Strategic measures to counter advanced network operations: Standardisation and automation of detection and warning

Tor E. K. Saltveit

Master’s Thesis
60 credits

Department of Informatics
Faculty of Mathematics and Natural Sciences

UNIVERSITY OF OSLO

May 2017
Strategic measures to counter advanced network operations:
Standardisation and automation of detection and warning

The aim of this thesis is to describe advanced computer network operations, investigate the present status of national defence efforts and suggest measures that may improve that status.

In the first part, the traits of advanced network operations are described. The strategic perspective is the focus, including the types of operations, the types of actors involved, targeting and possible gains, as well as intent behind the operations.

The thesis then describes cyber defence-related developments in Norway. This includes government initiatives, committees that have been appointed and offered advice on different components of strategy, and some of the national organisation around cyber defence, including some requirements both from the government and the private sector perspective for cyber defence to succeed.

Finally the thesis describes a framework for simplifying detection and warning of advanced network operations. The thesis hopes to offer inspiration towards further development of strategic solutions, as well as indicate areas of further research that could complement this work.
Acknowledgements

The project work surrounding this thesis has been made possible by the many generous people around me.

Firstly, I would like to thank my family for their patience with me. Cathrine has been particularly important to me, caring for our children and our household while I have been delving into network operations day and night.

Second, I would like to thank my colleagues in Telia, and previously in NSM, for their encouragement and facilitation.

Third, I would like to thank my advisor Audun for his pragmatic attitude towards my work and progress, for his weekend/holiday effort with revision, and for including me in work and research very relevant to the project.
Contents

1 Introduction ....................................................................................................................................... 2
  1.1 Computer network operations .................................................................................................... 2
  1.2 Statement of the problem ........................................................................................................... 2
  1.3 Research questions ..................................................................................................................... 3
  1.4 Research methods ....................................................................................................................... 3
    1.4.1 Systematic literature overview ............................................................................................ 3
    1.4.2 Case study ............................................................................................................................ 4
    1.4.3 Definition of a framework ................................................................................................... 5
    1.4.4 Walk-through test of the model............................................................................................ 5

2 Terminology – What exactly are network operations?...................................................................... 6
  2.1 Exploitation operations............................................................................................................... 6
  2.2 Offensive operations ................................................................................................................... 7
  2.3 Defensive operations .................................................................................................................. 8

3 CNA and CNE descriptions - The cyber kill chain ........................................................................... 9
  3.1 Signatures in the kill chain ....................................................................................................... 11
  3.2 State actors’ approach to managing the cyber kill chain .......................................................... 12
    3.2.1 Without repercussions, there is no incentive to stop.......................................................... 12

4 What makes cyber operations an attractive tool?............................................................................ 14
  4.1 First factor – Attribution complexity........................................................................................ 14
  4.2 Second factor – Low risk.......................................................................................................... 15
4.3 Third factor – Low cost ............................................................................................................ 15

4.4 Summary of the usability of cyber operations........................................................................... 16

5 Reverse-engineering the threat - Understanding intent based on advanced actor/state-sponsored targeting of CNOs .............................................................................................................................. 18

5.1 Targeting in espionage operations ............................................................................................ 18

5.2 Targeting in DDoS operations .................................................................................................. 19

5.3 Targeting in sabotage operations .............................................................................................. 19

5.4 Targeting in SCADA operations ............................................................................................... 20

5.5 Establishing intent and considering its operational value ........................................................ 21

5.6 What gains can be made from network operations? ................................................................. 21

5.6.1 Espionage ........................................................................................................................... 22

5.6.2 Sabotage ............................................................................................................................. 22

5.6.3 SCADA ................................................................................................................................... 24

6 Why are there no network operations to support military action? ........................................... 25

6.1 Only a limited amount of states actually possess the ability ................................................. 25

6.2 The gain is unpredictable ......................................................................................................... 25

6.3 Information infrastructure is vulnerable, but not that vulnerable ........................................ 26

6.4 Advanced operations like SCADA attacks require substantial resources .......................... 26

6.5 Research question A: What are the distinguishing traits of advanced computer network operations, when used as a strategic tool? .................................................................................................................. 27

7 State-level cyber defence evolution: Norway ............................................................................. 28

7.1 Cyber defence developments relevant to Norway ................................................................. 28
7.1.1 Coordination of efforts to prevent advanced network operations against Norwegian targets of national interest.................................................................28
7.1.2 Advanced network operations get the attention of the Norwegian government..............28
7.1.3 US focus on preventive measures to information security threats ..................................28
7.2 Norwegian focus on measures to increase national security on the cyber front ...............28
  7.2.1 The Lysne-report..............................................................................................................29
  7.2.2 The Traavik-report .........................................................................................................29
  7.2.3 Lysne II ..........................................................................................................................30
  7.2.4 What can be understood from the Norwegian Government initiatives ......................30
  7.2.5 Separation of cyber defence and intelligence collection .............................................32
  7.2.6 A sample case of national cyber incident handling in Norway......................................35
8 What conditions need to be fulfilled order for infrastructure owner companies to perform their part in national CND? ..............................................................................................................38
  8.1 State ownership of infrastructure and responsibilities .................................................38
    8.1.1 Business case and funding.........................................................................................38
    8.1.2 What threats should a company need to secure against? ........................................39
    8.1.3 Detection and warning..............................................................................................40
    8.1.4 Handling and restoration of services ........................................................................41
    8.1.5 Post-incident analysis ...............................................................................................43
  8.2 Company responsibilities .................................................................................................44
    8.2.1 Management .............................................................................................................44
    8.2.2 Roles and responsibilities .......................................................................................44
8.2.3 Governance and asset management ................................................................................... 45
8.2.4 Business benefits to pursuing a national security agenda .................................................. 46
8.2.5 A reluctance to implement effective security ..................................................................... 46
8.3 Detection and warning systems in cooperation with national security services .......... 48
9 The two basic categories of measures in cyber defence ................................................................. 49
  9.1.1 Preventive measures .......................................................................................................... 49
  9.1.2 Reactive measures ............................................................................................................. 49
10 Present state of national level detection and warning systems ................................................. 51
  10.1 Present model ......................................................................................................................... 51
  10.2 Stakeholders in CND .............................................................................................................. 52
  10.3 Research question B: What is the status in addressing shortcomings in the national defence
      effort against CNOs? ...................................................................................................................... 53
11 Strategic framework description ................................................................................................... 54
  11.1 Framework concept and purpose ............................................................................................ 54
  11.2 Attributes of the framework .................................................................................................... 54
    11.2.1 Synchronisation ............................................................................................................... 55
    11.2.2 Integrity ............................................................................................................................ 55
    11.2.3 Unity of effort .................................................................................................................. 55
    11.2.4 Prioritisation ..................................................................................................................... 56
    11.2.5 Excellence ........................................................................................................................ 56
    11.2.6 Prediction ......................................................................................................................... 56
    11.2.7 Agility .............................................................................................................................. 56
11.2.8 Collaboration ................................................................................................................... 56
11.2.9 Levels and critical factors in understanding a network operation ............................... 57
12 Basic elements of a CNO .............................................................................................................. 58
12.1 Actor ....................................................................................................................................... 58
12.1.1 Background ...................................................................................................................... 58
12.1.2 Categorisation .................................................................................................................. 59
12.2 Operation ................................................................................................................................ 62
12.2.1 Understanding the target .................................................................................................. 62
12.2.2 Defining the task .............................................................................................................. 65
12.3 The strategic intent ................................................................................................................. 66
12.3.1 Cause ................................................................................................................................ 66
12.3.2 Intensity ........................................................................................................................... 67
12.3.3 Highest ambition intent matrix ........................................................................................ 70
13 Revised model for cyber defence .............................................................................................. 72
13.1 Explanation of the revised model ........................................................................................... 72
13.1.1 Actor nomination ............................................................................................................. 72
13.1.2 Operation nomination ...................................................................................................... 73
13.1.3 Intent ................................................................................................................................ 73
13.1.4 Quality assurance ............................................................................................................. 74
13.2 Open research questions ......................................................................................................... 74
14 Summary and further work ......................................................................................................... 76
15 References ..................................................................................................................................... 79
“Today we have to address a new domain that we must secure to have peace and prosperity in the world of tomorrow.”

- Secretary of Defence Panetta on cybersecurity to the Business Executives for National Security in New York, 2012
1 Introduction

1.1 Computer network operations

The concept of cyber warfare started seeing popularisation in movies such as Stanley Kubrick’s “Dr Strangelove” from 1964, where the Doomsday device triggered the end of the world. Since then there has been a steady stream of fiction related to the concept, such as War Games and the Terminator-series of movies, as well as an entire category of literature. But only in recent years have the advanced, systematic and widespread uses of network operations started to manifest themselves and get noticed, even becoming apparent and prevalent. The artificial intelligence or autonomous decision-making to trigger the end of civilisation has taken a back seat to some other, simpler and more usable tools. Tailored to exploit weaknesses in information systems, these tools are designed for tasks like stealing information, creating bots or attack drones for a malicious network, or manipulating and sabotaging industrial control systems.

1.2 Statement of the problem

The defence of the information networks targeted by these attacks is a task that is increasing in both scope and complexity. Among the factors affecting this development are expanding networks, an increase in inter-connectivity and dependence between digital services, the fact that the targets are often situated outside of public infrastructure, and the continuing evolution of offensive computer network operations (CNOs). The timely understanding of, and response to, advanced network operations is therefore presently a significant challenge. This challenge is complicated further by the hesitance to share sensitive information. Many agencies tasked with computer network defence hesitate to share information they have about ongoing operations. Some reasons for this may be due to national classification and state secrets, the risk of compromise towards threat actors, or the risk of revealing vulnerabilities and targeting of a specific company targeted.

There is therefore a need for means to allow decision-makers at the national and strategic level to comprehend the nature of a computer network attack before the operation has completed its objectives, and before the intent behind the operation can be realised.

One key factor in simplifying this complex challenge, and simplifying the design of efficient systems for network defence, is to ensure a rapid common understanding of a CNO, as well as clear
1.3 Research questions

In the context of creating the necessary situational understanding to take timely action against an ongoing computer network operation:

A. What are the distinguishing traits of advanced computer network operations, when used as a strategic tool?
B. What is the status in addressing shortcomings in the national defence against CNOs?
C. How can a balance be reached between the need for confidentiality and the need for information sharing about cyber incidents?
D. In what way can the current national cyber defence model be improved regarding timely and sufficient information sharing?

1.4 Research methods

The main research method selected for this project is a systematic literature overview, case study of the cyber defence efforts by the Norwegian government, formulation of an improved framework for national level computer network detection and warning, and a structured hypothetical walk-through test of the method. Implementing the model in existing defence systems is for a number of reasons complicated and impractical within the bounds of this project, which is why a walk-through test is chosen.

1.4.1 Systematic literature overview

The necessary broad understanding of the topic is based on a systematic literature overview. Due to the high number of variables involved in strategic computer network operations, and the lack of a specific field of study that encompasses its entirety, literature must be chosen from several fields. The chosen literature not only demonstrates knowledge of the field, inspires ideas and helps define challenges – it also demonstrates an understanding of the dependencies between fields, the specific
relevance of the chosen items, and the complexity involved in addressing the challenges.

The process of working with the literature has had the following steps:

A. Having chosen a general topic, I have worked on identifying the different fields of study involved, from which literature would be needed to inform the topic. The fields include information security and in particular computer network operations, military strategy and operations, intelligence, national security administration, corporate security, public-private cooperation, national and international policy, conflict theory, standardisation and automation.

B. With the fields defined, my next step was to identify the relevant parts of each field to national level computer network defence. Whereas all these fields have impact on national solutions, part of the purpose is a simplification that allows increased efficiency and automation. To achieve this, it was important to understand theoretical aspects related to the intent behind and execution of state-sponsored network operations in conflict. It was necessary to examine some historic examples to illustrate the present scope of state-sponsored network operations, and thereby indicate which kind of operations are high value tools and which parts are more theoretical at this stage. It was helpful to illustrate important evolution in Norway’s strategic approach to cyber operations, and the different roles that must be managed to succeed in national computer network defence.

C. With this established, it was possible to define the basic conceptual elements of a framework for understanding, detecting and warning of network operations. It was also possible to identify some correlations or dependencies and an order of analysis that could simplify and enrich application of the framework.

1.4.2 Case study
To get an idea of the state of and importance placed on cyber defence at the state level, the evolution of cyber defence in Norway is presented. This will also highlight some strengths and weaknesses in the present defence model.
1.4.3 Definition of a framework

Following the literature review and case study, it is possible to formulate a hypothesis on an improved model. A framework depends on all the variables identified in the literature review. The essence of the framework should be to facilitate simplicity and automation.

1.4.4 Walk-through test of the model

With a framework defined, a sample case will be tested to demonstrate the value of the framework. The walk-through test will give an indication of the possible output from the framework. The chosen case will illustrate the main differences between the present model of national defence, and the possible improvement with a solution based off the framework. Although an implementation of the suggested framework would be a better indication of the value of the framework, that is not within the scope of this project.
2 Terminology – What exactly are network operations?

“The supreme art of war is to subdue the enemy without fighting.”

— Sun Tzu, The Art of War

According to the Joint Publications (JP), the doctrine framework for the US military forces and the basis for the NATO Allied Joint Publications, computer network operations (CNO) are one of five core capabilities defined under information operations. In the most recent revision the term has changed to cyber operations, but until this point CNO has been divided into three distinct areas:

Computer network attack (CNA),
Computer network exploitation or espionage (CNE) and
Computer network defence (CND).

These definitions appear to have been relabeled with the release of a classified JP 3-12 for cyber operations. However, the terms have seen widespread civilian use, are listed on Wikipedia and are likely to survive the revisions of the JP. They will serve as an overall categorisation of network operations for the purposes of this thesis.

Network operations attributed to the same actor, with the same intent, can be considered part of the same campaign.

A closed network has no direct physical or logical connection to outside networks. Such a system is dependent on air-gap’ing (physical data transfer via external storage such as CD’s, memory sticks or external harddisks) or through hardware that allows one-way communication in from lower security systems but with no ability to communicate back out.

2.1 Exploitation operations

An exploitation operation entails the compromise of computer systems with the purpose of extracting information, hence the common association with espionage. An exploitation operation
can develop into an attack operation. However, targeting is generally quite different in those two areas, and for that reason this is usually not practical. In fact, it may be possible to deduce the intent behind an operation based on the choice of targets. This will be discussed in greater detail later.

