civilian society needs support from the armed forces, such as the tragic events in Regjeringskvartalet and Utøya in 2011, [10] and [11] and the more recent landslide in Gjerdrum on the 30th of December 2020, [12]. The armed forces have increasingly outsourced various services to civilian businesses, such as transportation, health services, food, energy, certain communication facilities, and more. This gives the armed forces a relatively long civilian-based supply chain. The civilian society would use the same services. This is not in itself a problem - this would have been the case in the old defence concept as well. Likewise, the fact that the civilian authorities would have had to prioritise between the needs of the armed forces and the civilian society in case of a war. What has changed is the increased "just-in-time" production of a lot of goods that must be transported over huge distances, [13]. As we saw in the early stages of the current COVID-19 pandemic, where Personal Protective Equipment, (PPE), for health workers was in very high demand the world over, and the readiness stores just did not exist. Over the last thirty years, international business and service

deliveries have been increasingly internationalised with complicated ownership structures. Which could become a problem in a crisis or a war, as there are more potential targets that can affect the ability of those dependent on it to do what it is they do. While a kinetic attack may be impossible, a cyberattack may be feasible and also deniable as it could be difficult to attribute. While there is high demand for civilian services, this is a challenge in a crisis that could become a severe issue in a war. There is also the problem that all of these services are dependent on digitised solutions, such as storage management solutions, order line systems, delivery systems, secure payment systems and so on, to work efficiently, [1]. These digitised solutions and systems are exposed to cyberattacks, both in peacetime, in crisis and most certainly in a war [14]. Trying to follow the business dependencies that the new Total Defence concept depends on is a challenge. Trying to trace all software, hardware, storage facilities, people, and more than those businesses depend on is impossible. Businesses that are deemed Critical Infrastructure have extra obligations under the security laws and, in addition, may get assistance from the national security authority if required.

1.2 The new Total Defence concept and Cyberspace

An all-encompassing definition of what Cyberspace is does not yet exist. Daniel Kuehl lists several attempts in [15]. Several of the early attempts described by Kuehl focus on the technical aspect of cyberspace, that it is a network of computers, communication infrastructure or limits itself to the internet and the World Wide Web. However, Kuehl put forward that Cyberspace is a interconnected network of networks, transcending borders and allowing for creation, storage, exchange, manipulation and exploitation of information. For the purposes of this

[1] The armed forces are also highly dependent on digitised solutions - but that is not a topic for this thesis

thesis the way Bigelow in [16] describes cyberspace littorals is more suitable. Bigelow bases his work on the idea of Cyberspace littorals, first put forward by Whithers in his master thesis and described here:[17]. Bigelow sees there as being not one instance of cyberspace but many, with Internet being the largest instance by far. An individual instance of Cyberspace consists of the hardware, software, information and more that enable end to end connections, transfer data, enable transactions and disseminate information. Crucially, all networks connect to what Withers [17] defines as Cyberspace littorals. This is where each individual instance of Cyberspace meets other domains. These other domains include but are not limited to buildings, transportation networks, the radio frequency spectrum, the supporting personnel, perceptions and attitudes shaped through mass and social media. What is key with this way of perceiving Cyberspace is more than just a network. It is the ability to cause effects[2] through Cyberspace onto domains in the real world. This has placed a new tool in the hands of the world's leaders, the ability to project power through Cyberspace, as described by Joseph s. Nye [18]. To the best of my knowledge, there is yet to be found a reliable way to deter and dissuade in Cyberspace. The challenge is the most digitized nations are the most vulnerable, with the most to loose. This creates an imbalance that less digitized nations can exploit and use to their advantage. Put simply, they can attack in Cyberspace with little or no risk that the victim is able to retaliate trough Cyber, as there is very little to attack, as described by Nye in [19]. Within the new Total Defence concept, the various actors (departments) are responsible for maintaining the security of their information assets in Cyberspace. The Justice Department has an overall responsibility for coordination between the departments [3]. Beyond that, the new Total Defence concept is mainly concerned with the security of Critical Infrastructure, such as energy, electricity, food, water and more. Without which, everything will stop in the end. In the civilian sector, businesses with similar di-

[2]In military terms, effects are deny, disrupt, destroy, delay and degrade

gital challenges and sufficient resources have joined up and established their own Computer Emergency Response Teams (CERT) and share the cost. Among them, we find Nordic Financial CERT for the finance industry in the Nordics, Kraft CERT for the energy industry, HelseCERT for the Health sector and Kommune CISRT for the municipalities, to mention just a few. These are private business entities and are de facto also divided by the sector principle but by a different mechanism as it is common challenges that have brought the owners together.

1.3 Research problem

The importance of Cyberspace to businesses, government and society as a whole has increased enormously over the past decades. Reviewing publicly available reports such as those from the Norwegian secret services, National Security Authorities (NSM) and the Police Security Services (PST), we find that foreign states are very interested and pursue various activities in Cyberspace, ranging from government espionage to industrial espionage in the private sector and a whole lot of other activities. [20]. The National Security Authority (NSM) points out that Norwegian businesses lack understanding of the real threat, and consequently, the defences are not adequate and do not scale to the threat. Moreover, they also point out that threat actors increasingly exploit organisations' increasingly longer supply chains to gain a foothold such as persistent access into the digital infrastructure of their intended target. Simply because most organisations cannot follow up on the required security level of their sub-contractors. [21]. However, Nation State level activities in Cyberspace are not the only problem at hand. Looking at Næringslivets Sikkerhetsråd (NSR), reports: Mørketallsundersøkelsen, we get an overview of the state of affairs in the private sector, note that these numbers do not differentiate between crime and nation state activities. [22] Where 14% report that they have detected hacking and data breach attempts, 13% have detected phishing

or other manipulation type attacks, and 11% have detected attempts at injecting malware or viruses. There are other categories as well, but these are the larger numbers and, frankly, severe threats to any organisation. For private businesses exposed to a cyberattack in any form, the police are the only outside agency that provides support unless the organisation is a member of one of the CERT's. The exception is organisations that run Critical Infrastructure, which may also have other options. If we consider the numbers of reports to outside agencies from [22], 11% is reported to the police, 4% is reported to a sector CERT, and 2% is reported to NorCERT (the government). Consequently, most businesses are left to their own devices when dealing with a cyber incident. The police are doing what they can, but the crimes are complicated to investigate and frequently require police cooperation internationally and a significant amount of digital forensics all of which can take time. Having said that, they do have successes, such as infiltrating criminals VPN solution and consequently being able to take down different gangs, [23].

In the context of the new Total Defence concept and its role in defending the private sector in peace, crisis and war including threats arising through cyberspace, this thesis aims to answer the following overarching question:

What should the new Total Defence concepts role be in defending the civilian sector in times of increasingly hostile cyber operations

R1: What does the civilian sector need from the new Total Defence concept to effectively defend its place in Cyberspace?

R2: Does the State do enough to help with how the civilian sector protects and defends itself in Cyberspace?

R3: Is there sufficient cyber situational awareness in the Norwegian civilian sector?

Chapter 2

Literature review

2.1 Background

At the time of this writing there is a major war ongoing in central Europe. If nothing else the Russian invasion of Ukraine shows that there are states that are willing to use power to reach their ambition. Moreover, this war has already changed the security politics in western Europe and in Norway. The armed forces and civilian preparedness are getting an extra 3,5 billion this year, [24]. At present it is impossible to know how the war will end and what the long term geopolitical consequences will be, one scenario is a militarily and economically weakened Russia and a China that will much more dominant than at present. [25]. However, a militarily weakened Russia does not mean that it Cyber capacities are weakened and the Intelligence services public reports has consistently pointed to Russia and China as the most active actors in Cyberspace in Norway for the past few years. [26], [27], [20]. Predicting the future is not a science, however, as the war in Ukraine reaches its conclusion or a stalemate. European security policy will change, the new Total Defence concept will evolve as the requirements and challenges gradually manifest themselves. The Norwegian defence policy and strategy will change as a consequence of the likely inclusion of Finland and Sweden into

NATO.

The gradual and increasing digitization of society enabled by computers and networked systems lead the US Air Force to define Cyberspace as a domain in middle of the 1990s, [28]. It is quite obvious that digitization has had a positive effect on business, enabling new business models, reduce cost and enable a higher degree of automation. However, it has also enabled nation states to establish nation state hackers, with the mission to attack and enable espionage and other activities, [29]. Moreover, as more and more business has become digitized, criminals have found ways to monetize attacks in Cyberspace. Verizon publishes a yearly report detailing attacks statistics in different sectors. Approximate 90% of attacks have a financial motivation and approx 10% have a different motivation. [30], however, one should be careful to think that these numbers represent the state actor vs the criminal actor ratio, some state sponsored attacks may result in financial gain.

