**FINNISH NATIONAL DEFENCE UNIVERSITY**

# KNOWING ME, KNOWING YOU
## National Cyber Security Situation Understanding Within a Network of actors

Master's Thesis

Niklas Nykter

SM 7
National Security

April 2018

**FINNISH NATIONAL DEFENCE UNIVERSITY**

| Course<br>**Masters of Military Science 7, Interagency Co-operation** | Programme<br>**National Security** |
|---|---|
| Author<br>**Niklas Nykter** | |
| Thesis Title<br>**Knowing Me, Knowing You - National Cyber Security Situation Understanding Within a Network of Actors** | |
| Major<br>**Leadership** | Repository<br>**National Defence University Library** |
| Date:<br>**April 2018** | Pages Appendix Pages<br>**64** **1** |


**ABSTRACT**

This thesis studies the emergence of Shared Situation Understanding within the context of National Cyber Security among a network of actors. Cyber Security is a key enabler of continuity and resilience for functioning of ICT infrastructure, upon which many societal functions are built. In the modern globally networked world, national cyber security is under threat from national actors, criminals, misuse and other issues.

Situation Awareness is today accepted as a key part of any cyber security operation, but how does Shared Situation Awareness emerge within the national cyber security context? This thesis looks at the Situation Awareness of different actors, how they produce Situation Understanding and how this information is then shared within the network. Main question for this thesis is: how does Shared Situation Understanding emerge from these networks? Empirical research was conducted via interviews of national cyber security actors, three of which represented the governmental actors and three the private sector. Their cyber security frameworks, Situation Awareness-function and Situation Understanding-processes were assessed.

The national cyber security networks have some information sharing operations functional, but there is limited information exchange. Sharing of SA-level information is somewhat effective, but there is limited sharing of SU-level information Especially between the private organizations information sharing is limited, most successful sharing is done via a central governmental node. There should be more emphasis on information sharing framework definition, ways of working and understanding of private organization incentives to join and work within such networks.



KEY WORDS:

Cyber, cyber space, cyber threat, cyber security, national cyber security, situation awareness, situation understanding, shared situation awareness

**MAANPUOLUSTUSKORKEAKOULU**

| | |
|---|---|
| Kurssi<br>**Sotatieteiden maisterikurssi 7, viranomaisyhteistyön koulutusohjelma** | Linja<br>**Kansallinen turvallisuus** |
| Tekijä<br>**Niklas Nykter** | |
| Tutkielman nimi<br>**Kansallinen kyberturvallisuus – Tilanneymmärrys toimijoiden verkostossa** | |
| Oppiaine johon työ liittyy<br>**Johtaminen** | Säilytyspaikka<br>**Kurssikirjasto (MPKK:n kirjasto)** |
| Aika<br>**Huhtikuu 2018** | Tekstisivuja Liitesivuja<br>**64** **1** |


**TIIVISTELMÄ**

Tämä Pro Gradu -tutkimus käsittelee jaettua tilanneymmärrystä kansallisen kyberturvallisuuden verkostoissa. Nykypäivän verkottuneessa ja globaalissa maailmassa kyberturvallisuus on yksi toimintavarmuuden tae. Uhkia ja haavoittuvuuksia vastaan suojaudutaan kansallisesti verkostossa, jossa on sekä kansallisia että yksityisiä toimijoita verkostoissa.

Tilannekuvaa pidetään nykyään yleisesti yhtenä avaintekijänä tehokkaan kyberturvallisuustoiminnan luomisessa, mutta miten tilannekuvatietoa jaetaan kansallisen kyberturvallisuuden verkostoissa? Tämä tutkielma pyrki tutkimaan tapoja, joilla toimijat ensin tuottavat omasta tilannekuvastaan tilanneymmärrystä ja jakavat näitä tietoja kansallisissa verkostoissa, kansallisen jaetun tilanneymmärryksen tuottamiseksi. Tutkimus toteutettiin kuuden kansallisen kyberturvallisuuden verkoston toimijan haastatteluina, joista kolme oli kansallisia toimijoita ja kolme yksityistä organisaatiota. Haastatteluissa käsiteltiin heidän kyberturvallisuuden toimintakehikkoa, tilannekuvaa, -ymmärrystä sekä toimintaa verkostoissa näiden tietojen jakamiseksi.

Kansallisissa verkostoissa jaetaan jonkin verran tietoa, mutta varsinainen tiedonvaihto jää vähäiseksi. Tilannekuvaan liittyvää tietoa jaetaan, mutta tilanneymmärrykseen liittyvää tietoa hyvin paljon vähemmän. Erityisesti yksityiset yritykset eivät juuri jaa keskenään tietoa, vaan jakaminen tapahtuu verkoston keskiössä olevan kansallisen toimijan kautta. Huomiota tulisikin kiinnittää tiedonjaon toimintakehikon määrittelemiseksi, toimintamallien luomiseksi sekä yksityisten yritysten kannustimien ymmärtämiseksi toimivan tiedonvaihdon aikaansaamisessa.



AVAINSANAT

Kyber, kyberavaruus, kyberuhka, kyberturvallisuus, kansallinen kyberturvallisuus, tilannekuva, tilanneymmärrys, jaettu tilanneymmärrys

## TABLE OF CONTENTS

# NATIONAL CYBER SECURITY – SITUATION UNDERSTANDING WITHIN A NETWORK OF ACTORS

## 1 INTRODUCTION

Three major dimensions have been added to the definition of warfare and the battlefield over the last few decades: (1) space, (2) electromagnetic spectrum and (3) minds (in terms of information and psychological warfare). The integration of battlefield systems into a single, overarching master-system, has inducted the battlefield troops as part of the cyber space as well. This kind of system of systems is a prime target for an attacker possessing cyber-attack capabilities and provides a single point of failure for all connected systems. Thus, understanding cyber and being able to protect systems connected to it is essential, not only for the battlefield troops, but specifically the command and control functions. (Sirén, 2011, Kosola & Solante 2013.)

Beyond the battlefield, these developments pose challenges to the protection of civil society. As we are witnessing a brave new world built on communication networks and computers, the cyber space is increasingly plagued by DDoS-attacks, ransomware, malware, cyber espionage and data breaches. Monitoring and protecting the cyber security is becoming a crucial part of national security, especially in terms of the value of continuity and preparedness for upkeeping the functions of society. A society that cannot protect its cyber infrastructure, is vulnerable to a number of cyber-attacks; ranging from the activist hackers wreaking havoc just for show to nation states trying to undermine the democratic stability of a neighbour. At the same time a realization is emerging that technical solutions by themselves cannot offer complete protection, but rather the answer to the cyber conundrum lies in cooperation, communication and a functioning network of public and private actors (Lehto, Limnéll, Kokkomäki, Pöyhönen & Salminen, 2018, 14-15).