2.2 Offensive operations

“Information warfare operations concepts are new because of the increasing potential (or threat) to affect capacity and perception in the information and perception domains as well as the physical domain. These information operations are also new because these domains are vulnerable to attacks that do not require physical force alone.” (Waltz, 1998: p. 8).

An offensive operation entails disruption, denial, corruption and/or destruction of information, computer systems or the physical systems connected to them. These types of operations include, but are not limited to:

(Distributed) Denial of Service (DDoS/DoS). These attacks are the most apparent or visible, as well as the most common. They are also the types of attacks with the least damage potential. In its simplest form an individual can order a DoS attack through the Internet with a credit card. The attack involves a network of computers, which are often compromised private clients, make repeated requests to a server so that the server is unable to respond. The service, for instance through information on a webpage, is thereby inaccessible while the attack is in effect. The attack can be stopped by blocking traffic from the network that is sending an unusually high number of requests. DDoS is in a sense the CNA equivalent of repeatedly ringing a doorbell and running away – mostly disturbing and annoying, not that grave. However, this does depend on the service in question, and the denial of some services could potentially be life-threatening, such as emergency rescue treatment of critical patients, where specialists may need network access to registers and patient information.

Other types of denial of service attacks can be domain hijacking, DNS rerouting, DNS spoofing or BGP hijacking. Essentially an attacker masquerades as the domain under attack through various mechanisms. The result is that the visitors to the domain are, for a period of approximately a few hours to days or even longer, redirected to a domain controlled by the attacker. This allows the spread of misinformation, more advanced attacks or malware.
**Defacing.** The compromise of a website and a subsequent altering of the content, usually placing a visible political or ideological message.

**Sabotage.** The compromise of a system and a subsequent infection of malware which can alter or destroy information or hardware such that the system no longer is functional. Attacks on industrial control, or supervisory control and data acquisition systems (ICS or SCADA), are the most advanced types of sabotage. In these cases the compromised systems also have the potential to manipulate physical installations. Therefore the sabotage may result in damage beyond the information systems, for instance through the manipulation of traffic lights, air traffic control instruments, ship navigation, cooling systems for power plants etc.

### 2.3 Defensive operations

Defensive operations are primarily actions on one’s own systems.

**Passive measures** may include:
- Signature filters and rule-based access for incoming traffic, for instance through a firewall.
- Filtering of potentially harmful email attachments.
- Limited rights for the system users.
- Quick implementation of patches and security upgrades.
- Processes to detect anomalies in network traffic and processes running on the internal systems.
- Logging of traffic and data transported out of the system.

**Active measures** may include:
- Sinkholing, where the command chain to the intruder is cut and control over the malware is taken by the target system owner (or a third party).
- Honeypots or honeynets, where a false network is built to chart an actor’s movements and actions.
- Hack-back, where malware masked as data of interest is exfiltrated by the original attacker and ends up compromising the attacker’s system.
3 CNA and CNE descriptions - The cyber kill chain

Hutchins et al. (2011) have defined the “cyber kill chain” (p. 4-5), which is a useful standard for understanding the steps in a network operation. Exploitation and offensive operations are similar in execution up to the last step; therefore it is practical to view these phenomena as one. The idea behind the kill chain is that if one is able to disrupt the attack at any of these stages, the attack fails. By categorising and clearly defining each step, one can work methodically at reducing vulnerability and understanding risk. For instance, while prioritising and building detection capabilities, it would be advisable to make sure one’s system has the ability to detect an attack at any stage of the logical path all compromises follow.

The simplest types of network attacks, like denial of service and many types of defacing, do not require a compromise of the target (although it may require the compromise of the business hosting the target’s website). Therefore there is little warning ahead of these sorts of attacks. But the more advanced types of attacks require a client compromise of some sort. The cyber kill chain for such an attack is defined as follows:

1. **Reconnaissance** - identify the target of the operation. For state actors, this may for instance involve agent activity by participating in conferences or pursuing persons of particular interest, or it may be as simple as researching websites, exploring resource people through social media or mailing lists. Also, it may include scans of target systems.

2. **Weaponisation** - prepare malware for delivery to the target. A typical way of doing this is to combine malware to a document or a computer file that the user considers harmless. Such files may be of very general interest, like random nature images. Low priority operations like those are generally easy to identify and avoid. However, advanced intelligence based operations may for instance exploit minutes from meetings the target recently has attended. The emails may also come from people the target knows, and appear very genuine. These types of social engineering are a lot more demanding to identify.

3. **Delivery** - transmission of the weapon to the targeted environment. Some typical methods for delivery are:

   - Phishing (large target group) or spearphishing (explicitly targeted) - which entails an email with a file attachment or a link to a website containing malware. Simple phishing can originate from a wide variety of criminal actors, whereas spearphishing can be a product of good intelligence and
appear to originate from co-workers or leaders in the target’s own company. Spearphishing will also typically contain very relevant and current information for the specific target.

- Watering hole attacks - the compromise of a website the attacker knows or suspects the target will visit. By knowing details about the target (like their IP-address) it is possible to be selective about who to serve malware and who simply gets a normal experience from visiting the site. In this manner, the attacker is able to reduce the likelihood of detection.

- External storage devices, like USB memory sticks, CDs with autorun etc.

- Human agents - manipulating people with the ability to give physical access to a system.

4. Exploitation - activation of the exploit malware. This usually involves taking advantage of vulnerabilities in operating systems or applications, or by tricking the system user to allow rights to more functionality than he intended. In practice this involves running programs, opening documents, following website links or simply visiting infected websites. Generally exploitation is more or less a given development if the earlier social engineering or manipulation was a success, and assuming the reconnaissance efforts gave accurate results. Some pitfalls may be different version numbers of applications than predicted, a different or newer OS, or even an older OS in some cases.

5. Installation – command & control malware is downloaded, installed and hides on a system, often in a way that makes it persistent and lets it survive a reboot or attempts to remove it. From this stage on, the user has been tricked and the exploitation phase is over. At this point it is more about avoiding technical detection systems of various sorts. Proficient state actors will have mechanisms to reduce the chance of discovery, as well as to retain persistence even beyond discovery.

6. Command and Control - communication from the infected system to the threat actor. Once communication is in place, it is possible for the actor to navigate the compromised network. In closed networks command and control has to be maintained through messages exfiltrated and infiltrated via air-gap’ing, for instance with removable storage devices like USB memory sticks.

7. Action - pursuing the actual intent of the infiltration. This could be exfiltrating data, further movement within the network, or sabotage. It is only at this stage that one can verify the purpose of the operation. State actors generally put some effort into reducing the likelihood that they leave a digital trace straight home. One way to avoid this is for instance to send data along a cable or other carrier where the actor also has signal intelligence coverage. Following the digital trace, it will
appear as if the data is sent down a dead-end or to a third party.

3.1 Signatures in the kill chain

Both espionage and advanced offensive operations require a compromise of the target as described in the seven steps described above. Even though it can be argued that basic signal intelligence could intercept transmissions and achieve the same goals as a CNE operation, the fact is that “Strong cryptography cannot be cracked even with the most powerful computers of today (sterk kryptografi vil de ikke klare å knekke selv med dagens aller kraftigste maskiner)” (Raddum, 2014). This forces the actors to conduct endpoint system compromise instead. This activity omits a signature. As described in the cyber kill chain, it is possible to detect an advanced operation in many phases.

In some cases it is possible to detect an advanced operation as early as in the reconnaissance stage, in the sense that this activity may include active contact with the target or browsing of target websites. The address of the system used for recon can reveal its association with earlier attack attempts.

When the malware is being delivered, it is certainly possible to detect an email with a request to click on a link or open a document. There may be advanced social engineering involved in this stage, but regardless it is usually possible to implement mechanisms to control the origin and authenticity of an email request of that kind. For instance, one can telephone the author of the email. If the author denies having sent the email, it is generally safe to treat it as a compromise attempt. Watering holes can be trickier to detect, as the mere browsing of a site can result in a compromise, and there is no preceding indication of a manipulation attempt.

Exploitation and installation are steps where a thorough system process analysis may show the signature of malware being activated. Blacklists and whitelists for executables are examples of measures that may help in that regard.

Once the operation gets to the command and control phase, it is generally easier to detect, as this requires exchanges with an outside communications node. Network traffic can be filtered for malicious domains and addresses.

While the malware is conducting its actions on the target system, one can potentially detect both movement within the system, the activation of new processes, as well as communication out and
exfiltration of data.

3.2 State actors’ approach to managing the cyber kill chain

State actors in particular generally make a fairly significant effort to reduce the likelihood of being detected in all these stages. Using the APT1 as an example, which was attributed by Mandiant to the 3rd General Staff Department of the Chinese People’s Liberation Army, their modus operandi included sophisticated social engineering such as manually assessing and responding to verification emails. “Email recipients have replied to the spear phishing messages, believing they were communicating with their acquaintances. In one case a person replied, “I’m not sure if this is legit, so I didn’t open it.” Within 20 minutes, someone in APT1 responded with a terse email back: ‘It’s legit.’” (Mandiant 2013, p. 29).

Technically as well, “the vast majority of the time they use what appear to be their own custom backdoors” (Mandiant 2013, p. 30), which makes detection significantly harder as no antivirus-product will have signatures from known cases of exploitation attempts.

However, custom development is not always the case. “APT1 intruders occasionally use publicly available backdoors such as Poison Ivy and Gh0st RAT” (Mandiant 2013, p. 30). Similar observations can be made for other CNE campaigns. Hence, one can deduce that while state actors do have the capability to develop and deliver advanced malware with very low likelihood of detection, they also use commonly known and easily detectable tools.

3.2.1 Without repercussions, there is no incentive to stop

“The international nature of the net simply makes it impossible to enforce the laws of every country individually” (Rigby, 1995).

The political consequences from the APT1 discovery was a direct address from the US government to the Chinese, but little more than that. As a result, the Chinese “expanded the scope of its cyber espionage despite the greater public scrutiny these operations received in 2013” (Keck, 2014). As Keck mentions, Snowden’s revelations of the US government’s own CNE programs (Greenwald, 2013) did hamper US efforts to some extent. But the dispute ended as claims in open media
between the two governments where China pointed to the fact that although there may be network infrastructure in China that facilitates CNE operations against the US, that does not mean that the Chinese government is involved. Outside of the very small IT security or counter-intelligence realm, it is difficult to understand the nuances and validity of the various claims. It is also near impossible to tie the actual operations to the decision-maker behind them. This holds true for other campaigns than the Chinese as well: “There is no conclusive evidence that either set of attacks [on Estonia and Georgia] was executed or sanctioned by the Russian government—though there is no evidence that it tried to stop them, either.” (Economist, 2008). Consequently, it is very difficult for any state to justify the same kinds of punitive measures as if a Chinese citizen had been apprehended while attempting to break into the Pentagon during night hours. With the consequences limited to diplomacy-level rhetoric, the espionage continues - as the rewards are significant. This also explains the varying degree of operational security displayed in state-sponsored CNE operations: although they would prefer to avoid detection, it appears that some states expect to be discovered. As long as the threat actors can maintain plausible deniability by contesting the attribution value of technical findings, it may to some be worth risking detection. “All sorts of ‘translation problems’ arise when trying to apply existing international rules relating to terrorism and warfare to online attacks” (Economist, 2008). From the actor’s perspective, the necessary security measures to avoid attribution towards themselves altogether would cost more than the rewards gained from simply collecting broadly.
4 What makes cyber operations an attractive tool?

In general, the challenges presented by advanced network operations have manifested themselves in many forms. The Stuxnet (Kelley, 2013) and Black Energy (Lipovsky and Cherepanov, 2016) attacks on critical infrastructure are examples of some of the more concerning manifestations for a nation state. They are an indication of what a motivated and well-funded actor may be capable of achieving when attacking critical infrastructure, in those cases hindering a nuclear program and shutting down power to a region of a city. Such an attack does not represent a new scale of damage in war. In fact, no cyber-attack to date has been used in close coordination with conventional armed forces, particularly not in the sense that conventional forces have been dependant on the effects of a cyber-attack. The reason seems fairly clear – the results of a cyber-attack are less predictable in effect and in timing than conventional vectors of attack. So, what use do state actors have of advanced network operations, if the precision is lower than the existing weapons in the toolbox?

4.1 First factor – Attribution complexity

The first obvious factor is the complexity surrounding attribution. In the more analogue world of terror, espionage and state sponsored sabotage, three-letter intelligence and security agencies typically keep their cards tight to their chest. In contrast to this, the discussions in information security forums and intelligence communities around actors, indicators and evidence are remarkably open and detailed compared to what is traditional in intelligence and national security work. Even so, attribution to an actor is often circumstantial more than concrete, and the understanding of the exact intent is often general more than specific. From the perspective of international affairs, foreign policy, security policy, international cooperation and alliances, cyber attribution has to date not legitimized or resulted in potent sanctions.

Actor attribution typically boils down to technical indicators of compromise, the use of methodology or specific toolkits, or traffic towards network infrastructure associated with previous similarly ambiguous operations. More specific attribution has been used, such as the 2013 APT1 report by Mandiant, where individual Chinese citizens were associated with systematic network operations towards targets in the US. Even in that case, their association with a Chinese state agency was only circumstantial. This association did result in legal action from the US (Henderson, 2014) but as the author of the article comments – “It's clear that these arrest warrants are largely
symbolic”.

If this act from the US Attorney General was an indication of a desire for change of policy in the US, and that the ambiguous attribution of advanced network operations was going to lead to much more clear action from the parties subject to these operations, that effort was made much more challenging by the Snowden leaks later the same year as APT1 got the cyber security communities’ attention (Szoldra, 2016). The leaks became a reminder that however illegal, unfair and unethical one might want to consider hacking, cyber-crime, and advanced network operations against industry targets, the fact is that in intelligence and security matters, every state has their own interests first in mind. And in the espionage game, the US are undoubtedly the best in their league. Armed with evidence of this, China suddenly had a plausible story of being the real victim (Phillips, 2013).

4.2 Second factor – Low risk

In traditional espionage and intelligence work, agents need to be selected, trained and placed in the target country. As far as state security goes, few threats are regarded as potent as foreign state agents, and few crimes are punished as severely. Traditionally most states have had the death penalty as a possible consequence to treason and espionage, and some still do to this day.

The vast majority of state sponsored network operations are conducted by engineers from their state capital or a large city region, where there is no risk of prosecution from a foreign state. The possibility of identifying specific involvement of individuals, such as was revealed in the APT1 case, requires lax security in the first place from the operators. Even in that case, pursuing the individuals with association to state agencies is very challenging. The individuals could be arrested if they travelled outside of their own country, or they could be targeted by covert operations in their home country, but the escalation in method, the impact of such an operation and even the risk involved in such a covert operation would hardly be justified in any perspective. The risk of advanced network operations agents being compromised, arrested or otherwise targeted is significantly lower than if they were operating in the target country.