2.2 Cyberwar and cybercrime

The term Cyberwar has been used by academics and practitioners alike. In his 2010 book Richard A. Clarke [31] saw cyberwar as the next great threat to national security . Conversely, three years later Thomas Rid declared that cyberwar will not take place [32]. Whether the term is used to scare monger or to accurately describe a genuine threat, there are a number of significant events that give the term a level of validity. It has frequently been used to describe the events in Estonia in 2007 when a massive denial of service attack rendered most of the Estonian public services and banks useless. [33]. Following a decision by the Estonian government to move a Russian monument to the fallen soldiers from the second world war. Cyberwar is also used to describe events leading up to and following the brief

war between Russia and Georgia in 2008, where many of the same techniques as in Estonia where used. The difference being that it was followed by a traditionally military attack, [34]. The Stuxnet attack against the Iranian nuclear centrifuges in Natanz in 2010 is more of an example of a targeted strike rather than a war, [35]. In 2017 a devastating cyber attack hit Ukraine and rapidly spread globally through international businesses in Ukraine. Initially NotPetya was thought to be a ransomware virus. Unfortunately, it turned out to be a cyber weapon that was purely destructive. It was not possible to decrypt the files encrypted by the virus. [36].

Although categorized as a covert influence campaign [37], the attacks on the American presidential election in 2016 are an example of a state authorized cyberwar campaign. The well documented [38], [39] and [40] operation intended to deepen already existing political divides and reduce the reputation of one of the candidates. This type of operation is not uncommon among intelligence communities [37]. However, this attack, with respect to speed and scale, would not have been possible without the reach and access to specific groups and demographics that cyberspace allows. There are evidence to suggest that the aim was to aid Trump into the White House [41]. However there was also the opportunity to deepen already existing political divides and reduce the reputation of one of the candidates. Scott Applegate lists several situations where actions in Cyberspace has had effect in real life, including causing fatalities[42]. These examples show how Cyberspace can be used to obtain effects in the "real world" - or the littorals of Cyberspace.

These are examples of power projection and policy agendas at work. Although it can be debated to which degree the Estonian case was premeditated. Each example can be seen in terms of what von Clausewitz saw as "instruments of policy", (On War, 1832 page 88), [43]. However is it war? One of the criteria the General

sets out in his multilayered discussion of war is that war is violent.

The Norwegian peace researcher Johan Galtung introduced the term "structural violence" in his 1969 paper "Violence, Peace and Peace Research", [44]. Galtungs initial point before discussing violence in general is that if peace is absence of violence and our definition of violence is limited to deprivation of health, killing in the extreme form by an actor who intends this to be the consequence. Consequently, with this definition of violence and peace unacceptable social orders would still be a state of peace. Galtung argues that we need an extended definition of violence to be able to address this. To do so Galtung starts his definition by pointing out that violence - in his domain - is the difference between the actual and the potential, that is what is actually possible to achieve and what is the potential given different circumstances. Further, he explores violence over six different dimensions. The first one being between physical and psychological violence. The second one is the distinction between the negative and the positive approach to influence, between punishment and reward. The third distinction is if violence is present when no one or no object is hurt? Is it violence if only the threat of violence is present? The fourth distinction is if it is violence if there is an absence of an actor - a subject, there is nobody committing the violence. This is really the structural violence - the violence cannot be traced back to one or several actors. The violence is built into the structure and shows up as unequal power. The fifth distinction is between intended and unintended violence, this is important for the judicial system and decisions around guilt. Finally, there is the distinction between manifest and latent violence. Does this mean that cyberpower or the threat of cyberpower is violence? This depends, Galtung makes the distinction between the actual and the potential. Norway is a highly digitized society, consequently, the application of cyberpower or the threat of it can lead to the actual being less than the potential. I.e. that certain digitization steps are not taken or that protection meas-

ures need to be significantly stronger, making usability suffer for instance. In less developed countries or countries plagued by civil war cyberpower will not matter much as there is less digitization, if any. Other forms of structural violence may very well be present. Moreover, one could argue that the lack of resources to digitize is a form of structural violence, but the influencing factors are others than the threat of cyberattack. Finally, cyber defence of Norway is logical, but fragmented. The armed forces are responsible for their own infrastructure, however, significant portions of that infrastructure is bought or rented from civilian businesses. For civilian businesses and most of government the police is the place to get help. Over the last few years the police has added resources to fight cybercrime with the creation of Kripos National Cybercrime center, (NC3) and NSM's National Cyber security center, (NCSC). Moreover, civilian businesses - the larger Cyber security firms - have qualified themselves for access and intel sharing with NC3 and NCSC. Unfortunately, there is not sufficient resources to go around, consequently, those who get help in a crisis will be businesses that run critical infrastructure, (from the government) or those with sufficient funds to hire consultants to help. All the while, the "little guy" probably do not reach their potential. One could argue the case for structural violence in Norwegian cyberdefense.

The open threat assessments published yearly by the Norwegian Intelligence service [26], [27] and [20], have the last few years pointed clearly at the activities against Norwegian society in Cyberspace and elsewhere. These activities does not limit itself to just the government, armed forces and other high value targets. It extends also to civilian life and business, in the form of state sponsored industrial espionage and other intelligence gathering activities. Moreover, Europol reports ever increasing criminal activity in Cyberspace through their reports [45]. EUs Agency for Cybersecurity, ENISA has published numerous reports on Cybercrime, such as [46], in addition there are countless consultancy reports and special studies

that all point to an increase in both state sponsored Cyber activity and increased volume and sophistication of Cybercriminals. Here in Norway Næringslivets Sikkerhetsråd publish a bi-annually report "Mørketallsundersøkelsen" [47] states that more than half of Norwegian businesses have experienced some form of Cyber incident in the last year. While the more serious incidents are rare, (such as loss of data and industrial espionage), they do indeed happen. While the more simple to execute crimes such as phishing attempts are quite common. Unfortunately, a lot of these incidents are detected by luck rather than structured security work. Although, for those businesses that have and enforce an Information Security Management System have a better detection rate and generally gets off incidents with lesser consequences than those who don't have one. Finally and most unfortunately, many tools created with security in mind is just as useful for wrongdoers. If a cyber weapon is deployed by a nation state or a criminal, its tools, techniques and secrets will be revealed to the world. Not only to the defenders but also to other hackers. . NSA among others have lost some of its tools to the open internet, it is also well known that nation states collect and hide zero-days that they can see value in keeping secret to later use them against others.

2.3 Cyber threat intelligence

A cyberattack can be launched and executed almost at the speed of light. Network bandwidth and CPU speeds being the limiting factor. Consequently, the tool chain required to detect and deal with cyberattacks have to deal with an ever increasing amount of data and do so quickly. From the early days of the Morris worm, when antivirus software eventually got distributed on floppy disks to today where Intrusion detection systems, Intrusion prevention systems and machine learning systems and artificial intelligence work in tandem to detect, stop and prevent cyberattacks. As the threat has gone from an occasional virus on a floppy disk to

hundreds of millions of new malware each year it is clear that we need effective tools. Said tools have gone from simple signature based to today's much more advanced tools that analyse program behaviour for attack patterns. For example [48] contains examples on research on a wide range of these approaches. The tools that have come to the market in later years, shows some promise of providing more forensics data on an incident than what previously has been available.

The Cyber-Kill-Chain from Lockheed-Martin [49], is a structured approach to collect and analyse data from own infrastructure to be able to detect various actors as early as possible. It has been criticized for being dependent on a network perimeter to be able to monitor the in-going and outgoing traffic. A different approach is the diamond model, [50], which is less dependent on technology and tools and more about how to structure information into four categories for intelligence analysis. However, most of the research done is focused on actionable intelligence and techniques to stop and disrupt attackers as quickly as possible. The result is lots of Indicators of Compromise, (IOC's). Collecting forensic evidence and understand how the attack or incident unfolded is the starting point. The results can often be shared with others as Indicators of Compromise, (IOC's), and other tactical lever intelligence. Which others can use and look for in their networks and systems. For many this is sufficient, however, it makes sense to explore further. The next level, the operational level, we should try to understand the high level of the attackers architecture and his or hers profile, the what of the attacker. Finally, at the strategic level we try to understand who is responsible for the attack, what are their motivations, rationale, significance - the who and why. Then we can consider what the response should be, [51]. To achieve this however, requires first of all that the organization that does this has a level of "problematic" traffic or attacks to analyze or access to reliable data of such attacks. Moreover, the organization will need a lot of expertise on computer forensics, traditional

intelligence trade craft and analysis and experts in other fields such as sociology, history, political science and more. At this level you may not need to wait for the attack to unfold before you detect it, prepare for it and be ready. The other point is that very few business organizations have this capability, not only due to cost but also the fact that nation states have resources that are inaccessible for the average citizen. Such as wiretapping of phones and a whole lot more.It is worth noting that provided that you have intelligence at the strategic level, a warning of attack could come from monitoring of a known group that are in the early stages of planning. Consequently, it can be argued that sharing of intelligence is the only viable way forward, those who have it must find ways to share safely. This is difficult for several reasons, firstly, "How do you know", sources and methods, (at least those of a nation state), must remain secret. Second, sharing potentially business critical data can be viewed unfavorably by various competition authorities. Consequently, there has to be a legal framework to work within. Within the sector wise CERTs we have in Norway there is a legal framework to be able to share data with similar businesses - that are in competition. If Bank A knows that Bank B has an ongoing Cyber incident, that could be a competitive advantage in certain circumstances. Consequently, data is only shared between the employees that actually need it. Moreover, the police is establishing sharing agreements with business entities and CERTs. If we are going to get to the level where we can do maximum damage or cause maximum trouble for cybercriminals, state actors etc we need to get to and stay on the top of the "Attackers pyramid of Pain", [52] know their Tactics, techniques and procedures - we have to invest in intelligence. Consequently, this is a welcome development and probably a requirement in the way forward. There are examples of incidents where strategic and operational intelligence has been vital to reduce the effect, thwart and then force cyber criminal gangs to give up Norway as a viable target for their activities. Unfortunately, these examples are

not publicly available.