Compared to the times before far reaching information technology emerging in the society, national security was almost fully directed and ensured by the state. The army, stockpiles and reserves are just a few of the mechanisms that nation states used to manage the national security. While the need for cooperation grew as nations moved toward modernity, the current digital infrastructure is previously unseen in its complexity. In Finland, the aim of the Cyber Security Strategy is the ability to protect the essential functions of society from cyber-attacks in all circumstances. The tools to manage this are speed, transparency and co-ordination between actors. At the same time, the strategy acknowledges the fact that cyber security is a networked function, consisting of governmental, private and NGO-actors, who all must be committed to common goals and follow mutually agreed ways of working. (Finnish Government, 2013.)

## 1.1 Background

> *"The complexity, effectiveness, and capability of cyber-attacks is growing faster than the defensive capabilities."*
> Lehto & Limnéll (2017, 180)

To get the deteriorating situation under control, national and private actors need to be able to understand their current status, to identify weaknesses within the systems and understand threats to their own operations. On a national level, a common understanding must be created, to provide a baseline for development, information sharing and directing actions. Only when you understand your current plight, can you truly focus efforts to correct them. Whether it be on a national or organizational level, situation awareness is key to long term improvement in cyber security.

The first problem that arises is the unclear definition of cyber security, especially on the national level. As national security has evolved, less of the infrastructure and functions that require safeguarding are in the hands of national governments. Rather, private infrastructure has expanded and even personal devices need to be included within the scope of modern national cyber security. How can a government secure infrastructure, devices and functions that are not in its direct control? One recent trend, seen in cyber security, but encompassing other fields as well, is the explosion of regulation. But surely, there must be more that can be done? The facilitation of cooperation and building of trust between competitive areas is something that the government is in prime position to manufacture.

But the question is how? In Finland, plenty of resolutions and strategies have been produced in the field of cyber security relating to the nation state: different security strategies, cyber security strategies and implementation programmes. However, results are yet to provide much comfort. The research project by Lehto, Limnéll, Innola, Pöyhönen, Rusi and Salmela (2017) paints a picture that is less rosy than the usual proclamations of Finland as a global leader in cyber security. The project team concludes that there is no shared situation awareness for cyber security on a national level, in addition co-operation is rather sporadic and remains siloed both in different fields of governmental functions as well as different private sectors. (Lehto et al., 2017.)

When you state your aim to be a global leader, but end up lacking behind every selected western peer, something is awry (Lehto et al., 2017, rank Finland far below the top in their study of cyber security capabilities). The challenge for cyber security is the bridging of high-minded visions and goal statements with the nitty-gritty of everyday work to ensure security of cyber space. Obviously, when it comes to development actions one big enabler is money, but one would venture a more efficient use of current capabilities and resources could provide leaps in overall ability in cyber security. Especially fostering co-operation and providing safe spaces for information exchange, best practices with the governmental seal of approval and assertions of confidentiality might have big effects overall.

This thesis takes on these themes head on, first through looking to understand what cyber security is and what it means for a nation state. The republic of Finland will act as our frame of reference and research case. Finland began the great cyber leap forward in 2014 by unveiling the national cyber security strategy and other initiatives. This development has not built the expected momentum, however, as the recently published research by Lehto et al. (2017) reveals. The grandiose aims of Finland as the front runner of cyber security in the world have been dampened by a dose of reality, as investment efficiency and coordination do not seem to be on a level that would provide leverage for a small nation to be able to reach beyond its limits. Once we have clarity of what one understands by cyber security and what it means within a national context, we move on towards situation awareness and understanding. To understand the national cyber security network, this thesis takes a view of situation awareness and understanding and what they mean in the context of national cyber security.

## 1.2 Research aims

This thesis has two major guiding principles: (1) what is cyber and cyber security, (2) situation understanding. Looking at these two principles, we aim to provide a look at what cyber security is from a national point-of-view and how in that context can you build situation understanding. After looking at these two concepts from a theoretical point of view, the theory is then tested via themed interviews of national cyber security actors. Finally, we combine the theoretical and empirical views to draw conclusions and provide discussion on the topics

The main research question that this thesis aims to answer is:

- How does situation understanding form in a network of national cyber security actors, through shared situation awareness and understanding?

Supporting research questions are:

- What is situation understanding composed of within the context of national cyber security?
- How does situation understanding arise from situation awareness?

# 2 METHODOLOGY

This chapter will present the study methodology and the two theoretical models, that were used as the guiding principles in this thesis. The study will consist of the theory building using an abductive content analysis and the empirical research conducted via themed interviews. The theory will be built on two distinct parts: (1) the concept analysis of cyber and (2) the current research of situation awareness and understanding through a literature analysis. The interview themes will be built on the guiding principles and the theoretical understanding built from the literature analysis.

The first of the guiding principles presented as the theoretical background is the concept analysis of cyber security presented as background for the whole study in chapter 3.1, the view of cyber and its sub-concepts is based on two different collections of sources: (1) on scientific literature and (2) the formal documents of the Finnish Government on the issue. A synthesis on the views is presented as a conclusion of the chapter that will guide the study throughout as a context.

The second guiding principle is our view on situation understanding, that will be provided by two main theories on situation awareness and how it can be leveraged in cyber context. The two guiding theoretical views are: (1) Endsley's (e.g. Endsley 1988, 1993, 1995) view on pure situation awareness and (2) Boyd's (e.g. Boyd 1986, 1987, 1995) OODA-loop on decision making. This view was then tested through as a case study by conducting themed interviews with six national cyber security actors. The interviews were analysed through the prism of the theoretical view of Situation Awareness (SA) and Situation Understanding (SU).

## 2.1 Qualitative Case Study

The study used qualitative research methods to build a theoretical view of the concepts of cyber security and situation awareness. Qualitative research aims to look at the research problem from many angles and to represent real life concepts through theoretical analysis. The aim is to ask "why?" relating to the research topic in addition to asking "what?". Why does the phenomenon happen and why is it important? (Hirsjärvi, Remes & Sajavaara, 2015 & Alasuutari 1999.)

The aim of qualitative research is to understand the subject of the research, rather than to map direct universal causality between phenomena. The subjects of the study are natural actors and the research is conducted in a space, where all functions cannot be controlled. The results provide understanding behind the phenomena, rather than strict scientific conclusions ready to be tested. The case study as a method will provide deep understanding into the phenomena and dynamics and factors within a certain phenomenon. The benefits of a case study are its flexibility and consideration of context. A case study aims for a holistic understanding and usually will provide new questions to base further inquiry on. (Hirsjärvi et al., 2015, Rantapelkonen & Koistinen, 2016.)