4.3 Third factor – Low cost
There are several aspects of the cost factor. Firstly survival, which is closely related to risk. As there is little need to train agents for survival and clandestine operations in every aspect of their life, they are free to focus solely on their specific network operation task.

Second, there is the operational environment. In a conventional operation, agents would need to traverse some physical space to reach their target. Typically this would include the infiltration of illegals or secret agents into a different country, staying undetected and without arousing suspicion, obtaining access to a guarded site, breaching an information system or a secure storage area, and an equivalent exfiltration. Exfiltrations are often more challenging than infiltrations, as there is the added risk of detection of the completed operation, not only the movement itself.

Third, there is logistics. This would include the storage and transportation of tools, plans, vehicles, communication equipment, possibly weapons, and certainly funds. In the good old days of traditional espionage, agents would exfiltrate a briefcase of documents at a time, and exchange that briefcase for cash in a neutral country café. With advanced network operations, one single extraction of documents, as part of a single operation towards a solitary target, can contain information equivalent to tens of truckloads of paper documents. In one ftp operation modern spies can approach the equivalent quantity to what an entire agency could collect in a year of analogue work (although most likely not with the same precision, diversity or value). One fascinating aspect of advanced network operations is the amount of resources that need to be dedicated to analysis, to make this collection practical and worthwhile. But as costly as that may be for many states, it is certainly orders of magnitudes cheaper than if the collection was conducted through traditional methods.

4.4 Summary of the usability of cyber operations

In sum, advanced network operations present a budget tool that is low risk and hard to pinpoint to an origin. For espionage purposes one can hardly imagine a modern state without resources dedicated to the task. For sabotage or offensive purposes cyber operations are still not a game-changer equivalent to aircraft in the 30s or nuclear weapons in the 50s, but the versatility still makes it attractive for any state that wants to complement its toolkit for escalation of conflict and making political statements. When considering that offensive operations only differ from espionage operations in the late stages, a lot of the same competence applies to both types – as a state ramps
up their cyber espionage, they gain offensive cyber capabilities simultaneously. A relevant question in this regard is whether increased standardisation in the world’s IT platforms will result mostly in higher overall security, or instead more widespread exploitation of vulnerabilities.
5 Reverse-engineering the threat - Understanding intent based on advanced actor/state-sponsored targeting of CNOs

“Cyberwarfare can strike civilian targets with equal, if not greater, ease that it can political ones” (Wang, 2012).

“Attributing attacks to specific perpetrators is often difficult in cyberspace, where identities can be easily disguised. Consequently, if the attacker is misidentified, there is a great risk of harming innocent individuals or targeting the wrong place” (Kostadinov, 2013).

When considering intent, the first question to answer is who is behind the operation. But attribution is somewhat more straight-forward in the case of conventional military capabilities with a physical presence and signature. In those cases, it is possible to identify and monitor base activity, alert levels, physical movement or relocation of hardware or troops. In cyberspace this is not the case, and much more guesswork may result. “The plethora of competing theories [is known] as ‘the fog of cyberwar’” (Economist, 2008). Due to the complexity of technical attribution with a high level of confidence, targeting can be the best tool to deduce intent in some cases. Targeting is different in espionage and in attack operations, and it is to some extent possible to understand the intent behind CNO based on targeting.

5.1 Targeting in espionage operations

Starting with campaigns that only have shown espionage (or information exfiltration) behaviour, one can look at Red October (Kaspersky 2013a), TeamSpy (Kaspersky 2013b), APT1 (Mandiant 2013), or the NSA revelations (Greenwald 2013). These campaigns have a few common traits.

- The targets contain information that is relevant and interesting to strategic level decision-makers, like foreign policy, advanced technology, research projects and business intelligence.

- The targets have low or no consequences from being shut down or incapacitated for a period of time, beyond inconvenience, neither to the public nor the government.
- In the cases where the targets themselves are potential sabotage targets, like a nuclear plant, the control systems have not been infiltrated.

5.2 Targeting in DDoS operations

Looking at known DDoS operations, where systems have not been compromised or damaged on any large scale, there are examples like the attacks on Estonia in 2007 (Wang, 2012), Georgia in 2008 (Economist, 2008), Japan in 2012 (Suri, 2012) and the US finance sector (Whittaker, 2013). “[Several Japanese websites are] victims of DDoS attacks, and include some really important sites like banking, power utility, and other private sector companies” (Suri 2012). These campaigns also have some common traits.

- The targets are not simultaneously compromised with malware.
- The targets and the downtime of the targets are very visible to the public.
- Downtime translates almost directly to the government losing prestige.
- The targets have little or no military value, and the downtime would not affect or compliment conventional military operations.

5.3 Targeting in sabotage operations

There have been a few examples of large scale sabotage operations. North Korea attacked South Korean networks during the spring of 2013 (USA Today, 2013). Saudi Arabia’s oil and gas sector was attacked by an advanced actor, likely Iran (Bronk, 2013). And Ukraine has seen some CNA activity during its recent conflict with Russia (Bumgarner, 2014), including a BGP hijacking of a Ukrainian news agency. There are a few common factors or interest in these cases:

- The targets have low intelligence value.
- The targets and the downtime are very visible to the public, or affects public services.
- Downtime translates almost directly to the government losing prestige. In the case of Saudi
Arabia, downtime also equals significant financial cost.

- The targets have little or no military value, and the downtime would not affect or compliment conventional operations substantially.

5.4 Targeting in SCADA operations

The known SCADA operations of large significance are firstly the Stuxnet attack on Iran’s nuclear program (Kelley, 2013), and two similar-looking power plant attacks towards Ukraine (Condliffe, 2016).

What is the difference between sabotage and SCADA-system attacks? Technically the latter is a subset of the former. However, there is a difference in complexity when the sabotage implies the custom design of a plan and software or firmware to address a specific control system beyond the initial information system and network breach. Stuxnet clearly distinguishes itself from everything else in this regard. The Fancy Bear attacks against Ukraine are somewhat less sophisticated in the sense that they mainly took over legitimate access credentials and manually shut down power substations, but in doing so they also did create and infiltrate custom firmware and blocked out operators from correcting the changes. One could call it a hybrid, or a “poor man’s Stuxnet” – but compared to any other network operation it is still head and shoulders above everything else.

The Stuxnet operation was highly complex and consisted of several independent operations to reach its final objective. In this case, the ultimate target was a control system for the refinement of weapon-grade Uranium. There is little doubt about the target and basic intent of the malware, which was to sabotage Iran’s nuclear program. Although this target also has an espionage value in its own right, the most significant effect an adversary could gain from that information would be to prepare an attack on the system itself. In that sense one could consider the preceding espionage operation part of the reconnaissance effort for the attack.

However, there is another aspect to this operation. Although there is little doubt what the malware was built and deployed to do, there is some doubt as to what the intent of the operation was. Some speculate that this CNA had little actual effect, seeing as Iran may have intensified its nuclear weapons development efforts after the attack. But on the other hand, the actor behind the attack (some sources claim the US, Israel or both) was able to discredit the Iranian government, maybe
soothe the most impatient interest groups or lobbyists in the US or Israel, and demonstrate a potent response without risking the lives of soldiers or even taking any Iranian lives. This is a unique trait of network attack operations.

The Ukraine power grid attacks also have indications of long-term planning, detailed logistics, a very well thought-through strategy and custom-made malware and firmware. Although the resources invested in these operations were most likely significantly less than the Stuxnet operation, the impact is still substantial, and in that sense one could say that the Fancy Bear-attacks were more cost-efficient. This development could be a first indication of how SCADA-system attacks will manifest themselves at the next lower tier of cyber actors: the countries one step down from the US.

5.5 Establishing intent and considering its operational value

Based on the types of operations mentioned above, it is possible to conduct a basic value assessment on a target with respect to espionage and sabotage (and possibly control systems manipulation). Current empirical evidence suggests that the target’s highest value strongly indicates the intent behind the operation. If the target system is an information repository, generally the operation is intended as espionage, whereas if the target system has large public use, is visible and its uptime affects government prestige, it is an attractive target for sabotage or SCADA-system attacks.

This logic has other applications than post-incident analysis. Applying this logic to preventive measures, it is a relatively simple task to place sectors and specific areas of industry and government into one category or the other. Once that is done, one can deduce that any given target will be at high risk for espionage and low risk for sabotage, or vice versa. This also means that political tension between two states, where sabotage may become a more relevant political tool, places sabotage targets at greater risk. All this sort of analysis can give guidance to Computer Emergency Response Team (CERT) readiness, system administrator vigilance, restrictions in user privilege levels in companies that are particularly attractive targets, etc.

5.6 What gains can be made from network operations?
5.6.1 Espionage

Clearly the greatest gain states have from network operations today is espionage. There is low risk, in the sense that the actor does not have to be present in the country or business that he is spying on. There is enough ambiguity in attribution to where espionage accusations are deniable in the eyes of the layman world, and the knowledge gain is unprecedented.

Traditionally, espionage has always been considered a national high priority activity. Even under circumstances where months or years of risky, international agent handling is necessary to exfiltrate a few briefcases of documents, this has been true. CNE operations make it possible to exfiltrate information equivalent to tens of shipping containers filled with documents in a single extraction, in an operation against a single target. No longer is the limit in what quantities of information one can acquire, but rather what sort of logistics exist to manage all the information obtained. The Internet has provided a golden cyber-age of espionage.

Espionage is an international gentleman’s sport that very few states seems to have any real objections to, and where almost all states play a part themselves. It is only recently that the US have tried to object to China’s levels of espionage as “un-gentleman-like”, particularly seeing as most of their targeting is for research and economic rather than a security gain. The US themselves have received criticism for blurring the line between necessary espionage activity to secure their own state, and unnecessary collection of personal information that results in an invasion of privacy.

The magnitude of information that can be collected and the knowledge that can be gained through CNE is so substantial that it can be a significant factor in supporting research programs and closing a complete technology gap between two countries.

5.6.2 Sabotage

“[The use of cyberattacks] is a political tool…It has become a proven political weapon as a way of intimidating your enemy” (Wang, 2012).

5.6.2.1 Intimidation

The empirical evidence suggests two basic uses of computer network attack operations. First there is the intimidation of another state. Mostly this is effective when a large state like Russia or China attack a much smaller state which basically does not have the resources to defend itself adequately.
“The actual damage done was minimal” (Economist, 2008) in Russia’s CNA towards Georgia, which makes it easier to avoid any international repercussions - while the threat of something more substantial always looms overhead. This strategy places the smaller state, like Estonia or Georgia, in a position where they have to evaluate whether their political opposition to Russia is worth the continued denial of service or worse. One thing is the systems that are affected; another thing altogether is the promise of what may follow if they continue to be disobedient. “Offensive operational capabilities require the capability to identify and specify the targets of attack (targeting) and then to attack those targets. [...] In addition to these two, a third offensive capability is required at the highest (perceptual) level of the operational model: the ability to manage the perceptions of all parties in the conflict to achieve the desired end.” Walts, 1998: p. 162). With offensive network operations, a state has demonstrated their willingness to follow threats with actions.

5.6.2.2 Psychological operation against one’s own population

The other basic use of CNA seems to be as a psychological operation mostly against one’s own population. “The virus caused significant disruption to the world’s largest oil producer” (Bronk, 2013). Although one can argue that Iran was able to inflict damage to a significant competitor to their own national industry in their Aramco attack, or even that they intimidated Saudi-Arabia or the US, there was probably at least as high an effect on their own population. Considering the fact that Iran had recently been the victim of Stuxnet themselves, they were in a position where they needed to regain some authority in the eyes of their own population. Also, one could see that even as damaging and serious an attack that Stuxnet was, and even though Iran and other countries pointed out suspect nations behind the attack, there were no consequences or any repercussions from the United Nations or any other large international body. Not only would this leave Iran needing to make a point of their own to not lose face internally, but it would also encourage them to use a similar type of consequence-free network attack themselves. From that perspective, it is possible to view these attacks as multi-purposed but certainly with a large and maybe even primary objective of settling internal unrest. “Despite its vast resources as Saudi Arabia’s national oil and gas firm, Aramco, according to reports, took almost two weeks to recover from the damage” (Bronk, 2013). The psychological value of being able to inflict this kind of a blow to a large business with substantial resources is significant.

North Korea was in a similar position before the waves of CNA against South Korea. Although
North Korea historically are willing to take substantial risk, including the actual shelling of South Korean inhabited areas and the sinking of military vessels, these types of actions cannot be used indiscriminately. Combined with intense warlike rhetoric and the test launching of missiles potentially equipped with nuclear, biological or chemical warheads, there is a very real risk of a response from the neighbouring countries or the US. Against a backdrop like this, it is very convenient to use political tools that pose a low risk and that it is difficult to attribute precisely. “Does any of this [CNA] really count as an act of war?” (Economist, 2008). And so the destruction of IT systems that have a very visible effect on South Korea’s population is an excellent way of demonstrating a new, potent capability to their own people. Although the attack “shut down tens of thousands of computers at South Korean broadcasters and banks” (USA Today, 2013), whether or not it changed the military manoeuvre plans of the US and South Korea, or whether it intimidated South Korea to make more concessions towards North Korea, is not as apparent.

5.6.3 SCADA

Industrial control system attacks are the types of attacks that have the highest damage potential, and for some states it is an available tool. Empirical evidence in the cases of Stuxnet and Black Energy shows limited damage compared to the resources invested, but one could also argue the main priorities in those cases were either remaining undetected in the case of Stuxnet, and making a political statement in the case of Black Energy. Had the main intent exclusively been damage, those scenarios may have looked slightly different.

Generally one should regard a modern information and ICS system as more secure than an older one. However, the combination of old and new technologies and vulnerabilities, as well as the complexity of existing ICS solutions, will in many cases provide an additional barrier for attackers. Standardisation of and uniformity in information system could in the future also allow for systematic, broad-sweeping vulnerability exploits. Today, it is much more a case of tailoring an attack to one specific platform, which limits the reusability of the work done to prepare the attack. As systems become more standardised and modularised, one might therefore expect to see broader use of ICS attacks.
6 Why are there no network operations to support military action?

“For a cyberattack to qualify as “cyberwar”, some observers argue, it must take place alongside actual military operations” (Economist, 2008).

“When Russian forces invaded Crimea they didn’t blind the Ukrainian government with massive cyber attacks. Such attacks were not launched, because the strategic and operational environments in Ukraine and Crimea were much different from those in Georgia” (Bumgarner, 2014).