An influence campaign would be very difficult for the Norwegian society to defend against. Norwegian preparedness and readiness is spread out over many different departments and agencies, making a coordinate response challenging. Moreover, an influence campaign is a complex affair and even to detect it would be challenging.[53]

2.4 Situational Awareness

Situational awareness is a capability sought after by governments, enterprises and other stakeholders. The aim is to have information on the main features of a situation, and it depends on knowledge about the world or environment of current interest. Knowledge, in this case, maybe exemplified with such diverse subjects as history, economy, political and political science, sociology and more. [54] The process is to compile, process and fuse data as well as to provide an estimate of its quality. [55] It is an exercise with a technical side as well as a cognitive side. The quality of the process, the quality of the information gathered, and the understanding of the decision-makers can all contribute toward the successful or unsuccessful resolution of a situation. [56] Consequently, situational awareness is not something that relies on good intelligence alone.

The most important sources of intelligence for the new Total Defence concept are the intelligence services of the Norwegian state, primarily the armed forces Intelligence service and the Police Security Services (PST). These organizations (together with NSM) publish open threat and risk assessments once a year[1] as part of an effort to increase both the civilian sector's understanding and the general public's understanding of the threats facing the state and society. However, the cyber domain is complex, and so is the threat environment. [14], [45] It would be

[1] Previously referenced, for example, [20]

unrealistic to expect the general public to have deep knowledge of cybersecurity. At least there is reason to suspect it can be improved. [57] One would expect cybersecurity specialists to have a degree of situational awareness concerning cybersecurity issues. Moreover, it is possible to build cyber security awareness through the technical means in one's own it-infrastructure and various more cognitive tasks such as being aware of the current situation, awareness of the impact of the attack, and being aware of the attacker's behaviour and more. [58] However, it can be questioned to what extent this is possible for most businesses and other organizations in Norway. Some are members of one of the CERTs available, these will typically support members with some sort of threat intelligence, for example KraftCERT [59] and Nordic Financial CERT [60].

Chapter 3

Research methodology and design

3.1 Introduction

The new Total Defence concept is regulated by law and government-owned and regulated long-term plans and initiatives. It is also evolving with the changing world around us. One such security concern is cyberspace and how it has increasingly become an issue for all sectors within Norwegian society. Maintaining a safe and secure modern society depends upon digitalization. This means protecting against, managing, and recovering from cyber incidents when they occur. It is, therefore, a shared function relying upon good cooperation across organizational entities and societal functions. Consequently, the new Total Defence concept is both reliant upon and vulnerable to cyberspace. This thesis explores the possibilities for closer collaboration between the actors in the new Total Defence concept and elements of the civilian sector currently not associated with it.

A qualitative approach was chosen as it involves in-depth interviews with respondents who can potentially provide expert insight into the problem space. This

study could have been broadened with other approaches to research in addition to the interviews conducted. Various mixed methods could have been applied with questionnaires or other data collection forms. This would have added further validity through the ability to, for example, triangulate data sets.

3.2 Research method

This study explores the relationship between the new Total Defence concept and the civilian sector across the conflict spectrum. The exploratory nature of the research questions and the need to dig deep to gain an understanding of the problem space and the natural world complexity of it are some of the criteria to evaluate when deciding on qualitative methods. [61].

The general purpose of a qualitative research method is to explore a phenomenon to gain a better understanding. Not as much to measure or test theories. The principal characteristic of qualitative research is that it describes reality with text and not necessarily with numbers and figures. According to Strauss and Corbin, the definition of qualitative research is this:

> *"Any kind of research that produces findings not arrived at by means of statistical procedures or other means of quantification." (Strauss and Corbin, 1990, page 17) [62]*

3.3 Theoretical foundation

The qualitative research methodology and theoretical framework that seems to fit this study's requirements the best is grounded theory, (or emergent theory which is an alternative name). An alternative would be a Phenomenological study approach as both are flexible approaches that frequently use interviews as data collection method. [61]. Grounded theory is frequently used when there is little or

no theory on a subject. In this case there is ample documentation on what the new Total Defence concept is, in terms of regulations and what it is to achieve, but next to nothing on the relationship between the new Total Defence concept and the civilian sector in Cyberspace.

Grounded theory is characterised by using data to develop a theory, rather than using theory from literature to form a hypothesis to test. However, in this study the aim is not to develop a theory but to form a set of recommendations based on the data collected through interviews.

3.4 Researcher bias

It is important that the researcher is aware of own perceptions and biases. However, in practice it is impossible to avoid. There are strategies to apply to reduce the problem, [61] lists the following, (one is documented here, the other two elsewhere in the this chapter):

- **Strive for balance, fairness and completeness in data analysis and interpretation**
- **Carefully document your analysis procedures**
- **Be upfront about personal biases in the final report**

As a professional in the information security / IT security space. I have worked in organizations with support from a sector CERT and I have worked in organizations without such support. There is an obvious interest in getting support from the new Total Defence concept or organizations within it that can offer such support both, in terms of intelligence and advice.

3.5 Data collection method

There are several categories of qualitative interview designs to choose from, Turner lists the following three [63]:

Informal conversational interview This is the most flexible approach to interviews, there are no prepared questions and the conversations and range of questions follows from the interaction with the interviewee and the responses. Clarifications can be gained and it is considered beneficial since it allows for flexibility and exploration of a subject. However, some researchers views this kind of interview as unreliable and difficult to code.

General interview guide approach This is considerable more structured than the informal conversational interview as the researcher uses a set of pre-determined questions. However the researcher is given freedom in how the questions are posed and are free to follow up with questions that are not pre-determined to clarify issues or based on prompts from the participants.

Standardized open-ended interview The standard open-ended interview is very structured as an interview guide is used and all questions are pre-determined and should be asked in the same way to all respondents. However, the questions have to be open-ended to allow the respondents some freedom in answering and reflect on the questions. The idea is to get as rich a response from the interview subjects as possible. This frequently causes issues with coding as it may be difficult for the researcher to extract similar themes or topics from the different interviews.

For the purposes of this study Standardized open-ended interviews where selected, to provide as rich a response from the interviewee as possible and at the same time reduce the complexities of data analysis and coding as much as possible.

3.5.1 Motivation for the interview questions

The interview guide for the interviews can be found in Appendix A.

To be able to gain insights into and be able to answer the research questions, themes or categories where selected to build the questions around and to aid in the data analysis.

For research question one: *What does the civilian sector need from the new Total Defence concept to effectively defend it's place in cyberspace?* The following themes where selected. To be able to answer the question it is necessary to gain knowledge about the threats and how they affect the state and society. Moreover, how these threats and the situation change if we are in a crisis or a war. Consequently, the following themes where identified and incorporated into questions in the interview guide.

Threats against state
Threats against society
The most significant threats
Threshold of war
Is this a conflict
The new defence concepts defensive role in peace
The new defence concept role in a crisis or a war
Securing the state vs society

For research question two *Does the State do enough to help with how the civilian sector protects and defend itself in cyberspace?* The following themes where identified and selected. To be able to answer the question it is necessary to know who is responsible for what, if those entities does enough or if they should do more and

with the background in the literature study, how it is perceived that a given entity is responsible for critical infrastructure or not.

Should the state do more
Should big entities get help
Do bigger entities have a responsibility to help others
Limited to critical infrastructure - is it enough given the threat
Everyone for themselves

For research question three *Is there sufficient cyber situational awareness in the Norwegian civilian sector?* It is required to know how the respondents perceive the situational awareness in the general public and if they, as subject matter experts, and the security community have deeper understanding. In relation to the overarching research question it is also interesting to know if good situational awareness is limited to those who seek it out on their own-

The public understanding
Do you have this understanding
Is it shared
Understanding limited to those who seek it out

3.5.2 Selection of people to interview

Given that the interview objects would need to have some basic knowledge of both the new Total Defence concept, cyber security and to a degree knowledge with respect to how preparedness and readiness works in different parts of the the state and the private sector it took some research to gather a list of potential interview candidates. As it where half the interview candidates came of that list

while the other half self-selected to a degree, this allowed a gender balance of 50-50 to be achieved. Three out of the six where known to me and I to them.