In the scope of this thesis is to understand how cyber security and national cyber security are defined by research and the Finnish government. The aim of the empirical research was to test the theoretical view of cyber security within the network of national cyber security actors. What happens in this network of actors, when the aim is to build situation understanding with the aim of preserving and improving national cyber security? As the basis of our case study, we built an understanding of the concept of national cyber security, then through the interviews a sample of this network of national cyber security actors was used as he case study sample.

## 2.2 Abductive Content Analysis

According to Peirce abductive reasoning is based on the value of the guiding principle, while his model of logic is itself based on the belief that facts, or practical experience, are always logical and experience itself cannot be doubted. Only the presentation of experience on a general level can be doubted; the presentation of experience is always logical or un-logical. According to this line of thinking, logic is independent from deduction, which can be based even on vague intuitive assumption, but also from facts themselves and behaviour which are always logical. Pierce states that when analysing collected material using abductive method, one mustn't look to "abduct" all phenomena or processes, but rather rely on the inherent ability of humans to come to the right conclusions, even intuitively. Intuition cannot, however, function as a source of information, rather fundamental categorization is required. (Peirce, 1931-58, Peirce, 1958, Feibelman, 1960.)

Abduction as a concept is related to induction and deduction, abduction means to look for a meaning from observed phenomena. Abduction itself does not produce new information, but acts as a way to track down information. Abduction is proven to be correct, when the phenomena is examined and the conclusion is that the issue is as claimed. The thought process of the student ranges from content analysis to existing models, with the student combining these points of view, sometimes in very creative ways. When taking an abductive approach, the experience based knowledge of the student is brought out through creative, intuitive hypothesis, that is examined by the student. Abductive approach looks for alternative points of view and additional information acquired through these views. (Grönfors, 2011, Tuomi & Sarajärvi, 2002.)

The theoretical background content was analysed through abductive content analysis, where previous theory acts as a guiding principle for the study (Peirce, 1958, 96-97), here our two main theoretical views will act as the guiding principles: (1) concept analysis of cyber and (2) Situation awareness and understanding research. The aim was to study the theories behind situation awareness and understanding and based on these theories look to build a view on what SA and SU are in the context of national cyber security, based on our other guiding principle of cyber security. This view was then tested through themed interviews of actual stakeholders of national security to validate the view.

The second guiding principle consists of the two main theories on situation awareness and understanding by Mica R. Endsley's model of Situation Awareness (e.g. Endsley, 2000) and John R. Boyd's OODA-loop model (e.g. Boyd, 1987). The two models map together as analysed in chapter 3.2. and complement each other in ways that are beneficial to the scope of this study. The guiding theories are complemented by a look at situation awareness and understanding within a network of actors and then by bringing the situation awareness and understanding view to the cyber realm, looking at SA within a cyber-context.

Abductive research will always have uncertainty factors built into it, as the analysis is based on the intuition and conclusions of the student. We will look to confirm the theoretical views via information gathering through themed interviews. The interview structure was based on the structure of the theoretical background and this structure was also used in the analysis and codification of the interview data. This analysis and codification provide reliability and validity to the study. (Rantapelkonen & Koistinen, 2016.)

## 2.3 Theme Interviews

The empirical data was gathered through theme interviews of current national cyber security actors and how situation awareness is constructed within this network of actors. The interview themes were based on the theoretical understanding of national cyber security and the model of cybersecurity situation awareness, with the aim of validation of the view based on theory in the real world. Theme interviews are based on loose themes, that stem from theory. These themes were covered with the interviewees without strictly restricting the flow of the interviews or conversations. As such, themed interviews leave a lot of flexibility to the conversation and can provide significant insight into the phenomenon under study. (Hirsjärvi et al., 2015.)

A themed interview assumes that the interviewee has experienced the phenomenon that is under study, as such he is a prime candidate for the interview. The interviewer must also have a deep understanding of the issue at hand, to be able to guide the interview and enable the interviewee to articulate his views and provide real insights. The interview is based on pre-selected themes that the interviewer has constructed upon his knowledge of the phenomenon. All interviews within the study were based on the same themes, but the actual interviews differed in scope, order and language used. These differences may provide insight to the student of the phenomenon in addition to the actual answers given within the interview. (Rantapelkonen & Koistinen, 2016.)

# 3 GUIDING PRINCIPLES

The abductive study of this thesis is guided by two main theoretical concepts: cyber security and situation understanding. These theoretical concepts are presented in depth in the following chapters. The guiding principles guide the research within the whole of this thesis, having had influence in everything related to the research, from the first tentative steps browsing through previous research to the theme interviews and discussion that were had with the interviewees. Finally, the results of the interviews are broken down according to the guiding principles and the research material collected through the interviews is analyzed based on the theoretical concepts of cyber security and situation understanding.

## 3.1 Cyber

We will begin by asking the question “what is cyber security?”. The answer will be provided by two distinct views: (1) a concept analysis of cyber security based on existing research and current literature, and (2) cyber security based on formal national security strategy of society, cyber security strategy and the implementation programme of the cyber security strategy from the Finnish government. Our aim is to understand whether the national point of view encompasses all that the current research understands by cyber security, what are the possible gaps and how they affect the building of situation awareness of national cyber security.

As Limnéll, Majewski and Salminen (2015, 29) state: the separation of the digital and physical realms in the world today is nearly impossible and thus the definition of cyber security in an exhaustive manner proves challenging. Cyber as a prefix alludes to the digital world, but as the digital and physical converge, it is difficult to make a clear distinction between the two. The importance of a common view of what is and what is not cyber security. This view is essential to provide a platform for cooperation and common functions, especially when the network requires private and public entities to function together.

### 3.1.1 Cyber Security – Research and Literature

There is no single definition of cyber security or related concept that would be globally accepted at this time. Depending on the source, cyber is seen as a prefix defined by what comes after it or as a definitive article, defining the concept that comes after. This chapter will gather and analyse different definitions of cyber and related concepts, to form an understanding which will be used within the scope of this study.

**Cyber**

Limnéll et al. (2015, 29-30) state that cyber is rarely seen by itself, but rather used in combination with a defining concept, more as a prefix or an adjective. For them prefix defines the realm as being "of cyber" and the following term determines the action or function. The United Kingdom Ministry of Defence (2016a, 3) defines cyber: "to operate and project power in and from cyberspace to influence the behaviour of people or the course of events". By this definition cyber is seen as the origin term, rather than just a prefix that requires a definitive term to follow. For the UK Ministry of Defence, the other terms, such as cyber space, -threat and security accrue their meaning form the prefix, for Limnéll et al. (2015), it is the other way around. The end result, however, is the same for both methods, as the following concepts and their analysis shall show. The term cyber within this study means to relate to the cyber space.