There have been several conflicts where one might expect CNO in support of conventional military operations, or simply to achieve military objectives. Libya and Syria are examples of conflicts where several world powers have had interests. Georgia and later Ukraine are examples where Russia in particular have had interests. North and South Korea have long had high tension between them, with several bloody exchanges, as have India and Pakistan, and Israel versus several other neighbouring countries. Yet there have not been any CNA operations which would qualify as complementary to conventional military operations, or of a scale where they could achieve military objectives by themselves. There are a few factors that may contribute to explain this.

6.1 Only a limited amount of states actually possess the ability

Different states’ cyber capabilities are closely guarded secrets. All the same, this type of capability is probably limited in its proliferation. It requires substantial effort to develop a weapon from network operations. Although many states have demonstrated an ability to exploit networks for espionage purposes, it is a somewhat different endeavour to inflict physical damage or to modify information in such a way that it qualifies as a weapon.

6.2 The gain is unpredictable

Even in the cases where states have efficient CNA weapons, it is unclear exactly what result a CNA operation might have. Predicting the target nation response, the total system damage and what
compensating means may exist, is bound to be either a significant intelligence challenge or
guesswork. An unpredictable operation is an operation of low military value. Lessons learned from
Stuxnet and Black Energy may reduce the uncertainty, which means that the likelihood of such
support to conventional attacks may increase in the future.

6.3 Information infrastructure is vulnerable, but not that vulnerable

Generally, it is reasonable to assume that advanced state actors are able to compromise most
unclassified information systems in any other state. But even in the case where they are able to
compromise and cause damage to a system, the scope of the damage is still relatively limited. One
may be able to shut down a few systems for a short period, but once a state mobilises its resources
to defend against the threat, it is only a matter of time before the CND efforts will start to pay off.
This means that even in the best case, CNA can result in little more than a temporary disruption to a
small amount of information systems, and the malware is likely limited in its ability to quickly
proliferate.

6.4 Advanced operations like SCADA attacks require substantial resources

“Cyber Command has matured into what I believe is a world-class organization. It has the capacity
to conduct a full range of missions inside cyberspace” (Panetta, 2012).

The ultimate worry is a SCADA attack on a nation’s critical infrastructure as a part of a military
campaign, like an invasion. Although Israel has been accused of shutting down Syrian radars with
network operations at one point (Page, 2007), it is unclear what truth there is to these claims, and
regardless it is a relatively limited incident that has not seen much repeated use. And the reason is
most likely as simple as the fact that SCADA attacks take a significant amount of time and
resources to plan and execute. For a state, those same resources could be spent on simply attacking
the target with other more conventional means. SCADA operations may be more attractive to an
actor who does not have the other conventional strike or sabotage options that a state does, like for
instance a terrorist. “Given that the next attackers may not be nation-states, civilian critical infrastructure becomes a troubling potential target” (Kelley, 2013).

6.5 Research question A: What are the distinguishing traits of advanced computer network operations, when used as a strategic tool?

The preceding chapters answer the first research question regarding the distinguishing traits of advanced computer network operations. The versatility, attribution difficulty, low risk and low cost makes it useful in nearly every stage of conflict between states. The targeting indicates that there is systematic exploitation of opportunities from a number of states, and although the usefulness of network operations in support of conventional operations is dubious, there are plenty of other areas where the gain is very apparent. As a tool of security policy, the likelihood of network operations being used increases when the above listed factors come into play or are of importance, and the future may bring even more widespread use of the most advanced operations as well.
7 State-level cyber defence evolution: Norway

7.1 Cyber defence developments relevant to Norway

7.1.1 Coordination of efforts to prevent advanced network operations against Norwegian targets of national interest

In 2006, NorCERT was established as part of the Norwegian government’s awareness of the increasing cyber threat (Norwegian Ministry of Defence, 2004). NorCERT, or Norwegian Computer Emergency Response Team, was tasked with coordinating work relating to the national defence against advanced network operations. Part of this initiative was the continued development of the national warning and detection system, Varslingssystem for digital infrastruktur (VDI).

7.1.2 Advanced network operations get the attention of the Norwegian government

By 2009, NorCERT was reporting a concerning development in the use of network operations (Asvall and Johansen, 2009). The focus of the message – careless USB stick risk – may not have been coincidental. In 2008 the USB-based agent.btz had been in the wild for a year (Finkle, 2014). The spyware started as an attack on Pentagon’s closed military networks in 2008, and spread to many countries in Europe by 2011 – including Norway. This was historic in the sense that it was the first known large-scale espionage operation with clear fingerprints of an advanced actor such as a state affiliated intelligence agency, and the hypothetical scenarios discussed in national security context until then, suddenly became very real.

7.1.3 US focus on preventive measures to information security threats

Internationally, the US House of Representatives passed a cyber security bill in 2012 (Kain, 2012). Although this bill eventually was stopped in the Senate, before it was revised and passed in 2015, it showed the level of attention the US Government had started paying to effective cyber defence.

7.2 Norwegian focus on measures to increase national security on
the cyber front

7.2.1 The Lysne-report

By 2014 the focus from the US, the world’s leading cyber authority, as well as increasing concerns from Norwegian national intelligence and security services, resulted in a Norwegian mapping of national vulnerabilities to cyber threats (Norwegian Ministry of Justice, 2014). The Lysne-report (Norwegian Ministry of Justice, 2015) describes, among many other topics, some weaknesses in the VDI-system as the primary national cyber defence detection mechanism. Similarly, the coordination between other prominent CERT and CSIRT organisations at the national level still had development potential in its support of efficient defence. Existing crisis management institutions such as police and armed forces had limited ability to manage a cyber crisis. Even a conventional attack, instigated by a single individual, Anders Behring Breivik, had only a few years earlier shown to present a significant challenge to national crisis management. The responsibility for managing a cyber crisis had been placed within the National Security Authority (NSM), which has no other operational or crisis management function within the Norwegian government. As a cyber crisis is likely to have other areas of effect than just networks, and may start as something completely different, these distributed responsibilities were described as potentially creating confusion right at the time when clarity is of the essence. Almost in parallel with these conclusions, the National Security Authority itself was asked to deliver its recommendations on how Norway should ensure national security in the period up to 2020. The government’s desire to orient itself in this complex matter was apparent.

7.2.2 The Traavik-report

In March 2015, even before the Lysne-report was completed in November 2015, the Norwegian government appointed another committee to investigate national cyber security matters. The Traavik-committee was tasked with suggesting new legislation to secure national interests and prevent the exploitation of vulnerabilities in critical infrastructure. In October 2016 the recommendations were ready (Norwegian Ministry of Defence, 2016a). Among other recommendations, the report suggested legislation needed to be more specific to be able to counter current threats. It suggested that Norwegian authorities had a more active advisory role towards owners of critical infrastructure, so as to enable them to assist in the defence of national values. It further suggested, quite significantly, that all information systems of critical importance to fundamental national functions, should be subject to protection through security legislation, and that
the foreign investment in national infrastructure should be regulated or even prevented. Terms such as “more comprehensive management of all national security” were used to describe the intent of the suggested changes.

### 7.2.3 Lysne II

In February 2016, the Norwegian Ministry of Defence appointed yet another committee lead by professor Olav Lysne (Norwegian Ministry of Defence, 2016b). Its task was to assess the need for a “digital border defence” (DBD) and consider the implications of such an initiative, particularly with regard to the invasion of privacy of Norwegian nationals.

By August the committee had concluded that a DBD was recommendable and could be seen as necessary in a democratic society, although the risk of unintentional violations of privacy and basic human rights is high and dependant on vigilant and competent control functions.

One caveat for the recommendation was that a DBD would offer “sufficient intelligence value”.

### 7.2.4 What can be understood from the Norwegian Government initiatives

The Norwegian Government’s increasing interest in cyber security is evident. At the same time, some confusion around effective measures to counter cyber threats also seems apparent. This is perhaps not so surprising. To the technically uninitiated, the complexity of advanced network operations makes them intangible. Adding to this, computer network defence specialists typically focus more on the detailed descriptions of the technicalities in the operations than the necessary prerequisites for them and the likely intent behind them. Ironically this focus, and the abundant reporting of it, offers more to the attacker than to decision-makers in the defending countries, as the actors are able to understand how they were detected and how to avoid that same mistake in the future.

All the same, this confusion and lack of direction represents a significant challenge in the development of effective computer network defence. The government reports advising on the strategy surrounding CND, avoids specifics regarding what to achieve, who should be achieving it,
and how (as those questions were not part of the order). On the topic of how to improve national cyber security, Norway appears to be without clear strategic foundation.

### 7.2.4.1 Who is responsible for advice in cyber defence matters?

In a national crisis, the Ministry of Justice is responsible for coordination and leadership. In a state of war, the Ministry of Defence and the Armed Forces take over that role. So inherently there is some confusion as to who does what in a crisis, depending on whether you should consider it an act of war or not.

In a national cyber crisis, the National Security Authority (NSM) is responsible for the coordination, but not leadership. This adds a third actor to the equation, an actor which has no other crisis management role and no manned operations center beyond NorCERT, and which does not have authority to instruct other government bodies. To add to this confusion, NSM reports to both the Ministry of Justice and the Ministry of Defence, meaning that in a time of crisis when both Ministries would likely have an insatiable appetite for information, they would both be demanding it from the same directorate directly – and likely tasking them additionally in the process. The result could very likely be an overworked operational unit (NorCERT), doing double work and receiving double direction, without the staffing or competence to lead a national crisis, and without the authority to implement any measures of value directly.

### 7.2.4.2 From general national strategy directly to operationalisation?

Dispositions like these indicate that the problems surrounding CNOs are not only related to lack of specific subject matter competence, but also to a lacking organisation for implementation of the strategy. Generally speaking, a defined strategy should be implemented by creating an organisation. Once the organisation is defined, necessary resources need to be allocated to the various parts. Once this is in place, the strategy can be operationalised.

Failure to create the necessary organisation will make it unclear exactly who has what role, responsibility, and authority, and the effort will suffer from a lack of both necessary and efficient processes. Some tasks will be managed by multiple actors – some tasks by none. Interfaces and boundaries will be undefined or unspecific, and essentially everything will require clarification.
from the ground up once the crisis manifests itself.

The lack of organisation of security is not a new phenomenon. Generally speaking, when security works optimally it is unnoticeable, and when security measures are inadequate and fail, it is tempting to conclude that investment in security hasn’t helped. Assigning significant resources to security requires the removal of resources from an area that would give much more tangible results, especially in the perspective of a four-year election cycle. At best, one will typically see decision-makers re-task existing units that may never have been organised according to the current strategy, or assign marginal increases to whatever units represent the closest thing one has to the actual security need, without considering the need for reorganisation. Going back a couple of decades, the Norwegian government did not have an information security need relating to the defence of computer systems and networks. Without such a need, it did not have a strategy for defence of networks, nor did it have an organisation for it beyond what parts could be squeezed into other parts of the state administration. And at this juncture it may be a relevant question whether a fundamentally different strategy is needed, with the reorganisation need that would follow.

7.2.5 Separation of cyber defence and intelligence collection

Adding to the lack of necessary organisation, the Norwegian government is also mixing principally different, complex dilemmas, both of them with potentially huge implementation ramifications to the public. Digital border control has both a security aspect and an intelligence aspect to it.

7.2.5.1 Cyber defence at the national border

From a security perspective, it is critical that one government body is able to see the entirety of malicious network traffic and system activity towards critical Norwegian infrastructure. This includes reconnaissance, targeted malware delivery, command and control (C2), exploitation/network traversal, and actions on such as exfiltration of information or acts of sabotage. The detection engines needed for core computer network defence, to detect known indicators of compromise or suspicious network and system behaviour, are by nature not particularly intrusive. The more sensitive details of content are typically not the essence of this work. Rather, CND takes an interest in point of origin for emails, headers, DNS translation failures when C2-infrastructure is offline, known malicious IPs or network traffic patterns. Although one
can argue that it is possible to deduce sensitive information from large quantities of such metadata, it is certainly an order of magnitude or two less sensitive than the manual scanning of message content. It should be noted that content does figure in as well, perhaps even increasingly – but a lot of security work can be accomplished before one needs to start looking at content, or one can use metadata and indicators of compromise as triggers for content and packet capture.

### 7.2.5.2 Intelligence collection through access to all national network traffic

When combating asymmetric threats such as terrorism, insurgence or hybrid warfare, there are two basic approaches: either you build up a massive defence that can counter any attack, anywhere, at any time, or you try to find out where and when the attack will take place and focus efforts on stopping that attack. Through knowledge of the time and place of specific threats, it is possible to avoid excessive and intrusive security measures that would otherwise need to be enforced broadly upon large segments of the population. Consequently, actionable intelligence is a rational way to reduce national security spending and impact to an acceptable level.

The Lysne II committee argued that the implementation of digital border defence would have to provide “sufficient intelligence value” to justify its existence. Again, the lack of focus suggests an organisational weakness surrounding Norwegian cyber defence. CND should not be the driving factor when considering broad intelligence collection of traffic content. The ramifications are orders of magnitudes different in functional CND and in indiscriminate intelligence collection, from the point of view of privacy. By not distinguishing between these two agendas, the dilemmas are treated and discussed as if they were inseparable and relevant to the same problem. It is not that the protection of the Norwegian public from assassinations and terrorist attacks is not important; clearly it is. It just requires entirely different measures than cyber defence. And this confusion is likely part of the reason why the digital border defence project has been discussed for years without successful implementation of either part of it. If the tasks given to the committees are unclear, and if the government bodies responsible for implementing digital border defence do not distinguish between the overlapping agendas of intelligence and cyber security in the proposal, then it is hard to make their point of view clear to anyone else either.

Despite this, let us assume that traffic content and the intelligence derived from it was critical also to the CND mission. One could argue that among the content collected there would also be command & control traffic towards threat actor infrastructure, or stolen and locally encrypted
information being exfiltrated from targets in Norway. The requirement of “sufficient intelligence value” is still valid in this context. Because collected information about an enemy threat actor is not intelligence until it is understood by the decision-maker tasked with utilizing the knowledge in question. A relevant question in this regard is whether or not Norwegian authorities are organised in such a manner that they are able to process information into actionable intelligence and act upon it before the operation is over.