All interviews recruited trough e-mail and the appointments for interviews where set. Each interview lasted approximately one hour. Prior to the interview the participants where provided with an information circular with information about the project, anonymity and procedures for achieving that. These are available as Appendix B and Appendix C

The interviews where conducted over Microsoft Teams and recorded on a separate recording device. To provide participants with anonymity all recordings will be deleted after the project is completed. Names and other personal information does not appear in the transcripts of the interviews. All transcripts and recordings are stored on encrypted drives and will be destroyed after the completion of the project.

The background, age bracket and gender of the respondents is as follows:

Code	**Background**	**Gender**	**Age**	**Experience**
P1	Network engineer with security responsibilities at an ISP	Male	50-55	30+yrs
P2	Former municipality CISO	Male	50-55	20+yrs
P3	Armed forces	Male	50-55	30+yrs
P4	Academic specialising in Cybersecurity	Female	50-55	25+yrs
P5	Cybersecurity specialist in the energy sector	Female	45-49	15+yrs
P6	Former employee at NSM	Female	60-65	8+yrs

A requirement within Grounded Theory is that the data collected must include the perspectives of the people being studied. [61]. The selected respondent should be qualified to maintain that requirement.

3.6 Ethical considerations

This study was carried out in accordance with the recommendations of The Norwegian Data Protection Authority. All subjects gave written informed consent to be interviewed. The subjects have been anonymized, no sensitive personal information was collected. The data has been stored on controlled electronic media, a dictaphone and an USB stick for backup. These will be erased upon completion of the project, when final grade is received.

3.7 Data analysis

The interviews where transcribed trough the use of the recording device and manually typing them into word documents.

The analysis process can be summarized as follows, based on [61]:

- Transcription and getting a general overview of the responses.
- Organize the data according to research question and theme the answer belong to.
- Identify subcategories within the data as the respondents will have different answers to the same questions and may see the world differently.
- Interpret the subcategories and summarize for each theme
- Interpret the themes and subcategories with respect to answers to the research questions and discuss.

The analysis started by going trough the transcribed interviews and highlighting the answers to the specific questions answered by the respondents. The wording of the answers varied significantly, however it was possible to identify which theme each answer belonged to. Leedy et. al. uses the therm category instead of themes, [61] and that is probably more correct terminology. The themes, (or cat-

egories), where sorted with respect to research question. All the data was entered into an excel spreadsheet according to research question, theme and respondent for easy access and analysis.

For each theme, subcategories where identified and tabulated into data points which where summarized, (in the results chapter), based on the response and an analysis of the respondents answer.

Finally, the data where interpreted with respect to the research questions, to conclude the study.

3.8 Quality assurance

The researcher is a key element in qualitative research, for the quality of the research and for the transparency of the process and how it led to the results and the conclusion. [61].

Validity in qualitative research should be addressed at the planning stage. To avoid issues with credibility and doing research that simply is not worth it.

3.8.1 Internal validity

I have clarified potential biases for me as a researcher as Leedy suggests, [61]. Moreover, I know half the respondents and they know me, this can influence results. Being open on these issues allows the reader to consider the validity of the research. Hopefully, this will increase credibility and provide a better understanding of the work.

3.8.2 External validity

This study is based on data from the real world, the respondents are experienced cyber security specialists. However the sample may not be representative as there are few respondents and no triangulation of data from other sources.

Consequently, a different researcher may come to different conclusions. However, the conclusion of this thesis still can provide valuable findings that can others can investigate further in the future.

3.8.3 Reliability

It is almost unavoidable that research will have dimensions that is not adequately covered and that there are weaknesses. If the research is reliable, it is repeatable and can be replicated at a later date by other researchers. In this study the question will be whether the respondents will answer differently to a different researcher.

During the interviews I have tried to avoid to ask questions in a leading way, allowing the respondents to reflect and answer the questions as they saw fit.

Chapter 4

Research results and analysis

4.1 Introduction

In this chapter I will present the data from the interviews centered on the research questions and the themes identified for each question. There is a short summary for each theme written by me that tries to sum up the answers, followed by a table summing up the key data elements and counts. This is followed by relevant quotes from some of the respondents relevant for each theme.

4.2 Themes relevant for research question one

Research question one is: R1: What does the civilian sector need from the New Total Defence Concept to effectively defend it's place in cyberspace?

Threats against the state

All of the participants listed one or several threats they considered the most important today. Ranging from influence operations, Ddos[1] attacks and ransom-

[1]A Ddos or Distributed denial of service attack is a malicious attempt to overload a website or service with traffic such that it is unusable for legitimate users

ware. However, three of the participants went a bit deeper and talked about more structural issues for us as a nation and population.

respondents	**Data element**	**Count**
P1, P3	Ransomware	2
P1	Ddos attacks	1
P1	Influence operations	1
P2, P4, P6	Lack of understanding and realization of threat level	3
P6	The states dependency on long civilian supply chains	1

"*We are naive as a nation, we don't understand that there are people out there with an agenda that will use whatever tools available to reach their goal. Hybrid threats, whatever. People think that Internet is about freedom, but anything that can be used can also be misused. Crime on the internet has surpassed all other crime in terms of money "earned". The kids are expert at privacy, in theory, but they don't get it and still act as it does not matter. As does the grown ups as they lack the tools to understand. This is a major threat to the state, society and the individual as it is too easy for someone with an agenda and a target to gain information on individuals, their place of work and their vulnerabilities.*"

- P2

Threats against society

The respondents did not in general separate between state and the society, not even on a direct question as we shall see later. Consequently the responses to this question was very much the same as questions about the state. However there are some interesting additions

respondents	Data element	Count
P2	Constant information gathering and influence operations	1
P6	Ability to run a business to a complete halt	1

The most significant threats

The answers here where significantly more varied. Ranging from Ddos attacks, ransomware and influence operations. However, more weight was put on influence operations that actually change peoples opinions and attacks on infrastructure or systems that are difficult to replace or get going again.

respondents	Data element	Count
P1, P3, P5	Ransomware	3
P1, P5	Ddos attacks	2
P1, P4	Influence operations	2
P2, P4	Lack of understanding and realization of threat level	2
P5	Information theft	1
P5	Ddos and information theft combined with blackmail	1
P6	Long term knockout of critical infrastructure that affects the whole society	1
P6	Long term knockout of important and critical businesses	1
P6	Criminals looking for money	1

"Ransomware, information theft and denial of service attacks combined with blackmail."

- P5

Threat increase the last few years

There is a general consensus that there is uncertainty in whether there is an increase in the last few years in terms of threats in cyberspace. Cyber threats are more written about in the press, consequently it is more in the public's mind. Additionally, we have digitized more and more and the increase may simply be a result of more targets. The current situation has been predicted a long time ago.

respondents	**Data element**	**Count**
P1	Is it an increase or is it just more publicized	1
P2, P3	More and more discover the ability to yield power in cyber	2
P3, P4, P5, P6	Increased digitization and more people and businesses in Cyberspace	4

"*There are economic incentives for criminals to make money. This and the fact that internet increasingly is available for everyone. This has been predicted several years ago. The internet is designed to be a sharing platform among equal trusting partners, that some see it as a platform for exploitation is not surprising at all. The state actors have been there all along, they just use the latest available technology.*"

- P5

Threshold of war

Our current situation is more of a "Grey" war, that is not an actual war that people die in, but an ongoing situation where tools are being prepared. Consequently, it is a constant struggle between defenders and attackers.

respondents	Data element	Count
P1	If important governmental functions are shut down	1
P2, P5, P6	Threshold erased, consequence a continuous "Grey" war	3
P3	What we see is well below the threshold of war	1
P3	The actions may very well have severe economic consequences	1
P4	People start dying	1

"*This very long and very grey, war is terminology used with respect to war against drugs for instance.It is no longer the case that war is declared on another state, you have such things as hybrid warfare for instance. Again it is not really something new, it is just exploiting the available opportunities at present time. .*"

- P5

"*I think the threshold of war is to an extent erased. What we have today is a situation of continual war, but in a preparatory sense. What a goverment wil decide is crossing the line is probably dynamic. This has been going on for years and is part of the interstate power struggles.*"

- P2

Is this a conflict, do you feel like you are in the trenches

The current situation is not a conflict at present, however it is a power struggle.

respondents	Data element	Count
P1, P4, P5	No, cyberattacks will irate and annoy	3
P2	yes, but not in trenches, in the open field	1
P3, P4, P6	Cyber is used as a tool in conflicts	3

"No, not really. A cyberattack does not have the capacity to take down an entire country without affecting others so it will also affect the attacker to a degree. Consequently a cyberattack will irritate and annoy. Maybe China and Russia have separated their networks sufficiently to do something like that, I do not know."

- P4

4.3 Themes relevant for research question two

Research question two is: R2 Does the state do enough to help?