**Cyber Space**

Most attribute the emergence of the term cyber space to William Gibson's 1984 classic science-fiction epic "Neuromancer", where it was described as *"A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data."* One cannot avoid being struck by the prescience of Mr. Gibson's vision, it seems to describe the current infrastructure to a t. Even if the particulars have evolved beyond his vision, the basic image of complexity and abstraction rings true. (Gibson, 1984.)

Earlier views of cyber space viewed it as a technical concept, for example the National Security Presidential Directive (NSPD) 54 from the Obama White House from 2008 definition is as follows: "Cyberspace means the interdependence network of IT infrastructures, and includes the Internet, telecoms networks, computer systems, and embedded processors and controllers in critical industries" (NSPD 54, 2008, 3). This view has greatly expanded in the intervening years, an absolutely critical addition is the social domain of cyber space, for example the US Army (2010, 8-9) based its view on cyber space on computers (including programmable units) and the connections between them, but added the virtual dimension formed by the interlink of those computers. The United Kingdom Cabinet Office (2011, 11-13) duly followed suit and referenced cybers space as a virtual domain, where individuals can interact with one another, leading to the exchange of ideas, information sharing, providing social support and trade among other things by using the global network.

NATO Cooperative Cyber Defence Center of Excellence (Klimburg, 2012, 8-9) defines cyber-space as something more than just internet and connected systems, hardware, software and information systems, as having a social component, including people and their interactions as well. Robinson, Disley, Potoglu, Reding, Culley, Penny, Botterman, Carpenter, Blackman and Millard (2012, 56-58) view cyberspace as reflecting partly a human construct, partly natural and partly informational constructs, but also as having a strong physical nature that reflects locality. As such the view on cyber space must be built on physical (i.e. the physical machines, devices and systems), logical (i.e. the virtual systems and their functions etc.) as well as social (i.e. the interactions of humans) domains. Rantapelkonen and Salminen (2013, 7) point out that actions in the cyber space are mostly run and managed by individual people and private organizations, that it isn't controlled by states. International organizations haven't been able to exert much influence on control activities within the domain.

A widely accepted model of cyber space is the three-dimensional model by Libicki (2007, 8-9), that separates cyber space into three separate, but interlinked domains. The three are: (1) physical layer (servers, wires, routers etc.), (2) syntactic or logical layer (software, protocols etc.) and (3) semantic or cognitive layer (information and ideas). The logical layer is usually today expanded to include the social aspects of cyber space, especially in relation to hybrid warfare (Lemieux, 2015, 22-23).

The US Army (2010, 8-12) divides the functions related to network and spectrum operations into three dimensions:

- Contest of Wills i.e. psychological operations against implacable foes, warring factions or potential adversaries
- Strategic engagement i.e. keeping friends at home, gaining allies abroad and keeping up support for operations
- Cyber-electromagnetic contest i.e. the dimension consisting of convergence of the wired, wireless and optical technologies

The US Army model third dimension is clearly what we understand as the cyber space, but reminding us that there are other dimensions to cyber security as well. (US Army, 2010, 8-12.)

Going further the US Army uses a very similar definition for cyber space as Libicki (2007), but defines the third dimension as Social layer, composed of the persona and cyber persona components (US Army, 2010, 9). The social layer focuses more on persons identification (e-mail, IP Adress etc.) information to add a human element into the cyber space conundrum. As such, the US Army differs from Lemieux (2015, 22-23) model, by attaching the social aspect to logical layer.

| **Physical Layer** | **Logical Layer** | **Social Layer** |
|---|---|---|
| Geographic Components  Physical Network Components  | Logical Network Components  | Persona Components  Cyber Persona Components  |

Figure 1. Cyber space concept model according to US Army (Adapted from US Army, 2010, 8.)

Within this study, the definition of cyber space will follow the US Army model, as a combination of three layers: (1) physical (servers, wires, routers etc.), (2) logical (software, protocols) and (3) social & cognitive (identities, information, ideas etc.).

**Cyber Threat**

According to Lemieux (2015, 19) the origins of cyber threats are caused through the complexity of information systems, that "…create unexpected vulnerabilities that human agents can use to make computer systems operate in unintended ways". Kärkkäinen (in Vankka, 2013, 13-14) expands the two major ways for cyber threats to emerge in a cognitive network context: The view is that threats can emerge from systems itself, i.e. software vulnerabilities or process vulnerabilities that outside agents are able to exploit. On the other hand, threats can emerge from the outside agents, through attack methods, for example man-in-the-middle attacks. The may also be threats that combine the two, i.e. an outside agent exploiting a vulnerability.

The US Army (2010, 13-14) categorizes cyber threats in many ways: (1) by sponsorship, (2) training, (3) education, (4) skills, (5) motivation, and (6) tools. For example, an advanced cyber threat can be sponsored by a nation-state and have advanced education. "The level of cyber threat is the combination of the actor's ability (skills and resources), opportunity (access to target), intent (attack, surveillance, exploit), and motive (national policy, war, profit, fame, personal reasons, and others)". (US Army, 2010.)

**Cyber-attack**

Defined by Chapple & Seidl (2015, 5-6) cyber-attacks are offensive acts that aim to cause physical or electronic damage by non-kinetic means. They also separate cyberwarfare into cyber-attacks and cyber espionage, where the aim is to steal sensitive information. Cyber warfare consists of the above offensive actions as well as defending yourself against the adversary's attacks.

Goldsmith (in Lemieux, 2015, 52) defines a cyber-attack as "an act that alter, degrades, or destroys adversary computer systems or the information in or transiting through those systems". He also differentiates cyber exploitation form an actual cyber-attack, where exploitation involves no disruption, but rather just the monitoring and related espionage on computer system and the copying of this data. One wonders whether this differentiation is necessary, as the owner of the stolen data, that is essential to the computer system or its user, might not see the bright side of the lack of an attack upon his system. Rühle (in Friis & Ringsmose, 2016, xi-xii) raises an important view of cyber-attacks: while in physical world kinetic attacks are visible, in cyber space intrusion may go unnoticed for any length of time. As such cyber-attacks may turn out to be the first shots fired in any conflict, maybe years before escalation into the physical realm.

We can define a cyber-attack as any purposeful action aimed at intrusion or exploitation of cyber infrastructure.

**Cyber Security**

Friis and Ringsmose (2016, 2-3) explain the difference between information security and cyber security through an example: "*... Edward Snowden's publication of sensitive documents from the NSA database is a breach in information security, not cyber security. However, had the same documents been stolen through an online attack on NSA's servers, it would qualify as a cyber-attack."* The difference can be articulated as using cyber domain as it is supposed to work, i.e. Snowden had access to the documents, he was allowed to handle them, but the breach happens when he discloses them to an unauthorized party. No misuse or attack on cyber domain itself, but rather on the contents, i.e. information.