Although there is a component of manual interaction and persistence over time in advanced offensive network operations, the core of the operations is the execution of a series of operations in quick succession. From a CND perspective, one cannot assume that all computer network attacks will have manual interaction in every step of the kill chain, with corresponding delay. When defending networks one must assume that attacks will be as automated as possible, maybe even completely automated – particularly the most critical and time-sensitive stages from delivery to compromise, from compromise to network traversal, and from location of a target to “actions on”, as the last kill chain step is called.

The only way to realistically combat an automated attack, is through automated defence. Any manual defence process to combat an automated attack process is likely to be at a significant disadvantage. In this case one can say that the strategy in reality is not to prevent computer network attacks, but focus on restoring service or simply suffering the loss of information. This is a strategy, just like an air defence strategy could be to let bombers through and then rebuild and repopulate after the raids have been completed. But as this example suggests, most nations have a higher ambition for their national security efforts.

7.2.5.3 Ambiguous Digital Border Defence recommendations

According to Snowden leaks, some of Norway’s allies have found creative work-arounds to some of the legislative challenges presented by dilemmas equivalent to those discussed regarding digital border defence (Masnick, 2013). The most potent collection methods in any state sit within the foreign intelligence services such as GCHQ and NSA (in the case of the UK and the US), as they do not have to concern themselves with the rights of their own citizens in the same way as internal security services such as MI5 or the FBI do. By using the foreign intelligence toolkit to collect from each other’s “out of bounds” areas, and then sharing that information when something interesting was detected, both British and US agencies were able to stay within the letter of the law, if perhaps
not the intent of it. There is little doubt that all involved agencies had considered this arrangement to be of “sufficient intelligence value” to justify the invasion of privacy and challenge of constitutional rights. Quite possibly lives have been saved from information collected in this manner. But this sort of self-regulation for the greater good will invariably manifest itself if the legislative authorities are content with ambiguous recommendations, rather than specific direction.

7.2.5.4 The configuration of cyber defence solutions

Automation of cyber defence can take many forms. At one extreme, one could envision a completely automated solution that would take human delay out of the equation altogether. Such a solution could monitor and analyse network traffic and activity and respond appropriately - up to and including the launching of nuclear missiles in retaliation. But although there needs to be a high degree of automation in defence mechanisms to counter automated attacks, the implementation of artificial intelligence with the possibility of initiating acts of war is likely best left to science fiction such as War Games. On the other hand, the reduction of ambiguity, confusion and unclarity in all levels of decision-making is of the essence. The establishment of a common understanding of the problem among national decision-makers is a higher priority than both precision and a variation of perspectives in a situation where time is critical.

This requires a common configuration of cyber defence solutions across a broad segment of Norway. Defence, law enforcement, information specialists, infrastructure owners, all areas of government and administration all need to have a common agreement and understanding of both process and operation. A government model where sector authorities coordinate needs for all actors in their sector towards national intelligence and security services, though sensible from an administrative point of view, cannot be implemented operationally in the same way. The delay in manual assessment and compilation of information will in all cases result in a critical delay between detection, warning and execution of mitigating activities.

7.2.6 A sample case of national cyber incident handling in Norway

One possible scenario with a foreign state attacking Norwegian interests could be to sabotage power suppliers in Norway.
7.2.6.1 Who will detect the attack?

Assuming Norwegian authorities already have received or developed signatures for a specific attack, it is still not certain that they will detect the attack. First, if the signatures in question were partner information or for other reasons classified, they would not be in use in unclassified sensor systems – including the national sensor system VDI.

Second, if the signatures were shared with other agencies than NSM, like the armed forces, the criminal police, the police security service, or the intelligence service, then there may be some delay before they make their way to NSM and NorCERT. Assuming the signatures make their way to NorCERT it will be possible to conduct some level of historic searches, but details may not be as prevalent post-incident as if the necessary signatures and the corresponding packet capture was available as the attack is ongoing.

Third, even if the signatures are shared with NSM and implemented in NorCERTs VDI, there is still the issue that VDI is a very limited service, only available to what is described by NSM as a representative selection of institutions within important national infrastructure (Nasjonal Sikkerhetsmyndighet, 2017). Some power companies are likely to be included in that mix; but as there is approximately a three-digit number of power suppliers in Norway, they are not all represented.

Typically, power supplier companies do not have the capability to manage advanced cyber threats within their own information systems. This sort of expert competence exists in the Power CERT, but there is not a network for detection and warning within the Power sector. The likelihood that any of these smaller companies would independently discover and act correctly upon an advanced attack is low.

So an attack towards the sector could typically start with the detection of one or a few indicators towards those institutions covered by VDI. But in a worst case, there would not be any of the VDI-covered companies in the target list, and the only way to understand that an attack was ongoing could be through a partner tip-off. Typically tips from partners are slower means of detection than internal signatures.

Once one or a selection of the targeted companies have been identified, the task to identify all targets starts. Typically this would involve the Power CERT, which would need to understand what
NorCERT already had discovered and then communicate that to all relevant companies in the sector. However, many of the companies involved are likely not capable of performing even simple signature checks, certainly not forensics. And with the order of 100 institutions that need follow-up, with possibly a similar number of different IT solutions and configurations, this task can take months.

As more and more companies are identified as targets or non-targets, the scope of the operation will start to become clear. Hopefully it will be possible to find later stages malware from one of the companies involved, which could allow analysis on what sort of toolkit the actor is using. A dream situation would be if it was possible to follow a smoking gun through all stages of malware right to an industrial control system infiltration, with coordinated timers for shutdown, common command & control-channels or integrity breaches. Typically however, there would only be first stage droppers available without extensive analysis on some of the target systems. If the threat actor has been able to achieve privilege escalation on the target system, it is quite possible that the malware has been removed or placed in hibernation to make it undetectable.

In this case, a bit of guesswork or history browsing would be in order. In what other types of operations has this malware and these methods been used, and can anything be understood about the actor or intent based on that? Convincing decision-makers that there is a problem that needs addressing can be a significant challenge, when the actual evidence may boil down to two known infected power companies with three more possible infections, and the malware is a stage one dropper used by small-time hackers, one or two more organised hacker groups and the odd low-funded state actor. The message up the chain of command may be along the lines of “It could be anything, but we can’t rule out an advanced group infiltration of some segment of the power supply sector”. Before escalating it is likely that NSM would want to coordinate with the other intelligence and security services, which again would require precious time. If this was to happen, say, during a holiday, the delay could possibly be even greater. Possibly there would not even be enough resources with the right competence at work to manage the incident without starting crisis management. By the time decision-makers were able to identify that the actual operation was a shutdown of a segment of the power grid in the middle of a national holiday, to punish Norway for some foreign affairs criticism of a less democratic regime, the operation is likely to have succeeded.
8 What conditions need to be fulfilled order for infrastructure owner companies to perform their part in national CND?

8.1 State ownership of infrastructure and responsibilities

Looking back a few decades, national infrastructure was to a much larger extent owned by the Norwegian state. The advantage of public ownership is that the government is in position to dictate exactly the security level they desire around critical infrastructure. Since then a lot of national infrastructure has been privatised, both within power, telecom and other sectors. From a cost savings and efficiency perspective, the privatisation effort makes obvious sense. From a security perspective however, there is a flipside to that coin.

8.1.1 Business case and funding

Whereas government wants to be rid of the headache that is managing every component of national infrastructure, typically they do not want this to result in an inadequate level of security. Unfortunately, the business case for high security in a private company has limits. To a point one can say that having a high level of security in a company will increase sales in the market. But depending on the competition, the sector and the market, that is only true to a certain extent. For many customers, it is assumed that there is a high level of security in the services provided by critical infrastructure owners anyway. For the business, the risk of failure is to a point worth it, to be able to compete on price levels. Especially if the time to restore operations is assessed to be low under normal circumstances.

What about mitigation for state operations or acts of war? Private companies are not equipped to manage those sorts of attacks alone. Those types of attacks are a matter of national security and national interests, and must therefore be addressed through specific and separate funding from Norwegian authorities. For instance, maybe remote access to an industrial control system is deemed risky, as such a feature could facilitate attacks from state actors. One could enforce a policy of on-site access only to the most critical systems. Consequently, there is a need for on-site shift work rather than just call lists for people working from home. This additional cost would typically be
something the authorities would need to cover, to make sure the company in question would be able
to stay in business in a competitive market where cost is critical to shareholders and owners.

8.1.2 What threats should a company need to secure against?

Some types of threats, such as bitter former employees, idealistic hackers or simple fraud are types
of actors that one would expect a serious company to have security measures against. But from a
national perspective, the government would like to see security measures to handle other types of
scenarios as well. Scenarios such as state espionage, sabotage and acts of war. This is where
security implementation gets tricky. Because no company operating in Norway has the ability to
stop a state sponsored espionage attempt. Although security measures in place at the company can
to some extent mitigate even state sponsored threats, it is impossible to secure a business
successfully from advanced actors without substantial support from the government.

If a company wants to make sure they do not hire a foreign agent as an operator of national
infrastructure, the only way they can avoid that from happening is if national counter-intelligence
work identifies such an agent and the company is made aware of it. Similarly, the only way a
company can secure themselves against sophisticated cyber threats is through sharing of classified
intelligence and signatures.

8.1.2.1 Aren’t all cyber threats openly available to the public anyway, through cyber
security publications?

Some may argue that the need for intelligence and security agencies to support infrastructure
owners is no longer present, as there is such high quality on open sources reports. This is a
misunderstanding. There is a lot of information on the Internet, and the mere presence of high
quality threat information widely dispersed in that vast sea of information does not directly translate
to this information being readily available to any given company as effective guidance for decision-
making. The identification of valuable sources, the broad yet sufficiently precise collection of
information, the analysis and dissemination of decision support is called open source intelligence
among intelligence agencies. It represents a separate skillset that very few companies would
typically need to invest in. In addition, the cyber intelligence requires another dimension of
competence that would be a unique specialisation even in an open source intelligence unit. In any
three/four-letter agency, the collection of such information would likely be assigned to cyber specialists.

For the chief security officer (CSO) of any infrastructure-owning company, the task of replicating the analysis done by tens, hundreds or even thousands of skilled collectors and analysts in the various security and intelligence services, is not feasible. Communicating a clear, relevant, detailed and accessible threat picture is therefore the responsibility of the government.

A point to make here is that a threat picture should not just be considered a briefing, at least in the context of advanced network operations. The threat picture should be a current, automated and distributed system for recognizing malicious network and system activity. Only with this understanding of a threat picture, would any company be able to fulfil their part in detection and warning of an attack.

### 8.1.3 Detection and warning

Once the threat picture is communicated, the necessary preventive measures can be implemented – where any excessive cost due to state actor prevention would need to be a joint venture with government support. One of those joint ventures would need to be a platform for detection and warning. Essentially the cooperation brings together a compilation of threat indicators and warnings with the actual traffic and activity present in the infrastructure, as with the VDI system. But typically, existing detection and warning systems lack the ability to present a warning that is meaningful above the cyber defence specialist level. This means that in order to communicate with the company affected, a degree of analysis and communication will be required. Typically the people set to cooperate will have vastly different backgrounds, and the operations centre may also be further hampered by classification and confidentiality requirements. Presenting the detection of an advanced operation for management level in a company might require a physical meeting, and the response from management is unpredictable. The management could for instance decide that in order to avoid criticism from media later, the company immediately re-tanks all infected servers. Not only would this destroy all potential evidence present on the server, it would also eliminate any possibility of determining the entry vector to the server, or any further network traversal from that server.

In order to avoid complications such as these, it is important that the government prepares potential
target companies for the sorts of scenarios that might occur, and that they have an understandable and sufficiently detailed explanation regarding what the actual problem is. This simplifies management communication and decisions. From the government side it is possible to communicate different types of crises, and then all parties could have training in what to do in such a case.

8.1.4 Handling and restoration of services

Presently there is no government service or institution in Norway that has dedicated tasks in the handling and restoration of services for critical infrastructure. Even within the VDI cooperation, Norwegian authorities generally do not have capacity to extensively support a company in handling. Certainly there are circumstances where the authorities would offer support, in a high priority case; but generally speaking it is up to the affected parties to manage their own systems and networks.

There are several reasons for this. One is obviously cost, but another is the limitations and privacy expectations present in a democratic country. Countries with less democratic traditions such as Russia, China or some other regions of Asia are able to leverage national security to the point where they directly interact with private computers and servers. Informed consent is an expectation in a democracy, but from the perspective of CND it can become somewhat of a liability when compared to those countries who do not have these concerns.

One problem with this state of affairs is that national security will likely not be the top (or hardly any) priority in the decision-making surrounding the handling. This means that national interests are not likely to be ensured. For instance, the security services may assess that a Norwegian company has been victim to a spear-phishing operation from a state actor, and a compromise has taken place. The target company now potentially has one or more servers infected with several different stages of very advanced malware. A server infected with malware from an advanced actor is interesting from several perspectives.

First, there is the analysis of the malware detected on the system. Creating binary hashes allows detection systems such as VDI to increase their detection ability. Then there is forensics analysis to determine what other malware may exist on the system, which may help build an understanding of the malware delivery and staging. There is the proliferation of malware to connected systems and networks, and of course there is the activity on the system – including the exfiltration of
information or violation of data or system integrity. If the company has been used as part of command & control infrastructure, it may even be possible to identify higher stages of infrastructure, and it may be possible to find other targets in Norway or abroad.

8.1.4.1 Infrastructure placement

Why would a threat actor place “all his eggs in one basket” and establish infrastructure in the same country as the operation is being conducted? Usually an advanced network operation will place a network traffic redirect through a 3rd party country where legislation is “favourable” for the threat actor, for instance low information security infrastructure, or lacking security cooperation with the target country. But in order to reduce the likelihood of detection, it is also preferable to limit the number of target hosts who communicate directly with the server abroad.

For instance, a threat actor may be running an operation against 10 targets in Norway, all of them controlled directly from foreign infrastructure. One or maybe two of these may be covered by VDI, and in that sense be afforded some extra attention by the government. To the extent that this operation has noticeable indicators, the VDI coverage is likely to bring the operation to the attention of the Norwegian security services. From there, it is very possible that the infrastructure information such as foreign IP addresses will end up blacklisted both in the VDI system and in all channels where NorCERT cooperates. In a short amount of time that specific infrastructure will be unusable for all VDI covered targets, and also all partners of NorCERT, meaning that this particular component of infrastructure may be useless for many or most of the targets in the ongoing operation, and highly unreliable for further command & control. Of the 8 targets unknown to NorCERT, 4-5 or even more may detect their compromise based on the shared indicators, and will be able to report back and help Norwegian authorities map the operation much more completely. In this case, the fact that each target communicates directly with infrastructure abroad results in the attacker suffering significant setbacks.