Should the state do more

In general yes, the state should do more to help, however this is difficult and not easy to achieve. One suggestion was more regulations for various technical gear that was vulnerable for attack. But the primary issue was more information sharing and less secrecy and more transparency.

respondents	**Data element**	**Count**
P1, P4	Regulations for a level playing field	2
P5	Regulation of critical infrastructure	1
P2, P3, P4, P6	Sharing more information and less secrecy	4
P3	Lack of a good, non intrusive model for helping	1

"The state has an important role in relation to the private sector, there has been established structures for a tight and good working relationship the national cyber security center, (NCSC) has an important role. I think this information sharing, where the point is to get it out quickly and sometimes the threat is found and reported from the private sector to NCSC. We could probably invest more into this, but

it is probably a insatiable need. There are also established several agreements with private businesses to aid in the incident handling. Getting attention from the press is unfortunately only possible when an attack has happened."

- P6

"I am very much in favour of sharing and transparency, those in the know should share more. And that these issues are discussed in more open forums than today. The state also has a responsibility for regulations and provide a level playing field. What is illegal here may be legal in other states and so on and so forth."

- P4

Should big entities get help

Consensus is that they should and to some extent they do. However, there is a difference between threat actors, crime is the responsibility of the police. Actors beyond that is definitely the responsibility of the state. But getting help is not without its own set of problems.

respondents	**Data element**	**Count**
P1, P2, P6	Yes, some do to and expect that	3
P1, P2	Smaller companies too	
P3	Regardless of size this is a police and state responsibility	1
P5	Expect them to be member of a CERT already	1
P5	Should establish a private-public cooperation forum	1

"*Or ask the opposite question, should they help the state? I am still in favour of openness and transparency. Any business will likely have business secrets etc that*

will be compromised if someone came in to run their network in a crisis. And the business itself knows most of anybody of its it infrastructure, thus direct help may not be optimal. But more sharing (both ways) will probably do more for security than anything else"

- P4

Do bigger entities have a responsibility to help others

This is complicated as businesses can and are in direct competition with each other and it is very difficult to formally put that kind of responsibility on an actor in the private sector. However, certain types of knowledge and best security practices can be shared, (and they do).

respondents	**Data element**	**Count**
P1, P2, P3, P4	Yes, but this is complicated legally and practically	4
P4	Should share knowledge and be transparent	1
P5, P6	Cannot put this responsibility on anyone legally	2

"*Yes, to maintain the society we have we have to look out for each other. Businesses are better served with actually having competition. Telenor is a good example, sharing information and competence. The National cybercrime centre is doing a good job, but they still are a bit anonymous and quiet.*"

- P2

Limited to critical infrastructure – is it enough given the threat

This is tricky, there is a lot of changes going on in what constitutes critical infrastructure due to the new security law. And it is by no means settled what is and what is not. The recent pandemic has shown that what is usually easily

accessible and easy to acquire may not be in a crisis. So much so that employees in the retail sector got preferential Right to kindergarten while other groups did not.

respondents	**Data element**	**Count**
P1, P2, P3, P4, P6	No, and what is Critical Infrastructure will change with time	5
P3	Insufficient resources to cover everything? - crisis management in large	1
P1, P4, P6	What is critical infrastructure can change in a crisis	3

"No, and I don't think that NSM thinks that either. After NCSC was established we've seen a stronger involvement in the civilian society. And as the departments gets done with what is critical infrastructure I think we'll see that a lot more is critical infrastructure than what we are used to think. However, placing responsibility doesn't mean that it is taken. Crisis's needs to be rehearsed, preparations made. when it all goes wrong you need people to know what to do."

- P2

"This is tricky, Telenor, Statnett etc is critical infrastructure. But the it systems of Rema 1000 could just as well be critical infrastructure. You have to make sure that people are fed. There are an awful lot that is critical infrastructure in a given situation. "

- P1

The new defence concepts role in peace

Several respondents point out the importance of using peace time for training and preparations. But also warns that the resources to do so must be present, otherwise the preparations will not be there when you need them. Moreover, the

role of the New Total Defence Concept in peace time should be handled by the line organizations set up to handle them, the police should handle crime and so on.

respondents	**Data element**	**Count**
P1, P2, P3, P4, P5, P6	Yes	6
P1, P4	Use peacetime for training and preparations	2

"*The new total defence concept is very big, it is private sector, the entire society and the armed forces. A good example of how the thing works is the recent pandemic. Figuring out what is critical, what is a priority to avoid that society breaks down completely.*"

- P5

The new defence concepts role in a crisis or a war

There is concern over long sub-contractor chains to deliver services during a crisis or a war. These could be prime targets themselves to hamper others in the chain. Moreover, who would get help first would be based on a risk assessment and an assessment on what is important now.

respondents	**Data element**	**Count**
P1, P2, P3, P4, P5, P6	Yes	6
P1, P5	long supply chains and small businesses is a challenge	2
P4, P5, P6	Who gets help first is based on an risk assessment	3

"*We don't really know until we are there. It is important to remember that most businesses in Norway is small and that in cyber we need competency and these small companies can be critical factors in delivering services in a crisis or a war.*"

- P5

Securing the state vs the society

Overall, the distinction does not make any sense anymore from all participants.

respondents	Data element	Count
P1, P2, P3, P4	There is next to no difference, the separation makes no sense anymore	4

"*In the traditional sense you would think about the state as the administration and all that. But I don't think this is very useful anymore. In cyberspace, due to the digital revolution it all floats together and I doubt that this is a meaningful separation there.*"

- P2

Everyone for themselves

No, most will want to share information if they can and help each other out if they can.

respondents	Data element	Count
P1, P3,	No, but there is room for improvement	2

"*No not really, most will want to share information and improve the way that they defend themselves*"

- P1

Public understanding

In general, no there is not good understanding in the public. It may be improving due to more media attention etc, however, large attacks happens elsewhere which means that people may think it is someone else's problem.

respondents	**Data element**	**Count**
P5	I don't really know	1
P2	No	1
P1, P6	not enough understanding, but signs of improvement	2

"*Yes and no, in general I think maybe people are starting to understand that there are such things as influence operations and how they work. But I don't think they understand the severity of it. In general people don't really understand until it they feel it themselves. NSM has an important role in explaining these things to the public.*"

- P1

Do you have this understanding

As part of their job and with the ability to discuss matters with colleagues - yes. However, no one claims to know the full picture.

respondents	**Data element**	**Count**
P1, P2, P5	Yes, as part of my job I know more than most	3
P6	I recon my understanding is in line with the general public	1

"*Yes I think I do, as a result of my job as part of it is to know the threat picture.*"

- P5

Is it shared

The fact that the media has taken up an interest and write about cyber incidents and security helps. However, they mostly write about this once an attack has happened.

respondents	Data element	Count
P1	That the media writes about it helps the public understanding	1
P3, P4	Internal discussions for us in the field helps a lot	2
P1, P4	Big difference between the community and the public	2

""*For us that work in the field think we share a lot of common understanding. There are nuances and detail on specific bits of the field. If I think about my friends that do not work in the field, we are definitely more strict than they are. They are more positive than us*"."

- P4

Understanding limited to those who seek it out

Being proactive and interested is an asset, however we should not ignore people that speak different languages than us, (security language vs the business language). It is our responsibility to make ourselves understood outside of the security community.

respondents	Data element	Count
P1, P2, P3,	It helps to be interested and proactive, in general they know more	3
P5	Depends on the understanding you need	1

"*It is definitively an asset to be proactive and seek out information to better prepare and defend oneself and ones organization. Knowledge is king*"

- P1

Perspective changed

All but one say no, but - they have thought more about things they had not thought much about before

respondents	**Data element**	**Count**
P1	Yes	1
P2, P3, P6	My thinking has become more clear on some issues	3
P4, P5	Not really	2

"*Yes and no, I think my opinions have become more clear to myself and more cemented.*"

- P1

Chapter 5

Discussion

5.1 Introduction

The chapter is organized after the research questions. Consequently, the themes from the data and the relevant literature are discussed in sections.

5.2 R1: What does the civilian sector need from Totalforsvaret to effectively defend its space in Cyberspace?

The first part of the interviews deals with the threat against the state and society. However, the participants do not distinguish between state and society. Instead, they conclude that it is all and the same. From a certain perspective, this makes sense, ransomware can and do affect anyone from the smallest business to the huge corporations and parts of the government. As of late, ransomware has been a tool for criminals to gain a reasonably quick return on investment. On the other hand, influence campaigns are a tool that various state actors use that affects the entire society. Consequently, it is debatable if there exists an absolute separation between state and society. However, if we look at the literature and consider the statistics of attributable attacks and their culprits, we find that close to 90% are

criminal in their motivation, while 10% are state actors. Bearing in mind that there are criminal organizations that do the state actors bidding, it is still an argument that there are differences in the kinds of attacks that the state will experience - from primarily state actors or their helpers - looking for state secrets. While the society obviously will experience influence campaigns and other attacks typically associated with the state, the bulk of the activity will come from criminals, and the motivation will be financial. Consequently, the requirements in terms of intelligence and other forms of help are almost certainly somewhat different.