The Telecommunications Standardization Sector of International Telecommunications Union (ITU-T) Study Group (2008, 6-8) defines cyber security as the collection of tools, policies, security concepts and safeguards, guidelines, risk management approaches and actions, training, best practices, assurance and technologies that are used to protect the organisation's infrastructure and information related to the cyber space. This list includes roughly the same items as a definition of information security, but the difference between cyber and information comes from the domain that they relate: cyber security focuses solely on the organizational and user's assets that are within the cyber domain, i.e. the connected computing devices, information within them, infrastructure, applications, services, telecommunication systems, users, and the totality of transmitted and/or stored information in the cyber environment. (ITU-T Study Group, 2008.)

Andress and Winterfield (2014, 30-32) define cyber defence as a collection of information assurance, computer network defence, incident response and critical infrastructure protection, with the aim of preventing, detecting and responding to outside actor's attempts to deny or manipulate information and/or infrastructure. In this context cyber defence is seen as a subdomain of cyber security. Following from the above definitions that see cyber as a three-level domain, we must add social defence into this view, which consists mainly of training and awareness of cyber users.

We can define cyber security according to literature as the actions with the aim of safeguarding the function and functionalities of the cyber domain. These include governance (e.g. frameworks, guidelines, instructions), physical (e.g. protective cabinets, locks), logical (e.g. firewalls, virus protection), processes (e.g. monitoring, incident response) and social (e.g. training and awareness).

### 3.1.2 Cyber Security – Government Publications

Kaufmann (2013, 53-55) sees networking and being connected as integral to modern societies. This view has in the 2010s emerged as key component for modern nations, where it has emerged as one of the vital functions of modern society. This extends the view of national security towards the virtual world and has brought cyber security within the scope on national actors. National security, however, is not a clear concept, changing with the times and evolving nation states. A classical view stemming from the French revolution defines security for the individual as feeling free from the prospect of personal violation, a very private view of security. As nations evolved, the concept of national security grew to include the responsibility of the state to protect the individual and their rights. As such, the national security can be defined as the protection of the individual and his rights from all sudden and violent acts, internal and external, by the nation state. (Rothschild, 1995.)

Baldwin (1997, 5-6) finds the concept of national security as dangerously ambiguous, with the definition varying based on the needs of the definer. Wolfers (1952, 483) in his classic definition of security as "the absence of threats to acquired values" leaves a lot to interpretation, Baldwin (1997, 13) formulates this as "a low probability of damage to acquired values". National Security viewed this way can have no comprehensive definition, but rather provides a framework for a nation to define its values and build its own concept of national security. In this light, the notion of national security depends on both constitutional law and current legislation and statues of an individual nation, based largely on the current beliefs and values of the state. These beliefs are obviously in constant flux, so any definition needs to be examined as a moment in time.

The Constitution of Finland (1999/731) declares as the individual rights, among others, equality, the right to life, personal liberty and integrity, freedom of movement, the right to privacy, freedom of expression and right of access to information, electoral and participatory rights, protection of property and the right to work and the freedom to engage in commercial activity. This declaration, combined with the above definition of rights, forms the basis of Finnish national security. These are the rights and values that are to be protected from threats by the government. For a more in-depth look at how the nation state of Finland comprehends cyber security, we will take a detailed look at four governmental publications:

- The Strategy for Securing the Functions Vital to Society (2006)
- The Security Strategy for Society (2010, updated 2017)
- Finland's Cyber Security Strategy (2013)
- Implementation Programme for Finland's Cyber Security Strategy for 2017-2020 (2017)

**The Strategy for Securing the Functions Vital to Society**

The Strategy for Securing the Functions Vital to Society form 2006 summarises that the three dimensions of functions vital to society are national sovereignty, the security of society and the livelihood of the population in all situations (Finnish Government, 2006).

A more holistic view of the vital functions is as follows (Finnish Government, 2006):

- Management of Government affairs
- International activity
- National military defence
- Internal security
- Functioning of economy and infrastructure
- The population's income security and capability to function

- Psychological crisis tolerance

A quick analysis of this list produces aspects (national, international, technical, social) and actors (military, police, emergency services, governmental, private sector). National security in Finland is viewed as a holistic system, that involves all of society. National security strategy for society (Finnish Government, 2010) views the effort of upholding national security as a cooperative task, led by the government, but carried out in collaboration by governmental actors, national and local institutions and private sector.

Due to the age of the document, cyber security or risks do not play a big part of the strategy. However, we can clearly see that all the functions deemed vital have a cyber component and quick analysis will tell us, that almost none can be achieved without cyber security in the year 2017. Governmental affairs, military and economy and the income security of the people all run on IT-infrastructure and havoc may be wreaked upon them by cyber means exclusively. Fortunately, these lapses due to aging are addressed in the following documents.

Interestingly, the threat scenarios presented in the 2006 strategy paper do not include information security or cyber security at all. Rather, the strategy talks about disturbances against telecommunications or information systems. This shows the rapid evolution of cyber threats from 2006 to 2017. (Finnish Government, 2006.)

**The Security Strategy for Society**

Originally published in 2010 and recently updated in 2017, the Security Strategy for Society provides the guidelines for governmental entities, both national and local, for safeguarding national sovereignty and territorial integrity, based on comprehensive view of security for all society. The main view of the strategy is to detail the vital functions of society, threat scenarios for these functions and tasks of preparedness and crisis management for the different actors. The document takes the functions listed in 2006 and updates them:

- Management of Governmental Affairs
- International Activity
- Finland’s Defence Capability
- Internal Security
- Functioning of Economy and Infrastructure
- The Population’s Income Security and Capability to Function
- Psychological Crisis Tolerance

The differences between 2006 and 2010 lists of functions are superficial, rather based on different grouping of issues than true changes in the vital functions. This shows that while the world has changed plenty around us, the functions of the nation state have remained. Major changes, however, can be found in the threats articulated in the strategy. The emergence of cyber threats means that they are explicitly mentioned as the cause behind telecommunications and information systems major disturbances. The update of 2017 focuses the functions more, but the differences between the strategies are superficial. The main change relating to this study is the addition of preparedness to the functioning of the economy and infrastructure, an important addition regarding cyber security preparedness. (Finnish Government, 2010, 2017.)

The strategy states the functions to ensure preparedness and functionality of the infrastructure as the strategic tasks of governmental actors. The critical functions of telecommunications must be secured and a basic level of security must be mandated by national regulation. The Situation awareness of the critical infrastructure is based on common criteria and must function continuously. (Finnish Government 2010.)