Alternately, let us assume that the 10 Norwegian targets are connected through a command & control server in Norway, with a single exit point. Again, the two targets covered by VDI may result in NorCERT understanding that there is an operation ongoing, but this time the trail leads to a server in a Norwegian company.

This server cannot be blacklisted and shared, because it would risk putting a Norwegian company at
a significant disadvantage. Instead, the government would approach the companies and advise them of the problem. And this is where some companies may choose to instantly re-tank rather than conduct investigations or counter-intelligence operations. And so no information about the command & control infrastructure may be shared. Information about 4-5 other targets will never appear. The foreign link may be blocked, but the remaining 8 Norwegian targets can be redirected to different infrastructure and stay undetected.

The level of time and resources needed to effectively counter these kinds of operations are generally not of significant interest to a company that does not have national security as part of their direct agenda. In a case where a company has compromised systems that act as command & control infrastructure for a foreign state, the analysis of such a target would be critical to understanding what other national targets are compromised. A simple re-tanking would mean that the threat actor would take extra security precautions due to the detection, but then that the actor would simply associate the targets to other parts of their command & control network in order to continue operations.

8.1.5 Post-incident analysis

The post-incident analysis is where it is possible to learn from the incident. Most critically, this is where it is easiest to get an indication of the intent behind the operation, the vector of attack, and desired end-state. As more evidence can be collected, analysed and connected, a more precise picture of the chain of events can be drawn. For any given company to analyse their role independently in a national security context, will often give limited results. For instance, an attack against a single target, even if it is within critical infrastructure, may not be assessed to be a state actor at all. But an attack against a large cluster of targets in the same sector, is likely an operation that should have immediate national attention. And in between those two extremes there are any number of possible scenarios, the understanding of which is very highly dependent on the correlation of information from more than just a single company.

Even if all the information was available to individual stakeholders in critical infrastructure, the competence to collate the information most likely is not. Just like threat analysis is a complex topic, criminal investigation and forensics analysis is exactly the same. The specialised competence required to perform good analysis is very limited nationally, and should be focused in prioritised areas and units that can provide insight to everyone affected.
8.2 Company responsibilities

8.2.1 Management

The foundation of efficient security in a company lies in management understanding and acceptance of the complexity involved and work required. The National Security Authority has in their guide to security management (Nasjonal Sikkerhetsmyndighet, 2015) emphasised the importance of management involvement – including defining the ambition for security work, allocating necessary resources and regularly evaluating the state of security in the company.

Even among state owned companies or defence units, this needed dedication is not necessarily given. Intuitively, security is nothing but a money drain without a business case or visible results that provide any appreciable benefit. As previously discussed, when security is working at its best, you do not notice a thing. So when needing to do hard prioritisation between competing needs, in any given case there will often be low incentives for security.

In addition, the state of security is in many cases a matter of subjective assessment and risk willingness. What might be unacceptable or even violation of a law in one perspective, might also be the best available solution, a temporary exception while awaiting new solutions, or an acceptable pace in a ramp-up process. In financially challenging times, this flexibility in situational understanding makes it tempting to reassess the state of security and risk willingness according to the means available.

8.2.2 Roles and responsibilities

Security governance is to ensure compliance to an overall set of instructions and regulation. This is referred to as 2nd line of security, the operational level. Typically this is work assigned to an independent staff function, which advises management and has overall supervision of the state of security in the company. Maintaining security in all the different processes, solutions and aspects of work is the other. This is the 1st line of security, the tactical level. These types of security work are independent of each other, and managed through separate leadership in the same organisation. From a management point of view, it is not necessarily easy to grasp this nuance. 2nd line security advises and controls, whereas 1st line security work belongs in the working parts of the organisation, in
implementation and execution. The separation of these is necessary for the state of security in the company to reach the desired level. The line organisation will always want to front their solutions as adequate, and they cannot be expected to be neutral or objective in assessing their own work. But giving the security organisation the responsibility for the state of security can never work, as they do not have the competence to configure every solution in the company, they do not control the resources to do the work, they do not have the budget to make the investments and they do not have the overview to prioritise effectively. Security follow-up and control of compliance must be based on a top (or strategic) level management ambition and directive, be implemented through the line organisation, advised by the security department. Using the security organisation in the correct manner is essential to provide a foundation for combating advanced network operations. Just as at the national level, it is important that security functions do not become autonomous units with separate agendas and out of sync with both the management and the overall organisation, but rather an expression of the management’s security ambition and strategy.

8.2.3 Governance and asset management

With the proper security governance and understanding of security-related responsibilities in the line organisation, the security department is prepared to communicate and advise on the chosen solutions and strategies throughout the company. In order for this to be efficient, there needs to be established governance and defined processes for all other aspects of the business as well. General governance needs to reflect and be closely coordinated with security governance. For instance, in order for security to ensure that network management is compliant with security controls, there needs to be a clear and documented understanding of who manages networks, what responsibility lies in network management, what networks there are and how are they configured.

Like security, governance and administration is not always an appealing topic to management. It is an investment that requires more work, coordination and documentation from every asset and process owner. It requires discipline. Not everyone has the authority to perform all kinds of activities or make autonomous decisions. It requires organisation in a sort of hierarchy which is a somewhat unfamiliar cultural trait, both in developer and IT circles in particular, and Norway in general. The correlation between predictable and well defined processes and automation may not always be obvious, but these two come hand in hand – and in many cases one can argue that there can be no real governance or security without broad implementation of automated solutions.
8.2.4 Business benefits to pursuing a national security agenda

Having stated that maintaining all national security interests in a company usually is not a good business case, there are some aspects that are.

8.2.4.1 Risk mitigation

The controls and risk mitigation requirements for national security – the actual implemented measures to avoid breaches of confidentiality, integrity or availability – are not necessarily very different from what would be recommendable measures for company operations or customer security. By using national security measures as a baseline or desired position and handling exceptions from that, a company would be able to claim that they have a responsible level of security in the event of a breach.

8.2.4.2 Organising security work

Security work in a company has challenges and concerns in all the same security domains, whether or not national security is a factor. With the ISO 27001-standard as an example, the protection of information will require a policy, instructions, and guidelines. It will require an organisation of a dedicated 2nd line security department and a clarification of roles, responsibilities and processes in the line organisation. It will require instructions, governance and documentation of personnel management, facility management, IT, networks, operations, suppliers etc. None of this changes. Organising the security and governance work according to national guidelines, and with the suggested processes in place, will both entertain the security and governance needs in the organisation and provide a selling point compared to competitors.

8.2.5 A reluctance to implement effective security

The rationale companies use for opting out of recommended standards may in some cases have less to do with a gap between an implemented and reasonable level of security and more stringent
national recommendations, and more to do with the gap between the actual level of security and national recommendations. The director of NSM, Kjetil Nilsen, stated in 2014 “Norske virksomheter har ikke gjort det de skal for å sikre seg (Norwegian companies have not done their part in securing their assets)” (Johansen, 2014). With custom governance solutions instead of industry standards, and lacking easy measurement systems, a company can avoid meaningful comparison to defined objectives and the status of comparable companies, on topics that may reflect a lack of ambition within security.

8.2.5.1 Emergency communications exposed

Even a government organisation may struggle to incorporate security in a meaningful and comprehensive manner. The directorate for Emergency Communications (DNK) in Norway was recently reported to have had infrastructure, owned by Broadnet, managed from India (Lyngstøl, 2017).

One could question the decision to include a supplier based in India in national emergency communications. From the perspective of international security cooperation, India has no security agreement with Norway or NATO. Quite the contrary, India enjoys close ties with Russia, considering them their primary security partner, and the two states have recently embarked on improving cyber security together (Raghavan, 2016). For Norway, there is probably no other actor in the world more worrying from a cyber sabotage perspective than Russia.

In fact, cyber actors based in India have already manifested themselves as more than just a potential issue to deal with. Telenor suffered a breach from an actor dubbed Appin (Muncaster, 2013), which may or may not suggest involvement of the Indian IT Security company AppIn. It may not just be a one-off either: the actor has been associated with other similar type operations (Spring, 2016). From a supplier security perspective, where any foreign dependency is a no-no, it is difficult to see how security factored into the decision of placing such a dependency in India.

One possible explanation is that it did not. Based on media coverage Broadnet has not adhered to contractual requirements. So DNK had at same point stated “the following conditions are required”. But as anyone working in security can testify to, simply stating rules does not necessarily guarantee compliance. An ISO 27001-framework for information security would suggest that there was a defined process for audit of supplier management, to ensure that Broadnet actually adhered to the
requirements. The key difference between conducting such a process and not doing so, is that rather than suppliers just saying “we promise to comply” they present “this is how we comply”. In the event that Broadnet documented their solutions with their own supplier dependencies, one could most likely expect an auditor of security in the Directorate for Emergency Communications to react when Broadnet documents an Indian supplier of critical operations, based in a country outside of any international security cooperation with Norway.

The risk would have been on the table in other contexts as well. Before these audits would have been conducted, the decision to outsource to India was made in Broadnet. Again, ISO 27001 or an equivalent standard would suggest that such a decision was subject to a documented risk assessment. Moving operations to India would for any service provider in Norway be potentially controversial, even before Emergency Services and government contracts were considered. When that service provider is subject to additional and rigorous regulation through the national security legislation, the magnitude of the risk becomes unproportionately large. But the business case is equally obvious, and the absence of people with the competence to provide a comprehensive risk assessment from decision-making processes, is one possible explanation as to how a company regulated by security legislation ends up potentially facing criminal charges – which would be the first time in Norway someone has faced charges for violating the Security Law (Befring et al, 2017).

8.3 Detection and warning systems in cooperation with national security services

Finally, in order to reach a degree of automation of national cyber defence, there is no substitute for a detection and warning system that incorporates the accumulated knowledge of state agencies, and the real-time insight into the information systems that represent national infrastructure and interests.
There are many aspects to computer network defence operations, but one overall way to categorise defensive measures is to label them \textit{preventive} or \textit{reactive}. The preventive measures are every action a target conducts up to the point where a threat actor commences an offensive CNO against the network and in some way manifests itself, and the reactive measures are the mitigating efforts that follow detection.

\subsection*{9.1.1 Preventive measures}

Generally speaking, it is challenging and costly to implement preventive CND measures that offer any kind of guarantee against compromise. This is true for all sectors and industries. Companies, institutions and government agencies are required to make significant investments to avoid leaving their computer networks vulnerable to many types of threat actors. Defence in depth, such as patching, segmenting networks, reducing user rights, password discipline, whitelisting applications and filtering or inspecting email attachments is crucial to mitigate the risk of unwanted incidents. But any network threatened by an advanced group, with a direct or indirect connection to the Internet, runs a high risk of compromise. It is useful to assume that, at some point, any network of value to a threat actor will be compromised. In the event of a compromise, reactive measures are needed to determine the extent of damage and to mitigate intrusion in a timely manner.

\subsection*{9.1.2 Reactive measures}

Computer network operations (CNO) can be highly complex not only in their own nature, but also with regards to the response required to them. Incident handling surrounding these threats is therefore challenging on a number of levels, including understanding a CNO’s origin, its function and the intent behind it.

\subsubsection*{9.1.2.1 Incident handling}

Various actors are involved in the different stages of incident handling. Typically there will be government actors working on detection, there will be private security companies working on analysis and support, and targeted companies will typically be working on prevention and
restoration after an attack. The focus for this project will be on the specific tasks between the time when an incident is detected and when a warning is issued.

9.1.2.2 The challenge of the defender

Advanced groups may have a number of different intents for compromising a network; this may include espionage, sabotage or presence for later action. But regardless of their specific task, one can assume that advanced groups will often only need days, hours or even minutes to extract or modify the highest priority target data. A successful defence will require decisive action to be taken within that timeframe.

Upon detection, it is likely that the threat actor is already far into their operation and only a few steps away from starting to realise their objectives. The defenders, on the other hand, still have to orient themselves and make decisions before they can start acting. The challenge for the defenders is to restrict the attacker’s advantage and regain control from this reactive position.
10 Present state of national level detection and warning systems

10.1 Present model

One essential task for defenders is to reduce the time from detection to actionable warning to be as near real-time as possible. In the circumstance where the target system is protected by sensors, then an indicator of attack/compromise will typically trigger an alarm. The alarm will often be handled manually by the detecting agent and an assessment will need to made based on the present information. Once the alarm has been given a priority, it will be fed into a process where it is considered against other known cases, including information from open sources and partners, an preliminary attribution, an assessment of the target, scope and relevant advice at different levels.

![Diagram of Present model for detection and warning of cyber attacks]

Once this manual and iterative process has been completed, the detecting agent will be able to compose a warning. Generally the highest priority is given to the targeted company or institution, as they are an obvious relevant party. In some cases it can be challenging to determine if other parties...
should receive the warning. Examples include warnings that warrant government response, such as legal prosecution or military operations. Although this is very rarely relevant, the day it does become relevant would be the “moment of truth” for strategic cyber defence. One cannot assume that this situation never will occur. It is also necessary to assess the importance and relevance to national and international partners. For each warning distributed there is likely to be an increase in workload, and due to information sensitivity there is often a need for tailored warnings. The necessary balance between saving workload and wide information sharing leads to a risk that partners that would benefit from the warning might not receive it, or that valuable feedback on malware proliferation is lost.

Information standards with regards to CNO varies, and information sharing will often require a custom process by both parties before any value can be gained. There will also likely be a need for reassessing the warning and its implications by the partner, as the receiving party may not be given all the relevant information or be given insight into which factors were essential for the assessment. In order to obtain a balance between refining information and timeliness, a greater amount of automation and predictability is necessary between detection and warning. Simplicity is a requirement in both cases.

10.2 Stakeholders in CND

There are many stakeholders when responding to a CNO. In many cases companies own the targeted systems. The government is responsible for both policy to reduce risk, as well as strategic level response to secure national interests. Intelligence and security analysts in think tanks and consultant agencies assess the various components of a CNO and support companies in both preventive measures and restoration of services, and in a military scenario the armed forces will be required to consider CNOs as support or a force multiplier to an enemy’s conventional operations.

Also in many cases handling will for any single stakeholder be limited to just a small part of the cyber operation, such as detection and warning, malware analysis and signature development, reducing vulnerabilities, mapping operational details to an actor, designing security infrastructure or implementing policy. This means that the involvement of all stakeholders will be a very complex affair, complicating the already time-consuming manual processes further.
10.3 Research question B: What is the status in addressing shortcomings in the national defence effort against CNOs?