Information Security has been a growing business area for several years. Due to the fact that more and more organizations are exposed to cyberattacks. Respondent P5 points out that this is entirely predictable[1]. The internet and associated networks were set up between equal and trusting partners. As the technology has matured, so has the interest of parties whose primary interest has been exploitation with the aim of making money with whatever means available, or espionage or destruction, as pointed out by respondent P3. The increase in cyber threats may result from the increased attack surface arising from mass digitization. War is the most extreme form of enforcing one's will on another state. While examples of using Cyberattacks or cyber power in wars exist and have been a part of warfare since at least 2008 with the Russian attack on Georgia. No one has yet started a war that occurs solely in the Cyber Domain alone. However, does the civilian sector need to prepare for a Cyberwar, and when is a Cyberattack a war? While none of the interview participants supported the idea that we are currently in a cyberwar, it was clear that the activities they describe, such as exploiting opportunities to further their own agendas and preparation for future vulnerability exploitation, mean there is great competition occurring almost right up to the threshold of conventional 'war'. While we are not in the trenches, so to speak, we need to

[1]Bruce Schneier an American cryptologist, was mentioned by one of the interviewees as one of these predictors

accept that Cyberspace is contested. Consequently, the civilian sector may need to prepare for war or at least consider what could be the consequences of a real kinetic war and how that will affect their own corner of Cyberspace.

Considering the literature with the information provided by interview respondents, it can be assessed that, for the civilian sector to effectively defend its digital space, then the new Total Defence concept should focus on the following areas: Continue the publication of open threat assessments, perhaps increase the focus on the Cyber Domain. Provide more support and help preparing for crisis and war scenarios, to have a more robust civilian sector in the digital domain.

5.3 R2: Does the state do enough to help?

While interview the data shows that it is the responsibility of the state to protect and help the civilian sector, it also shows that in the context of cyberspace, and in particular cyber defence, it has been challenging to find a model that is not overly intrusive to the civilian business model concerning business interests, privacy concerns, intellectual property and legal aspects. The example given by P4 was that help easily could result in a third party being privy to full access to the victim's network and inner secrets, which could be problematic in some cases, even if state employees are sworn to secrecy. However, less secrecy, more transparency and information sharing should be done, provided a suitable model for information sharing can be found.

The state depends on the civilian sector to a large degree. The competencies required to run and secure many public and not so public services lie within these companies. Communication, transportation, logistic support, and delivery of computers, networks and software are all examples of services provided by the civilian sector that contribute to the supply chains for both society and the state. Not all of these third party suppliers may have the competencies to secure their services

without help or assistance from others. The interview data indicate that those who can, including the state, should help those who lack the resources. However, as P4 pointed out in the interviews, this help and information sharing should or could go both ways. Indeed as NSM points out in their public risk report, they need reports from the civilian sector as well. [21].

The new Total Defence concept will evolve and most certainly now with the almost certain addition of Sweden and Finland into NATO due to the war in Ukraine. However, this may set the focus on defence policy and the inevitable changes for Norwegian defence strategy and lessen the focus on Cyber related issues, at least for the short term.

In sum, the state requires help from the civilian sector, even if there is no solid sharing model at present. The data suggest that transparency is essential, that information and intelligence should be shared as much as possible, and that those who can should also contribute to publicly available research. Finally that also knowledge and best practices should be shared. Like some of the bigger civilian sector businesses are doing. Some of the required building blocks probably already exist to move forward. The civilian CERTs already have procedures and formats for sharing information internally and with their members. The same applies to the state. The challenge is to merge these two for mutual benefit. As pointed out by several of the interviewees, the establishment of the National Cyber Security Centre (NCSC) within NSM has helped, but it needs to evolve.

5.4 R3 Is there sufficient situational awareness in society?

From the study, it is evident that there is not sufficient understanding of the cyber situation in society. There is some evidence to suggest that it is improving

due to increased media interest. However, the problem with media is that it is usually only interested when there has been a successful attack, and then the attention disappears without discussing the deeper issues. That Cyberspace is a contested environment and various actors use it to forward their agenda or for financial gains. P3 suggests that one possible (partly) explanation is that people have trouble relating to threats that have no physical presence.

From the literature, we know that gaining solid situational awareness of any situation is a challenge. There is an extra technical challenge in the cyber domain to extract information from own infrastructure and combine that information with information from other sources and domains. In the study, P3 points out that to improve our ability to disseminate information and intelligence, it is essential to be able to discuss attacks, situations and incidents with other subject matter experts. Preferably also from other domains than cyber, this enhances our understanding and situational awareness.

To contribute to a better understanding and situational awareness, the study shows that the cyber security community must be more concrete and use examples that the audience can relate to more directly. Avoid talking about the latest cyber-attack the media is writing about, as it will quickly become technical and alienate the audience. Moreover, the same applies to the language used. Avoid using cyber security language and terms and use terminology the audience can relate to and understand.

Chapter 6

Recommendations and further work

6.1 Introduction

Through semi-structured interviews with a focus group, this study has investigated the role of the new Total Defence concept in defending the civilian sector across the conflict spectrum. Based on this research, the following recommendations are made together with a suggestion for further work.

6.2 Recommendations

The study revealed that with the threat the Norwegian society is under, there is a clear need for more information sharing and transparency from the state to the civilian sector and from the civilian sector to the state. Moreover, there is a need for an information-sharing model that can support this information sharing that is operationally sound and does not intrude on the secrets the various organizations may have that they need to keep for themselves. Finally, there is a need to enhance the public's understanding of the threat and the impact threats and attacks in

cyberspace have on society, business and the state. To achieve this or improve the situation, the cyber security community and its professionals should be more concrete in their communication and use language more in line with the language the public is using.

To summarize:

More transparency and information sharing between the state and civilian sector

Creation of a non-intrusive model for information exchange and other aid

The cyber security community must be more concrete in their communication with businesses and the general public and use a language that the audience can relate to

6.3 Further work

As this study has shown, there is a requirement for a model to share information and help the cyber defence actors in Norwegian society. Identifying this model is a serious challenge as it, for example, encompasses the requirement to keep secrets secret. Provide the correct information at a functional and not overwhelming level of detail. Moreover, maintain legal requirements as organizations sharing information may be in direct competition with each other. While the state cannot provide anyone with an advantage - there has to be a level playing ground for all involved. This is no easy task and likely requires work on different levels and subjects of study.

Chapter 7

Conclusion

The aim of this study is to explore what the new Total Defence concepts role should be in defending the civilian sector in times of increasingly hostile cyber operations.

The current cyber threat picture is dominated by ransomware and influence campaigns this will likely change in the future to something different. Moreover, the new total defence concept will evolve over time and change as the world around us changes. Now most recently as a consequence of the war in Ukraine and the likely inclusion of Sweden and Finland into NATO. The latter will likely also change Norwegian defence policy and strategy dramatically.

The study has utilized semi-structured interviews with a focus group to explore the relationship between the new Total Defence concept and the civilian sector. First, what does the civilian sector need in terms of help, what are the threats to society and the state? Second, who should provide help and does this change across the conflict spectrum? Finally, is there sufficient understanding and situational awareness in the Norwegian society and within the security community given the threat we are under?

This study showed that the civilian sector not only needs help from the state,

but that it would also benefit the state to provide this cyber support. The question remains; what kind of help and how to provide it. As presented in this thesis, so far it has proved difficult to create a 'state-civilian sector' model that is sufficiently non-intrusive and operationally effective at the same time. To improve the public understanding of the situation in cyberspace and the threat we are under, cyber security specialists should take care to be concrete and use a language that the audience will recognize and not feel alienated by.

The study has identified more transparency and more information sharing as key ingredients to how the state can and should provide support to certain elements of the civilian sector. It is important to note that the supply chains in both the states own infrastructure and in the private sector are long, and that not all suppliers in the chain are large organizations with large and efficient cyber security organizations. These specific organizations may require more support than larger organizations with more resources. In addition, the civilian sector should also contribute back to the state.

Bibliography

[1] Norheim-Martinsen, *Det nye totalforsvaret*. Gyldendal, 2019.

[2] P. M. Norheim-Martinsen, 'Introduksjon: Det nye totalforsvaret - utviklingstrekk og utfordringer,' in *Det nye totalforsvaret*. 2019.

[3] J. o. b. Forsvarsdepartementet, *Støtte og samarbeid, en beskrivelse av totalforsvaret i dag*, 2018. [Online]. Available: https://www.regjeringen.no/contentassets/5a9bd774183b4d548e33da101e7f7d43/stotte-og-samarbeid-en-beskrivelse-av-totalforsvaret-i-da.pdf.

[4] NATO, 'Collective defence - article 5,' North Atlantic Treaty Organization, Tech. Rep., 2022. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_110496.htm.

[5] E. Daltveit, J. F. Geiner and P. Ydstebø, 'Trender i millitære ope'rasjoner,' *Forsvarets forskningsinstitutt*, 2010.

[6] K. Schwab, *THE FOURTH INDUSTRIAL REVOLUTION (INDUSTRY 4.0) A SOCIAL INNOVATION PERSPECTIVE*. 2017. DOI: 10.25073/0866-773x/97.

[7] A. B. Thomstad, 'Totalforsvaret i et millitært perspektiv,' in *Det nye totalforsvaret*, P. M. Norheim-Martinsen, Ed. Gyldendal, 2019, ch. Totalforsvaret i et millitært perspektiv, pp. 41–61.