The strategy lists the following items, that can be understood as relating to national cyber security:

- Governmental Situation Awareness Office
- Connections to Foreign Nations and International Organisations
- Military Defence of Finland
- Security of Emergency Services
- Functioning of Financial Infrastructure
- Functioning of Communications Infrastructure
- Functioning of Governmental IT Infrastructure
- Crisis Management and Situation Awareness
- Emergency Communications

In modern society, almost all the functions in the strategy run at least partly on ICT-infrastructure, and as such can be affected by cyber threats. Those listed above are the ones explicitly within the cyber realm and in the scope of this thesis. (Finnish Government, 2010.)

The above strategies form the basis for governmental cyber security strategy and the implementation programme, analysed below. The above documents and analysis create a framework for functions and actors as well as actions that need to be safeguarded by effective national cyber security, i.e. the documents present an asset identification of sorts, the crown jewels to protect. When it comes to actual cyber security or actions thereof, we need to take a closer look at the cyber intensive documents.

**Finland's Cyber Security Strategy**

Published in 2013, Finland's Cyber Security Strategy extends the framework of the previous publications to the cyber domain. The start is promisingly succinct (Finnish Government, 2013, 1):

> "*Cyber security means the desired end state in which the cyber domain is reliable and in which its functioning is ensured."*

Here we have a definition of cyber security by the government: a functioning cyber domain. The cyber domain is defined as (Finnish Government, 2013, 1):

> "*... interdependent, multipurpose electronic data processing environment..."*

Finland's cyber security vision is based on safeguarding the vital functions of government presented in the previous chapters. These functions are to be secured from cyber threats in all situations. Additionally, a safe cyber domain is a competitive advantage for authorities and businesses. The goal is to be a global forerunner in cyber threat management and handling of disturbances caused by these threats. (Finnish Government, 2013.)

The Strategy deems that Government and different actors should have reliable, real-time situation picture that is communicated to all the actors within the cyber security sphere of Finland. Each ministry and administrative branch is responsible within their mandate and should aim to further the aims of the strategy within this mandate. The strategy aims for a shared situation awareness and national & international cooperation to build know-how. The means through which these aims are to be fulfilled include appropriate legislation and incentives, to ensure compliance from different actors. The Government must assign tasks, service models and management standards to authorities and business community to further the goals of cyber security. The key actions include establishing network of key actors, raising awareness, facilitating cooperation and information sharing. (Finnish Government, 2013.)

The governmental central situation awareness actor is the National Cyber Security Centre (NCSC-FI) under the Finnish Communication Regulatory Authority (FICORA)[1]. Police handle investigations related to cyber-crime. Military defence will be tasked with intelligence as well as cyber-attack and defence capabilities under the Ministry of Defence. These declarations are the closest we get to responsibilities within the strategy, no critical business actors are named, other than the tradition of history of close public-private cooperation, which must be maintained. (Finnish Government, 2013.)

Like any good strategy, the Cyber Security Strategy is a vague vision of a well-functioning society; all actors working in cooperation for a cyber secure future. The reality, however, is that the high-minded concepts must be operationalized, cooperation facilitated and information sharing networks built. The strength, according to the strategy, is Finland's history of a small, capable and collaborative country and the holistic security approach with a long history. How these previous successes will be transformed into the cyber domain? These questions are answered in the Implementation Programme in the next chapter.

[1] Appendix 1 lists the governmental actors referenced within this thesis and their current (as of 04/2018) Finnish designations

**Implementation Programme for Finland's Cyber Security Strategy**

The Implementation Programme for Finland's Cyber Security Strategy is a plan published by the Security Committee with the aim to implement the cyber security vision and the stated ten strategic goals. The Security Committee is a body working towards comprehensive security across the government and ministries, based under the Ministry of Defence. It coordinates preparedness measures and the implementation of the new cyber security strategy. (Security Committee, 2017b.)

The implementation programme is based on the Cyber Security Strategy as well as the 2017 government research programme "Finland's cyber security: the present state, vision, and the actions needed to achieve the vision". As such the implementation programme draws its main guidelines form the cyber security strategy, but updates its actions based on the later study. As we have seen, cyber security and threats have evolved during the five or so years since the publication of the original strategy paper. (Security Committee, 2017a.)

The Implementation programme is built on three items as its cyber security vision

- *Finland can secure its vital functions against cyber threats in all situations.*
- *Citizens, the authorities and businesses can effectively utilise a safe cyber domain and the competence arising from cyber security measures, both nationally and internationally.*
- *By 2016, Finland is the global forerunner in cyber threat preparedness and in managing the disturbances caused by these threats*

(Security Committee, 2017a, 7.)

This vision frames the view on national cyber security: (1) securing the vital functions, (2) safe cyber domain and (3) effective preparedness and incident management.

The implementation programme repeats the aims of the Cyber Security Strategy, grouping the initiatives to achieve these goals into three: (1) Leadership to ensure that the Cyber Security Vision is realized, (2) Society's vital digitalised functions will be assured and (3) The cyber competence of citizens, the business community and the public sector will contribute security to digitalisation. The drive to transform cyber security is based on leadership, mainly by the government, in creating effective management and steering structures, models and legislation in addition to providing holistic situation awareness. Assurance of digital functions will be ensured by administrative and technological actions and the cyber competence development will ensure compliance within the cooperative actors (citizens, business community and public sector). (Security Committee, 2017a.)

The implementation programme expands the list of central actors to national cyber security, among them Prime Minister's office, all the ministries, The Secretariat of the Security Committee and the committee itself, Authorities (police, army etc.), Government ICT Centre (Valtori), counties, National Emergency Supply Agency (NESA) and the National Cyber Security Centre Finland (NCSC-FI) under FICORA (Security Committee, 2017a). The programme cannot delegate actions to private actors, so specific firms are not listed within these, but the scope of the programme shows that the gravity of the issue has expanded since the formulation of the strategy.

The leadership domain of the program consists of creating a holistic framework to govern the national cyber security, with effective legislation, guidelines, international cooperation, public-private collaboration backed-up by implementation of major cyber incident management model, comprising of cyber security situation picture, effective information sharing and monitoring and responding to cyber security incidents (Security Committee, 2017a). The leadership of national cyber security is on one side to provide regulation and guidance, but on the other act as the vanguard of cyber security in cases of emergency. The government must facilitate holistic cooperation and information sharing not only between public and private entities, but possibly even competitors (e.g. two network service providers), not an easy task. Effective and secure lines of communication, vulnerability and incident reporting structures need to be established, where confidentiality is paramount.