The preceding chapters have illustrated some of the most significant developments in Norway over the past decade. They have also described some of the challenges that the developments have attempted to address. The principal complexity present in public-private cooperation has also been demonstrated, the degree of manual assessment involved in incident handling, and the potential amount of stakeholders involved in even a single incident. But trying to manage this complexity by reducing membership in the process, might mean that significant value is lost to some of the stakeholders. A degree of simplicity, standardisation and automation is therefore most likely needed in order to succeed with computer network defence.
11 Strategic framework description

A strategic framework is a possible solution to comprehend the nature of a given threat within the required timeframe to effectively counter the attack. A CNO framework can offer a common approach to understand an incident among all involved parties. This understanding does not necessarily need to be a completely precise model of reality; it should serve as a basis for standardised communication, information sharing and predictable nomination of scenarios. The proposed framework can be simple in the sense that it only provides common classifications, but still be comprehensive enough to address the main factors of a CNO and reduce uncertainty for handlers and decision-makers at all levels.

11.1 Framework concept and purpose

Firstly, the framework should describe a general approach to interpreting and presenting a threat actor who is trying to conceal its nature and purpose, intended to provide overview in support of decision-making processes. This sort of prediction of covert intent is called intelligence. Other research on models to increase the understanding of cyber threats has observed “Improved cybersecurity requires digital threat intelligence”, with a focus on simplifying, standardising and automating the understanding and information sharing of threats (Bromander, Jøsang and Eian, 2016). Hence the framework should be intelligence based, and should consider relevant doctrine for intelligence products. A challenge when creating such a system is to narrow down the output to only contain information that can be considered true with some level of confidence.

The framework contains a limited set of scenarios based on existing evidence and a predictable assessment or weighting system. This tool can facilitate three different tasks:

- Identification of the most likely scenario
- Identification of the most dangerous scenario
- Disproving hypothesis in the most rational order

11.2 Attributes of the framework
CND changes over time; hence the framework must be dynamic and scalable.

It should be built with an infrastructural approach, with components that are independent units in their own right with standardisation and uses beyond this specific framework.

The framework must be implementable for existing detection and warning systems rather than require a completely new design. It must be comprehensive enough to encompass the most significant aspects of a CNO while still being as simple as possible.

The framework should adhere to the principles of intelligence from Joint Publication 2-0:

11.2.1 Synchronisation

Intelligence should be synchronised with operations and plans in order to influence decisions in a timely manner. Therefore, the framework should be simplistic enough to automate as many of the core processes as possible.

11.2.2 Integrity

The framework should facilitate transparency in the understanding of the various indicators of a CNO, in order to create predictability in the assessments. The interpretation and weight of an indicator which supports a hypothesis must be clearly defined and easily accessible.

11.2.3 Unity of effort

Through standardised representation of a CNO, it is possible to leverage many actors’ collection and analysis capabilities, combine them, and efficiently disseminate the results. Any provider of standardised signatures such as for antivirus programs could serve as a feed for threat intelligence in the framework.
11.2.4 Prioritisation

Through a common framework it is possible to understand how partner agencies nominate and prioritise a CNO. Everyone using the same common language will have the same understanding of how a given operation was assigned the priority it has been given, as opposed to there being a large degree of qualitative assessment involved. Qualitative assessments can rarely be communicated clearly enough in the timeframe available.

11.2.5 Excellence

In order to maintain the highest quality, the framework should be based on best practice components. This framework includes the cyber kill chain representation of threat actors at the tactical level, a mission task understanding at the operational level, and basic models of conflict theory at the strategic level.

11.2.6 Prediction

Modelling reality precisely, as a basis for intelligence, is a challenging task. In order to achieve the goal of presenting actionable intelligence in a timely manner, it is necessary to accept the risk of inaccuracy, pursue simplicity and develop pragmatic models. Describing history with high precision is a principally different activity from performing prediction, even though they are not unrelated activities.

11.2.7 Agility

The framework needs the flexibility to incorporate all manifestations of CNO, including projected and predicted future developments.

11.2.8 Collaboration

The framework should be a model subject to academic scrutiny and criticism, in order to encourage subject matter experts to contribute in the development of the framework.
11.2.9 Levels and critical factors in understanding a network operation

Three levels of war are defined in Joint Publication 2-0 - tactical, operational and strategic. A framework for CNO should use the same approach.
12 Basic elements of a CNO

12.1 Actor

12.1.1 Background

Understanding the actors who use network operations requires knowledge of several dimensions. One dimension is the allegiance of the actor. It may be an autonomous actor, with individual interests. But it may also provide a service for other interests. The actor may do both, and the more advanced and specialised the services are, the more likely it is that the actor represents more than a single type of interests. One can distinguish between different components of an actor, which may not even be fully aware of their role in an operation.

A sponsor represents the interest behind a network operation. Typically a sponsor will want to provide some distance or obfuscation between themselves and the execution of a network operation. In its simplest form, this may be a teenager ordering a denial of service (DoS) attack against a game server as retribution for losing at the game. By ordering a DoS attack through a web interface, the actual attack will originate from an attack infrastructure that an operator provides. The operator is in this case interested in the money of the sponsor, and together with other sponsors ordering similar kinds of attack, the operator has its expenses covered and is able to maintain and continue developing his infrastructure.

The payment in this case may be handled by a third party such as Paypal, which becomes a facilitator. Similarly the operator may be buying the malware to build a zombie network from a separate developer.

A more advanced example may involve the interests of a nation state. In this case the sponsor may represent an interest in espionage against or sabotage of another state's politics, business, industry or research. The sponsor might channel their interests through an intelligence or security service. Facilities may be provided through government institutions or public-private partnerships, and activities may be supported through military projects. Development of malware may be provided through research projects, and operations may be conducted by criminal networks in coordination with intelligence officers.

Adding to the complexity of this, any part of the actor picture may not actually represent the interests one might expect. For instance, one would generally consider that the involvement of a
government institution to be a sure sign of state involvement. But is that necessarily the case? In June 2015 BBC reported that “China's ex-security chief Zhou Yongkang has been jailed for life” (Hatton, 2015). Zhou Yongkang was once the head of the Ministry of Public Security (MPS). With responsibilities including the cyber-defence of China’s interests and operating the “Great Chinese Firewall”, the Ministry controls substantial resources with the necessary capabilities to conduct various kinds of cyber warfare. Although there may be a number of contributing factors and agendas behind a corruption charge of this sort, it still appears apparent that the former minister has conflicting interests with the leaders of the Communist Party. This conflict of interest may also manifest itself in the tasking of resources who play a role in advanced network operations. This means that even with a proven link to such a high level official, the real sponsor may in fact be another than the government in question, and the people involved may be unaware of the true purpose of their work.

For all practical purposes then, the idea of correct and precise attribution to a sponsor is at best very challenging. In many cases it may not be advisable, given the resources required, to make a precise actor assessment, and in some cases it will in fact be practically impossible. Yet this question is the first and most common in the handling of advanced network operations, and an unproportioned amount of time can easily be spent on this topic. In light of the complexity of the issue, a different approach to the question of the actor and the sponsor is to categorise and score the evidence present and create an attribution score that will indicate that some types of actors are more likely than others. Although this is not a precise method, it will in most cases indicate enough characteristics of an actor to start making qualified assessments about the most significant actor attributes, such as motivation, resources and government support.

12.1.2 Categorisation

At the first or tactical level the ambition may be limited to *understanding the actor*, a preliminary attribution and description of the actor based on indicators and existing intelligence. The framework should combine existing taxonomy and models into a larger whole. At the actor level, one way of representing the threat capabilities is through the cyber kill chain. Each step contains the various manifestations of the actor, including all possible indicators of compromise. The model should include both a quantified representation of the actor to support database implementation as well as a complete multi-source intelligence assessment of the actors, for strategic analysts. The detailed
manifestation of such a database is probably worthy of a project of its own, but the key point is that there needs to be a database manifestation of threat actors to use for comparison with technical indicators as they appear in the sensor system.

Whether the actor is previously known or not, it should still be categorised within one of the following:

- State
- Commercial
- Organised criminal
- Idealist
- Terrorist, individual or small group

### 12.1.2.1 State actor attributes

The tree- or four-letter agencies. Patient, well-funded, competent, with a significant network deployed and a smorgasbord of malware tools at their disposal. State actors represent all aspects of national security agendas, international security policy and the highest ambitions of network operations.

### 12.1.2.2 Commercial

Commercial cyber-actors use network operations to support a legitimate business or enterprise. Examples of notable businesses discussed in cyber security forums as having ties to cyber operations include Huawei, ZTE, Kaspersky Antivirus, Samsung, LG and ApplIn. These claims can be difficult to substantiate, and suspicions and accusations rarely lead to successful legal action. Some of these claims relate to state cooperation, but large enterprises can also have an interest in conducting their own industrial or corporate espionage to gain a market advantage. Their financial muscles, their expertise and the CND competence they already possess from defending their own values put them in a position where network espionage operations can be both an easy and tempting next step.
12.1.2.3 Organised criminal

The main difference between Organised criminal (OC) and Commercial actors is that OCs conduct network operations in support of illegal activities, rather than an otherwise legal business. Examples most commonly involve fraud, but could also include activities such as drug dealers, human trafficking, smugglers, arms dealers, or child porn distribution. Most phishing actors would sort under this category.

12.1.2.4 Idealist

Idealist actors include groups such as Wikileaks or Lizard Squad (Vaas, 2016). Typically these actors have significantly less in the ways of funds or possibility to establish network infrastructure, but may still have an organisation with competence to perform compromises or attacks against specific vulnerabilities (Haas, 2015). The label “Idealist” may be slightly misleading in the sense that not all of these actors necessarily think they are doing good, they just have an ideological persuasion of some sort that is different from national interests, business or money.

Although Idealist actors appear at the lower end of the cyber operations potency scale, the damage they can do is still international headlines-level. And the actors also include such groups as the Red Hackers (Hesterman, 2014). Once just dispersed individuals or small groups, they have been organised into a potent force through initiatives such as China’s Cyber Militia (Wittman, 2011), (Harris, 2008). With significant capability and capacity, Red Hackers represent a real force multiplier for China’s People’s Liberation Army (PLA) when coordinated and organised.

12.1.2.5 Terrorist, individual or small group

In all other regards, terrorists distinguish themselves in their willingness to cause damage and take lives indiscriminately. In the context of network operations however, terrorists have not established themselves as a factor above the complexity of individuals or small groups. Generally terrorists seem to prefer indulging in activities that allow profile pictures with military hardware such as machine guns and rocket launchers. The closest terrorists have come to network operation is cooperation with the next higher tier of actors; confused Idealists such as Lizard Squad’s flirting with ISIS (Miller, 2014). In addition there are clearly state actors that support various terrorist
groups, but in that case they are pursuing joint agendas rather than a separate terrorist agenda.

Characteristics of this group are no dedicated infrastructure, commercially available tools, low funds, short time span, and targets of individual rather than general interest.

12.1.2.6 Why not Insiders?

In many types of cyber threat actor categorisations, insiders are a separate category. However, insiders have no unique and shared agenda, but rather represent one or more of the actors above. In some cases insiders are aware, in other cases unaware. In some cases they are the actor; in other cases they are pressured, bribed or employed by the actor. Although the vulnerability of having an insider in place is significant, it does not change the fundamental actor landscape or agenda.

12.2 Operation

At the second or operational level the ambition may be to understand the operation being conducted, as a function of the actor, the target and the actor’s actions against a target. Based on this it is possible to deduce the specific mission tasks being executed in the operation.

12.2.1 Understanding the target

One component of an intelligence understanding of the operational environment (JIPOE) is the battle space. For the purpose of this framework, the battle space can best be understood by understanding the target of the CNO.

There are several aspects of a target. Firstly, a target represents knowledge. This may be classified information, business secrets or competitive technology. A target may also represent knowledge about an association or business deal. It may represent physical infrastructure in the target nation or area, such as power, communications or water supply. A target may be a vector towards a different target or a multitude of targets, and as such be attractive as part of the threat actor’s infrastructure.

Some people associated with a target may be openly known, and others may have covert roles.
Depending on how accessible the detailed information about a target is, it is possible to understand various aspects of the operation, such as the value of the target, the degree of preparation or reconnaissance efforts.

People in an organisation hold different roles. Although any employee may potentially represent an attack vector, it is more likely that the executive’s account holds more information of direct value to an espionage operation. Similarly, an operations engineer may be a likely target with an aim of manipulating control systems.
12.2.1.1 Categories

In defining the target value, it is possible to choose as detailed an approach as one desires. However, it is important to divide all possible targets into a category. One approach might be to use the government ministries/sectors, and sorting targets into one primary sector. Another might be to sort by function, such as defence, critical infrastructure, public services, crisis management, private sector and general population. For the purposes of this paper, the Industry Classification Benchmark (http://www.icbenchmark.com/) will form the basis for target categorisation.

For each subsector, the general attack and espionage value must be assessed for each of the actor categories, or even specific actors.

<table>
<thead>
<tr>
<th>Industry</th>
<th>Supersector</th>
<th>Sector</th>
<th>Subsector</th>
<th>Definition</th>
</tr>
</thead>
</table>
| 43210 | Health Care | 43211 | Health Care - Stewardship & Service | |}

Figure 2: Industry classification benchmark

12.2.2 Defining the task

The basis for understanding the operational task is a general classification. Military units as well as state sponsored groups from intelligence and security services can be assumed to pursue designated tasks. Other advanced groups likely pursue a similar disciplined approach to their targets, with specific ideas of what they are trying to achieve.

Mission tasks generally have constrained bounds and clear definitions, such as described in the Joint Mission Essential Task List (JMETL) Development Handbook and in Field Manual 3-90 Tactics of the US Army. JMETL describes the importance of simplifying operations as much as possible – “A joint force commander should assess the contribution of each task and include only the most essential tasks”. FM 3-90 also describes clear, precise tasks, with an exact ambition level, that do not overlap with other tasks, and that mean the same to everyone involved.

When trying to understand what the actor is doing, it is necessary to understand exactly what tasks can be achieved through CNO. Again, a standard should be applied, to benefit from field exposure and academic discussion. Once tasks are defined in a limited set, it is possible to rank the likelihood of the different possibilities based on existing evidence and intelligence. It is also important that the automated detection mechanisms are able to distinguish between tasks, or else the task understanding becomes hypothetical or academic.