[8] Regjeringen. (2021). 'Hovedprinsipper i beredskapsarbeidet,' [Online]. Available: https://www.regjeringen.no/no/tema/samfunnssikkerhet-og-

beredskap/innsikt/hovedprinsipper-i-beredskapsarbeidet/id2339996/ (visited on 01/05/2022).

[9] Regjeringen. (2003). 'Nasjonal krisehådtering,' [Online]. Available: https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Innstillinger/Stortinget/2002-2003/inns-200203-009/9/ (visited on 29/05/2022).

[10] S. Solheim, E. Senel and F. Ighoubah. (2014). 'Politiet har fått klarsignal til å bruke forsvaret,' [Online]. Available: https://www.nrk.no/norge/politiet-far-hjelp-av-forsvaret-1.11849651 (visited on 02/05/2022).

[11] NOU, 'Rapport fra 22. juli-kommisjonen,' 2012.

[12] M. Endregard, 'Totalforsvaret i et sivilt perspektiv,' in *Det nye totalforsvaret*, P. M. Norheim-Martinsen, Ed. Gyldendal, 2019, ch. Totalforsvaret i et sivilt perspektiv, pp. 62–80.

[13] T. Listou, 'Totalforsvaret og komersielle aktører - den dobble logistikkutfordringen,' in *Det nye totalforsvaret*, P. M. Norheim-Martinsen, Ed. Gyldendal, 2019, ch. Totalforsvaret og komersielle aktører - den doble logistikk utfordringen, pp. 100–116.

[14] Enisa. (2021). 'Threat landscape 2021,' [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (visited on 20/08/2021).

[15] D. T. Kuehl, *From cyberspace to cyberpower: defining the problem*. Potomac, 2011, ch. 2, pp. 24–42, ISBN: 1597974234.

[16] B. Bigelow, 'The topography of cyberspace and its consequences for operations,' *IEEE*, 2018.

[17] P. Withers, 'What is the utility of the fifth domain?' *Air Power Review*, vol. 18, no. 1, pp. 126–150, 2015.

[18] J. S. N. jr., *The future of power*. Public Affairs, 2011.

[19] J. S. Nye, 'Deterrence and dissuasion in cyberspace,' *International Security 41.3*, pp. 44–71, 2017.

[20] T. N. I. service, 'Fokus 2020,' The Norwegian Intelligence Service, Tech. Rep., 2020.

[21] N. sikkerhetsmyndighet, 'Risiko 2022,' Nasjonal sikkerhetsmyndighet, Tech. Rep., 2022. [Online]. Available: https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf.

[22] N. Sikkerhetsråd, 'Mørketallsundersøkelsen,' Næringslivets sikkerhetsråd, Tech. Rep., 2020.

[23] A. Scroxton. (2022). 'Police take down vpn inked to multiple ransomware hits,' [Online]. Available: https://www.computerweekly.com/news/252512108/Police-take-down-VPN-linked-to-multiple-ransomware-hits (visited on 20/01/2022).

[24] J. B. Morud and A. Rognstrand, 'Regjeringen foreslår 3,5 milliarder kroner ekstra for å styrke forsvaret og sivil beredskap i år,' Forsvarets Forum, Tech. Rep., 2022. [Online]. Available: https://forsvaretsforum.no/budsjett-forsvaret-politikk/regjeringen-foreslar-35-milliarder-kroner-ekstra-for-a-styrke-forsvaret-og-sivil-beredskap-i-ar/254626#:~:text=Regjeringen%20vil%20be%20Stortinget%20om,skal%20styrke%20den%20sivile%20beredskapen..

[25] Ø. Tunsjø. (2022). 'Krigen endrer usas forsvarsstrategi,' [Online]. Available: https://www.nrk.no/ytring/krigen-endrer-usas-forsvarsstrategi-1.15924930 (visited on 13/04/2022).

[26] T. N. I. service, 'Fokus 2018,' The Norwegian Intelligence service, Tech. Rep., 2018.

[27] T. N. I. service, 'Fokus 2019,' The Norwegian Intelligence service, Tech. Rep., 2019.

[28] M. Hayden. (2010). 'Black hat keynote,' [Online]. Available: https://www.youtube.com/watch?v=pKZDYgj0KTA (visited on 13/10/2021).

[29] R. Joyce. (30th Oct. 2016). 'Disrupting nation state hackers,' [Online]. Available: https://www.usenix.org/conference/enigma2016/conference-program/presentation/joyce (visited on 15/01/2022).

[30] Verizon. (2022). 'Data breach investigation report,' [Online]. Available: https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf (visited on 15/03/2022).

[31] R. A. Clarke and R. K. Knake, *Cyber war: The next threat to national security and what too do about it*. HarperCollins, 2010.

[32] T. Rid, 'Cyber war will not take place,' *Journal of Strategic Studies*, vol. 35, pp. 5–32, 2012.

[33] A. Jenik, 'Cyberwar in estonia and the middle east,' *Network Security*, vol. 2009, no. 4, pp. 4–6, 2009, ISSN: 1353-4858.

[34] D. Smith, 'Cyber-war!' *Tabula*, 2010.

[35] J. P. Farwell and R. Rohozinski, 'Stuxnet and the future of cyber war,' *Survival*, vol. 53, no. 1, pp. 23–40, 2011. DOI: 10.1080/00396338.2011.555586.

[36] A. Greenberg, *The untold story of notpetya, the most devastating cyberattack in history*, 2018. [Online]. Available: https://qualityplusconsulting.com/BBytes/2018-8-22_NotPetya-TheMost%20DevastatingCyberattackInHistory.pdf.

[37] M. Hayden. (2017). 'Oxford union 2017 q&a with mike hayden,' [Online]. Available: https://www.youtube.com/watch?v=exw9HpK_ytI (visited on 13/10/2021).

[38] R. Diresta and S. Grossman, 'Potemkin pages & personas: Assessing gru online operations,' in *Stanford Internet Observatory, Cyber Policy Center*. 2019.

[39] Diresta, 'The tactics & tropes of the internet research agency,' Tech. Rep., 2018.

[40] Howard, 'The ira, social media and political polarization in the united states,' 2018.

[41] D. S. Luke Harding Julian Borger, *Kremlin papers appear to show putin1s plot to put trump in the white house*, 2021. [Online]. Available: https://www.theguardian.com/world/2021/jul/15/kremlin-papers-appear-to-show-putins-plot-to-put-trump-in-white-house.

[42] S. D. Applegate, 'The dawn of kinetic cyber,' *5th international conference on cyber conflict*, 2013.

[43] C. v. Clausewitz, *On war*, M. Howard and P. Paret, Eds. Princeton, 1989.

[44] J. Galtung, 'Violence and peace, peace and research,' *Journal of Peace Research*, vol. 6, pp. 167–91, 1969.

[45] Europol, 'Internet organized crime threat assessment.,' Europol EC3 European Cybercrime Centre, Tech. Rep., 2019.

[46] ENISA, 'Threat landscape,' 2018.

[47] N. Sikkerhetsråd, 'Mørketallsundersøkelsen,' Næringslivets Sikkerhetsråd, Tech. Rep., 2018.

[48] A. Dehghantanha, Mauro, T. Conti and Dargahi, *Cyber Threat Intelligence*. Springer, 2018, vol. 70.

[49] R. A. E.M. Hutchins M.J. Cloppert, 'Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains,' *Leading Issues in Information Warfare & Security Research*, p. 80, 2011.

[50] C. B. Sergio Caltagirone Andrew Pendergast, 'The diamond model of intrusion analysis,' *DTIC Technical Reports*, 2013.

[51] T. Rid and B. Buchanan, 'Attributing cyber attacks,' *Journal of Strategic Studies*, vol. 38, no. 1-2, pp. 4–37, 2015.

[52] D. J. Bianco, *Pyramid of pain*, Website, 2013. [Online]. Available: `http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html`.

[53] A. Bergh, 'Påvirkningsoperasjoner i sosiale medier - oversik og utfordringer,' *FFI*, 2020.

[54] D. Omand, 'Etterretningsanalyse i den digitale tid, en innføring,' in, S. Stenslie, L. Haugom and B. H. Vaage, Eds. Fagbokforlaget, 2019, ch. Et historisk tilbakeblikk, pp. 33–50.

[55] U. Franke and J. Brynielsson, 'Cyber situational awareness – a systematic review of the literature,' *Computers amp; Security*, vol. 46, pp. 18–31, Oct. 2014. DOI: `10.1016/j.cose.2014.06.008`.

[56] D. Omand, *Securing the state*. Hurst & Company, 2014.

[57] K. Olmstead and A. Smith. (2016). 'What the public knows about cybersecurity,' [Online]. Available: `https://www.pewresearch.org/internet/`

wp-content/uploads/sites/9/2017/03/PI_2017.03.22_Cybersecurity-Quiz_FINAL.pdf (visited on 29/05/2022).