The assurance domain requires the safeguarding of vital digital functions of society, established through identification of these functions and stakeholders and protecting the critical infrastructure. Within the domain, we find functions such as electricity, telecommunications, security of supply and data protection. The domain extends to preparedness and business continuity within these functions, with security audit responsibilities assigned to make certain the level of security is acceptable. (Security Committee, 2017a.) The domain consists of the majority actual work within the programme, with major challenges in identifying and protecting the vital functions. The programme actions reveal the lack of clarity to the cyber domain, as asset identification is a major part. When it comes to cyber domain and security, this is natural, as something defined and identified, may be obsolete in a year. However, for our task of defining cyber security within the national context, this proves problematic.

The final domain deals with developing cyber competence among citizens, business community and public sector, to make sure digitalisation initiatives are completed securely. The two parts within this domain are the provisioning of a secure growth platform for digital businesses and cyber security training and exercises to improve awareness and provide actionable intelligence on actual cyber capabilities. (Security Committee, 2017a.) The third domain ensures that the actions of the previous two domains fall on fertile ground and there is ample awareness both within the citizens and the public and private sectors.

The implementation programme underlines the challenge that is the definition of cyber security within the national context. The problem is twofold: (1) what are the vital functions at any point in time? and (2) what does it mean to secure these functions? (For instance: in the case of communications: are different messaging applications vital or only one of them? Which one? Do we regard SMS as a viable back-up? Will we regard SMS viable in ten years?) We must accept that national cyber security changes as a function of time and technological and socio-logical development, what is critical today may be obsolete tomorrow. Whit these restrictions in mind, we must move on to conclude our journey through the cyber realm.

### 3.1.3 Conclusion

Cyber as a concept is at best muddled, but major problems arise from the fact that as a domain, cyber is under constant change. Cyber changes as a function of time, people, technology and processes evolve and affect change throughout the cyber domain, its technological levels and even people who operate within the domain. If we understand this complexity, we can make decision on how to form our definition: we must handle in generalization of some sort, to be able to steer clear of instant outdating of our concepts.

Cyber security is the safeguarding of cyber environment, which has multiple levels. At this moment, the levels can be defined as: (1) physical, (2) logical and (3) social, following e.g. from the US Army (2010) and Libicki (2007). The cyber threats and risks confronting the do-main may be focused on any level and effects may manifest on any level, i.e. physical threats with social effects are possible and vice versa. Cyber security controls include governance, physical, logical, processes and social.

On a national level cyber security is a challenge of public-private cooperation and coordination. Much of the infrastructure is run and developed by private actors, mainly for private customers, but the development of the last few decades has seen life-supporting services move to IT-systems and online services. Nutrition is still maintained by physical food; logistics, distribution and payment services rely on functioning IT-infrastructure. This dichotomy must always be kept in mind when talking about cyber security on a national level, the government can only safeguard a small part of the cyber infrastructure, rest is secured through interaction and co-operation with private entities or through legislation and regulation.

The governmental approach to cyber security is very similar to the one that we have seen in the literature. The initiatives, however, suffer from similar problems as our cyber definitions: how to deal with the time component and avoid issues with outdating? The government deals with these issues in two ways: (1) the documents are high-level and vague purposefully, and (2) they are updated regularly. As a consequence, we must engage in some interpretation as we move towards a view on national cyber security situation awareness, but as a whole the governmental papers have given us a solid footing to base our further study on.

## 3.2 Situation Awareness and Understanding

To be able to understand Situation Understanding (SU), we must step back and take a wider look at Situation Awareness (SA) as whole. SA and SU are related concepts and as such we must be able to remain within clearly defined boxes for them, in order not to obfuscate the discussion. We find that some of the discussion around SA and SU, even Situation Comprehension (SC) is sometimes used, fail because the definitions are unclear between the parties in the discussion. Looking at SU through the lens of SA-research will give us structure to separate them in an orderly manner.

Situation awareness (SA) provides the ability to identify what has happened and is happening (UK Ministry of Defence, 2016b, 5). Usually understood within the context of a decision-making-cycle or -process, the function of being aware of the elements and actions unfolding around oneself, to create an understanding that decisions can be based on known as SA is vital. Nofi (2000, 71) formulates a general definition of situation awareness as the development of a dynamic mental model of ones environment. In the complex world turning at a lightning pace, understanding of the situation around us is key to successful decision-making. The real benefit of SA, according to Endsley (in Garland, Wise & Hopkins, 1999, 258), is not improved performance, but rather the management of inherent risk of a performance error.

Up-to-date SA provides sound understanding of current status and a robust base for building Situation Understanding and further the basis for decision making. Situation understanding (SU) can be understood as sub-phase of complete SA-process (for example: Endsley & Garland, 2000), but in the scope of this thesis we will define Situation Understanding as having a sufficient level of knowledge to draw inferences and possible consequences from SA information (Alberts, Gartska, Hayes & Signori, 2001, 18-19). The further definition arises that SA is the rather mechanistic building of current and past events, whereas the true meaning of SU is to bring context to the SA-picture and provide basis for projection of future events, giving the observer a base for decision making and action (Endsley, 1995, 35-37).

### 3.2.1 Situation Awareness

Emergence of situation awareness research was based on the operational needs of more detailed understanding of SA. The pioneers have been aviation, both pilots and air traffic control, industrial plants and emergency services, but slowly and surely SA-thinking has penetrated almost any field, powered by the challenges of technological development. Currently one of the biggest fields developing SA-based thinking is the cyber security, where networked systems are producing information and these solutions are supported by the increasing computing power and focus on system usability. (Endsley & Garland, 2000, 1-2.)

Situation awareness is defined by Endsley (1988, 97-101) as:

> *"...the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future."*

The above definition comprises three dimensions: (1) perception of the current situation as a factor of space and time, (2) the comprehension of the situation based on the perceptions and (3) the projection of the future situation based on the previous dimensions. The work to define situation awareness has its root in operative functions, such as airplane piloting or emergency services, which can be seen from the definition, with its focus on time as a dimension.

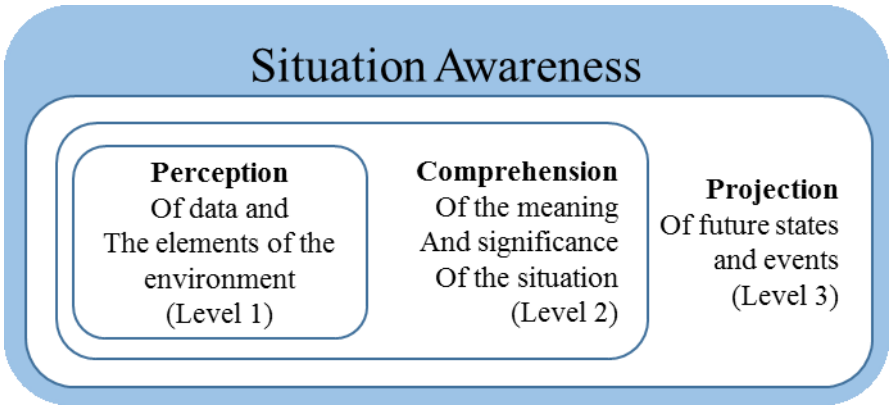


Figure 2. Dimensions of Situation Awareness according to Endsley (Adapted from Endsley, 1995, 35.)