The suggested tasks are therefore based on the violation of the common information security principles of Confidentiality, Integrity and Availability (CIA). Valid tasks are:

Data Denial
Degrading
Disruption
Destruction
Theft

In addition, two other tasks present themselves as reasonable to include in the framework:

Physical control system manipulation
IT resource manipulation or takeover, such as servers for threat infrastructure development

The reason for these two last categories are because they imply a resource investment far beyond what is accessible for most threat actors, and therefore a very high ambition. Also, it is possible to identify targets as having industrial control systems (ICS), and the breach of an ICS would immediately indicate that an ICS attack was ongoing. This binary detection mechanism makes it a simple task to manage in the framework.

Malicious infrastructure development through server takeover is not quite as binary. However, the likelihood that this task is being performed increases almost exponentially with each established malicious communication channel going out from the target. The first couple of connections can be attributed to normal command & control; but beyond that the likelihood of the server performing a network function is high. Therefore it is possible to see indications of this task from the first signs of detection.

12.3 The strategic intent

This framework will primarily address inter-state conflict, although the framework should also be more generally applicable. The intent behind a network operation can be generally defined as a function of cause and intensity. This provides a simple model for the political or strategic context of the operation.

12.3.1 Cause

Karl Marx has been called the father of conflict theory. He has described that the essential causes of conflict have their origin in class struggle (Marx & Engels, 1848). Since then C. Wright Mills has described modern conflict theory (Mills, 1956) with additional dimensions of conflict – where the distribution of power is at the core of conflict. The additional dimensions include military, economic and political systems.

Based on this, if we broaden or modernise Marx’ class conflict to a socio-cultural conflict, and if we label a military conflict as territorial, the following causes can be used:
Wealth or economy represents the basic resources at stake. Politics represents the tools to control wealth distribution. Territory gives access to the resources and population. Socio-cultural grouping creates groups with conflicting interests and ideas that can have agendas of their own, or be leveraged by others.

Given recent developments within international conflict, it also makes sense to designate a separate subcategory of socio-cultural or even political conflicts, namely religious ones. This is meaningful because state-like actors such as Taliban or ISIS draw such a large part of their politics from religion, because many states with Islam (which has not been through a reformation process) as their state religion are experiencing turmoil as they develop as nations, and because religious differences have inspired both fundamentalist and right-wing high profile terror attacks in recent years. So we add this category to causes:

Religious

12.3.2 Intensity

Intensity of inter-state conflict should be divided into easily separable levels. The key is that there should not be any interpretation needed to establish the level of conflict between two states.

Dissent/Hostile rhetoric

Sanctions

Threats of use of force

Deniable use of force
12.3.2.1 Dissent

The basic level of conflict is rhetoric, but no actual implemented measures that affect the opposing state.

12.3.2.2 Sanctions

Following rhetoric is the first level of escalation – sanctions. Trade embargos or tolls are examples of such measurable policy.

12.3.2.3 Threats of use of force

Following sanctions, one state may suggest that force may be used. Examples may include Russia’s threats towards Finland and Sweden when discussing NATO membership (O’Dwyer, 2016). This example is general, other threats may be more local and specific, such as when Turkey threatened Russia to stay out of their airspace (Seibert, 2015). In either case, this presents a new intensity of the conflict.

12.3.2.4 Deniable use of force

The deniable use of force is also a very perceivable escalation of conflict, such as when Russian soldiers invaded Crimea (Shevchenko, 2014). No one denied the existence of these troops, although it was unclear (or at least deniable) exactly who they represented. And as long as the troops have superiority and do not need protection as legal combatants, there is no real downside to maintaining this ambiguity. Quite the contrary, such ambiguity limits response options from the defending parties, as you cannot treat criminals or rebels as if they were the military forces of a foreign state. This limits the use of military action, and forces the defender into a law enforcement track.
12.3.2.5 Conventional operations

Finally, there is the state of war, where conventional forces are used openly between states.

One could argue that nuclear war is a higher escalation of conflict. But in the event a nuclear war became orders of magnitude more destructive than conventional war between superpowers, advanced network operations would most likely become a lesser concern.
12.3.3 Highest ambition intent matrix

The two factors Cause and Intensity can be paired in a matrix, which will give an indication of the likely **highest ambition** intent in each case.

<table>
<thead>
<tr>
<th>Dissent</th>
<th>Economic</th>
<th>Political</th>
<th>Territorial</th>
<th>Socio-c.</th>
<th>Religious</th>
</tr>
</thead>
<tbody>
<tr>
<td>Econ espionage</td>
<td>Change opinion</td>
<td>Make claim to land</td>
<td>Reduce standing of group</td>
<td>Reduce standing of religion</td>
<td></td>
</tr>
<tr>
<td>Sanctions</td>
<td>Reduce resource value</td>
<td>Psyops/manipulate opinion</td>
<td>Gain influence</td>
<td>Influence policy</td>
<td>Influence policy</td>
</tr>
<tr>
<td>Threats</td>
<td>Force change of resource use</td>
<td>Force subject change</td>
<td>Delegitimise ruling power</td>
<td>Limit rights of an ethnic group</td>
<td>Gain supporters, limit opposing religious group</td>
</tr>
<tr>
<td>Deniable</td>
<td>Deny resources</td>
<td>Force policy change</td>
<td>Incite civil war</td>
<td>Attack and confine ethnic group</td>
<td>Attack, confine or convert religious group</td>
</tr>
<tr>
<td>Conventional</td>
<td>Take over resources</td>
<td>Overthrow government</td>
<td>Annexation</td>
<td>Displacement/genocide</td>
<td>Conquest, conversion</td>
</tr>
</tbody>
</table>

*Table 1: Highest ambition intent matrix*

For each actor a given state or entity considers itself to be in conflict with, an assessment must be made. The assessment must describe which conflict types exist, and what intensity level is the conflict at. For instance, the Senkaku islands dispute put Japan and China in a territorial dispute
with the intensity of threats of use of force. This does not necessarily cover all conflicts between the two nations; they can also be considered to have other conflicts. South Korea can be said to have a Territorial conflict with North Korea at the Deniable use of force intensity level. China and the US can be described as having an Economic conflict at the Sanctions level. Any two entities may have more than one conflict, but the intensity should generally be described as the highest intensity of any conflict between them.

When populating the table, the entries should reflect empirical data to as large an extent as possible. In the event that for instance a territorial conflict at the deniable use of force level usually does not indicate an ambition of inciting civil war, the table should be modified accordingly. The examples used are mostly illustrative, not scientifically established. Creating the entries is most likely worthy of a separate project.
13 Revised model for cyber defence

The revised model illustrates the three basic elements of a network operation, and the processes which allow implementation in a detection and warning system.

13.1 Explanation of the revised model

13.1.1 Actor nomination

In this revised model, the indicator/indicators are automatically compared to an intel database, which is continuously maintained and improved by threat analysts. The comparison follows the cyber kill chain steps, and can be both specific items such as IP addresses, header info, content info, anomaly, or general methodology such as scans or email delivery from unknown origin.

Two basic conclusions can be reached from such a comparison: either the activity is attributed to one or more actors or actor categories in the database with some degree of confidence, or it is
dismissed. These thresholds are important to maintain so they provide functional assessments, but from this intel database comparison one can expect to be left with a few actor category nominations, with decreasing likelihood. For instance, traffic originating from government systems towards IP infrastructure listed in a state actor campaign from two years back, may be nominated, in order of likelihood, as

State actor
Organised crime actor
Idealist actor

13.1.2 Operation nomination

Once an actor is in place, the target and task must be understood. In the example above, if the only indicator is an IP address with earlier association to a state actor campaign, then that actor’s campaigns will give an indication of interests. If the target industry is overlapping, this increases confidence. Similarly the industry can be compared to the other relevant actors.

Task may not be able to assess based on the indicator, if there is no compromise. In that case the most likely task performed by that specific actor, towards the sector in question, is the default choice. After this assessment has been made, a new nomination exists, for instance:

State actor conducting information theft towards government target
Idealist actor conducting data degrading towards government target
Organised crime actor conducting information theft towards government target

13.1.3 Intent

For the State actor, the relationship between countries involved will direct us to the relevant table entry. For Norway and Russia, for instance, the conflict could be defined at the sanctions level, possibly bordering on the threat of use of force, and the conflict is at least both territorial and political. Similar assessments could be made for the other actors, and a complete nomination might look something like this:

Russian state actor conducting information theft towards government target, with the intent of
influencing Norwegian public opinion – low confidence.

Idealist actor conducting data degrading towards government target, with the intent of discrediting Norwegian authorities – low confidence.

Organised crime actor conducting information theft towards government target, with the intent of reducing resource value – low confidence (e.g. intelligence on smuggler routes, schedules).

13.1.4 Quality assurance

The first manual step occurs once the above automated steps are complete, and would be an assessment of the nominations, along with a presentation of the evidence that led to the nominations, and the exact details of the actors involved.

In the above example, seeing as all nominations are based off a single indicator, the confidence of all the nominations is low. On the other hand, the weight of the indicator has qualified for a nomination in the first place, and the context generated serves as a useful tool for warning the affected targets and having a slightly more informed discussion with them, until the different nominations can be confirmed or disproven.

13.2 Open research questions

The third research question is how can a balance be reached between the need for confidentiality and the need for information sharing about cyber incidents? It is unrealistic to expect that the communities managing sensitive information regarding network operations suddenly will develop a profoundly different attitude from their present reluctance to share abundantly. In many cases information classification, national security, legal matters and non-disclosure agreements will even make sharing impossible. But one beneficial aspect of a standardised framework is that there is no need to release all, or any of the information that leads to the general warning. In some cases, the mere fact that an operation has been detected may also be classified, but there would still be many cases where it would be possible to offer a warning based on secret indicators. The evidence for the categorisation does not need to be revealed in its entirety. This fact gives CND actors a metalanguage to discuss problems without needing to get so specific with details that they in reality
are revealing what sort of information they possess. This framework can therefore contribute towards sharing in a constructive but responsible way.

The fourth research question is in what way can the current national cyber defence model be improved regarding timely and sufficient information sharing? There is no question that manual assessment in every part of the analysis chain will generally give a higher quality prediction than automated generalisation will. However, the time lost in conducting these manual processes make the timely reaction to an operation extremely challenging or impossible. Whereas automation may not even put the actual scenario higher up than top three nominations in a standardised framework, it still puts the scenario “on the table”, it helps prioritise further analysis, and it simplifies the warning of involved stakeholders in a predictable, straight-forward way. With a manual assessment and conclusion, a warning may typically look like “your company is probably subject to a fraud attempt through phishing, but we also have concerns it may be something more serious”. With an automated framework, it would be possible to say that “there is activity towards your systems, and one of the top three scenario descriptions based on the existing evidence is state-sponsored corporate espionage. We have so far been unable to disprove that hypothesis”.

Analysts should not have the privilege of becoming biased to their first assumption, and a set of nominations forces them to consider alternatives. Also, the understanding of network operations needs to take place not only among cyber analysts, but also among a variety of other stakeholders and decision-makers. A modularised and standardised framework can help achieve this.
14 Summary and further work

“A camel is a horse designed by a committee”

- Sir Alec Issigonis, designer of the Mini Morris

This thesis describes a project that has investigated strategic challenges regarding computer network defence, including the design of a framework for more automated detection and warning solutions at the national level.

The complexity involved is two-fold. The subject matter itself is generally perceived as inaccessible for anyone not working within the field, and the amount of dependencies is both broad, deep and dynamic across many layers of technology and aspects of society. For these reasons the design and implementation of efficient and automated computer network defence solutions requires the collaboration of many sectors of government and stakeholders in industry, few of which have even the prerequisites to understand the complete picture and the magnitude of the challenge. Consequently, results within cyber defence solutions are generally the most mature in cultures with more autocratic regimes than Western democracies such as Norway. This framework has attempted to address this challenge by presenting a predictable assessment of an advanced network operation in a quantifiable manner, allowing easier standardised and unified implementation in detection and warning systems.

The thesis has described factors relevant to the usability of advanced network operations, namely attribution complexity, low risk and low cost. It has described how intent can be derived from the understanding of operations and targeting, and what gains can be made. The limited appearance of network operations to support conventional military operations has been discussed, and a brief timeline of national cyber defence development in Norway has been examined. Further, the roles and responsibilities played by both government and infrastructure owners has been described.

The thesis has presented national cyber defence mechanisms in place in Norway today in a simplistic manner, but in such a way as to examine potential for development in existing solutions.

The suggested framework to address some of this potential is based on three elements: the actor, the operation and the intent. Through a general classification scheme the framework can supply
analysts with a valuable tool in assessments and information sharing, by ranking the possible outcomes in each case according to existing evidence and available intelligence.

The understanding of the actor is based on the kill chain approach to technical indicators and evidence, as well as traditional intelligence analysis and a generic description of the actor type and potential.

The understanding of the operation is based on traditional actor interests, actions on target, and a classification of the target/targets.

The intent of the operation or campaign is based on the above factors as well as the strategic context of the operation – the relationship or conflict type and level between two states or entities.

Based on an automated nomination of most likely scenarios, the detection, understanding, contextualisation and warning of network operations will require significantly fewer manual steps than presently, as well as suggest an order in which to disprove possible hypotheses surrounding an advanced network operation or campaign.

This project has not examined existing national solutions to cyber defence in a comprehensive manner. The purpose of the project is to focus on the potential of a unified national approach to the phenomenon, and suggest a direction for further standardisation and improvement of efficiency.

The framework presented in this thesis has a strong focus on understanding actors and conflicts at or associated with the state level. Ideally, an implemented model would entertain other types of threats and scenarios to an even larger extent.

The thesis does not detail an implementable model. The amount and complexity of interfaces between systems alone would likely be a task requiring years of studies, but even as an independent model this framework would require significant further detailing. The design of an actor database, the weighting of indicators, the connection to physically manifested threat actors and agencies, the classification of all relevant targets within a country and a complete table of intent most likely all qualify as separate projects or programs of study.

Although this thesis does not present implementable solutions at any level, hopefully it can direct attention towards some of the overall needs in national cyber defence, guide further work within some of the more detailed fields, and inspire the development of cyber defence infrastructure, governance, processes and communication that will help swing the pendulum more towards the
targets of advanced network operations, rather than the threat actors behind them.
15 References

https://www.nrk.no/norge/minnebrikken-gjor-folk-til-spioner-1.6806957

https://www.nrk.no/norge/vurderer-a-politianmelde-nodnettskandalen-1.1336777

http://folk.uio.no/josang/papers/BJE2016-STIDS.pdf


http://www.economist.com/node/12673385


Muncaster, Phil (2013). 'India attacked Norwegian telco to get at Pakistan, China’ – report. Theregister: Published on www.theregister.co.uk. https://www.theregister.co.uk/2013/05/21/hangover_india_apt_discovered/


https://spectator.org/36718_chinas-cyber-militia/