[58] P. Barford, M. Dacier, T. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, J. Li, P. Liu, P. Ning, X. Ou, D. Song, L. Strater, V. Swarup, G. Tadda, C. Wang and J. Yen, 'Cyber situational awareness,' in. Springer US, 30th Sep. 2009, vol. 46, ch. Cyber SA: Situational Awareness for Cyber Defence, pp. 3–13. DOI: 10.1007/978-1-4419-0140-8_1.

[59] KraftCERT. (2021). 'Kraftcert tjenester,' [Online]. Available: https://www.kraftcert.no/tjenester.html (visited on 29/05/2022).

[60] N. F. CERT. (2022). 'Metode,' [Online]. Available: https://www.nfcert.org/#metode (visited on 29/05/2022).

[61] Leedy and J. Ormrod, in *Practical research : planning and design*. Pearson, 2015, p. 407.

[62] A. Strauss and J. Corbin, *Basics of Qualitative Research: Grounded Theory Procedures and Techniques.* SAGE Publications, 1990.

[63] I. Turner Daniel W., 'Qualitative interview design: A practical guide for novice investigators,' *The Qualitative Report*, vol. 15, no. 3, pp. 754–760, 2010. DOI: 10.46743/2160-3715/2010.1178.

Appendix A

Interview Guide

A.1 Interview guide

Introduction:

About me, my role as a researcher and the consent form.

Please tell me something about you and your role where you work?

State of affairs – what do you think about the various threats against Norwegian state and society in Cyberspace

Why would you say there has been an increase in threats against society in Cyberspace in the last few years?

What would you consider to be the most significant threats?

(This bit is stated by me to set a direction for the rest of the interview) Norwegian intelligence services warns of increased activity from foreign states. Mike Hayden describe a lot different activities as “Good old fashioned honourable espionage” up to a point. The Norwegian foregin affairs minister attributes attacks on

the Norwegian state assembly to Russian intelligence. Some threshold here has been crossed and govt is saying enough is enough.

What are your thoughts on the threshold of war?

Do you feel like you are "in the trenches" so to speak in some form of conflict?

Do you think the State should do more?

Relationship between "Det nye totalforsvaret» and civil society and buisnesses.

(Peace, crisis and war) Norway has few big entities that are capable of defending themselves, should or could they expect help?

Do they have a responsibility to provide help to others?

Does totalforsvaret have a role in aiding businesses in the time of peace?

How would this change in a crisis or war?

In cyber it is everyone for themselves?

As of now totalforsvaret is limited, to critical infrastructure in form of who will get direct help in a crisis, given the discussion so far, is this sufficient when we consider the threat we are under?

Why, do you think, we differentiate between securing the state and securing society?

Situational awareness

Is there an understanding in the general public in terms of what the situation really is?

Do you believe you have this understanding and is it a shared understanding?

Or is it limited to those who bother to investigate and use available tools and own creativity?

Finally: How has your perspective changed over the course of this interview?

Appendix B

Invitation to participate

B.1 Invitasjon til å delta i forskningsprosjekt om Totalforsvaret og dets rolle i forsvar av Cyberspace.

Hei,

Mitt navn er Kristian Andre Kastet og jeg studerer informasjonssikkerhet ved NTNU. I forbindelse med mitt master prosjekt så trenger jeg å snakke med folk som har god forståelse for hva det «nye totalforsvaret» er og som samtidig har god forståelse for Cybersikkerhets problemstillinger.

Jeg skal ikke behandle personopplysninger og innholdet fra samtaler blir håndtert konfidensielt. Alle data vil bli slettet så snart prosjektet er ferdigstilt i løpet av 2021. Det vil ikke under noen omstendighet være mulig å spore detaljer i masteroppgaven tilbake til deltageres identitet eller arbeidsgiver. Innsamling av data følger retningslinjer gitt ved NTNU og Norsk Senter for Forskningsdata, (NSD).

Intervjuet vil bli foretatt på et tidspunkt som passer deg og vil vare maksimalt en time. På grunn av covid-19 pandemien så vil intervjuet foregå over Zoom/Hangouts/Teams videomøte og lydopptak ved hjelp av ekstern diktafon.

Jeg håper du har anledning til å være med i studien.

Om du kan delta eller har spørsmål til studien så kan jeg kontaktes på:

krisaka@stud.ntnu.no eller 906 08 426

Med vennlig hilsen Kristian A. Kastet

Appendix C

Confidentiality

C.1 Personvern og konfidensialitet

Innholdet fra samtaler blir håndtert konfidensielt og jeg vil ikke spørre om personopplysninger. Dersom det i løpet av samtalen skulle komme opplysninger om navn på bedrift eller lignende, vil dette bli anonymisert ved avskrift fra intervju. Alle data vil bli slettet så snart prosjektet er ferdigstilt i løpet av 2021. Det vil ikke under noen omstendighet være mulig å spore innhold i masteroppgave tilbake til deltagers identitet og bedrift. Innsamling av data følger retningslinjer gitt ved NTNU og Norsk Senter For Forskningsdata (NSD).

Med vennlig hilsen Kristian A. Kastet Prosjektansvarlig

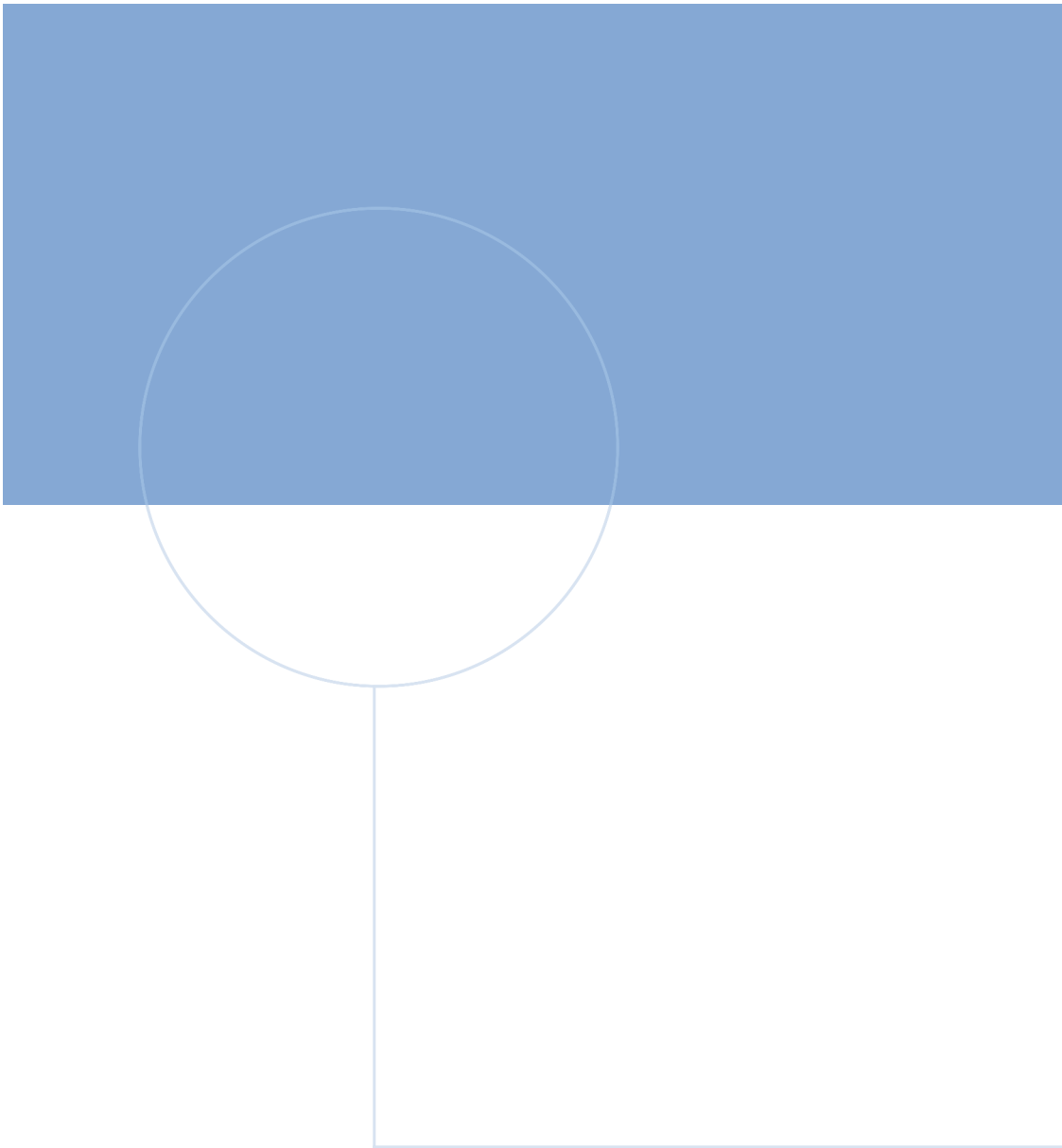
Samtykkeerklæring

Jeg har mottatt og forstått informasjonen om prosjektet, og har fått anledning til å stille spørsmål. Jeg samtykker til å

Å delta i intervju

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

(Signatur / dato prosjektdeltager)



NTNU

Norwegian University of
Science and Technology