The levels of SA can be described as follows (Endsley, 1995, 36-37):

- The first level is perception, the act of perceiving the status, attributes and dynamics of situation elements. The processes in use are monitoring and recognition of relevant elements. The SA consists of multiple SA elements (objects, events, people etc.) and their current states
- The second level is comprehension. It is the process of synthesizing the perception of the aforementioned elements into a single, overarching understanding of the status of the elements, the interaction between the elements and understanding how these elements affect the observer and their goals and objectives.
- The third level is projection. Projection is the capability to project the future actions of the environments elements. The projection phase requires the robust base of the previous levels, combined with the ability to extrapolate the actions and functions of the elements and how this will affect the relevant states.

In Endsley's model SA can be understood in two ways: (1) SA as the process of perception, comprehension and projection, or (2) SA as result and the end state of SA-process, for example Wickens (2008, 398-399) defines SA as the process of updating SA where SU is the end result. The duality of the concept of SA is important to understand and keep in mind, especially when we move towards the Shared Situation Awareness and SA in cyber context. Defined this way the SA-process is an ongoing function, updating constantly, whereas SA-as-a-result can be thought more as a snapshot in time, documentable as a report for instance, that can be used as the basis for building Situation Understanding.

In the military context, SA-thinking has been popularized mainly by Colonel (ret.) John R. Boyd through his developing of OODA-loop as concept of the decision cycle. Boyd's creation of the OODA-loop has its roots in aviation as well, as a former fighter pilot, the goal of his theory was to achieve success in air-to-air combat. In his later years, Boyd expanded his thinking into general military theory, overall military command-and-control, and was able to find many areas of combat, from strategic to tactical and operative level, where his model was effective. Boyd's work was later adapted to many different fields, such as business, by his close colleagues, known as acolytes. The essence of the OODA-loop is the creation of overwhelming decision-making ability to dominate the battlespace. (Coram, 2002 & Richards, 2004.)

Analysing the OODA-loop, the situation awareness is a combination of Observe and Orient-phases, that can both lead (in Boyd's theory the aim is to automate as much as possible, i.e. move from phase to phase faster, or to truly dominate your enemy, skip entire phases to jump straight from Observation to Action) to the Action-phase. In Boyd's thinking SA is divided into the two O-phases, with Observe concerned with looking from the inside out and collecting information; while Orient is concerned with analysis and internal comprehension of the situation. As a system, the Boyd SA more attuned to the operative needs of actors who require quick decisions, but as a framework for strategic thinking bolstered by some additional concepts, Boyd showed that it can work for strategic command as well. (Boyd 1986, 1987 & 1995.)

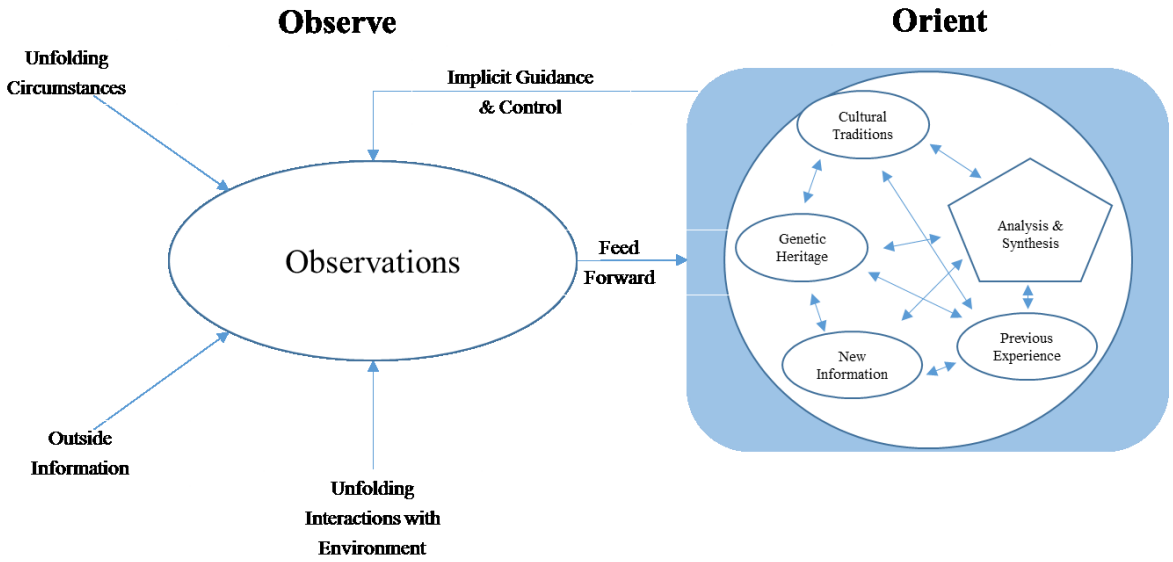


Figure 3. Observe and Orient by Boyd (Adapted from Boyd, 1995.)

In Boyd's model the duality of SA-as-process or SA-as-a-result are somewhat more muddled than in Endsley's, as the model is a dynamic, interchanging model of a thought-process. In Boyd's process, most of the phases are automatic when comprehension is at a high enough state, and as such the separation of these two elements on a fundamental level becomes harder. For the scope of this thesis, the dual view of SA prevails. However, Boyd's model has some important elements, that are beneficial to understanding SA in the cyber context especially: (1) understanding of friction as a key element arising from ambiguity, deception and uncertainty and (2) concept of schwerpunkt as orientation, where a common view and goals function to reduce friction, where this common goal acts as pull-together factor for all actors. The benefit of Boyd's thinking is that he sees the decision-making loop from a higher level as well and through his thinking we can take a view of how to improve cyber SA. (Boyd, 1987.)

Comparing the two models, it is clear that semantically they fit together very well. Endsley's Perception- and Comprehension-levels can be understood in a similar frame to Boyd's Observe- and Orient-phases. The actions within the boxes are quite similar, and the aims and results work in similar vein. The difference can be seen in the final level and phase; Endsley's Projection is inherently a function of SA-process, when Boyd's Decide- and Act-phases move him out of a strict SA-frame and into the area of decision making. For our purposes in this study, the SA-frame will be understood as the combination of Endsley's Comprehension and Projection-levels as well as Boyd's Orient-phase.

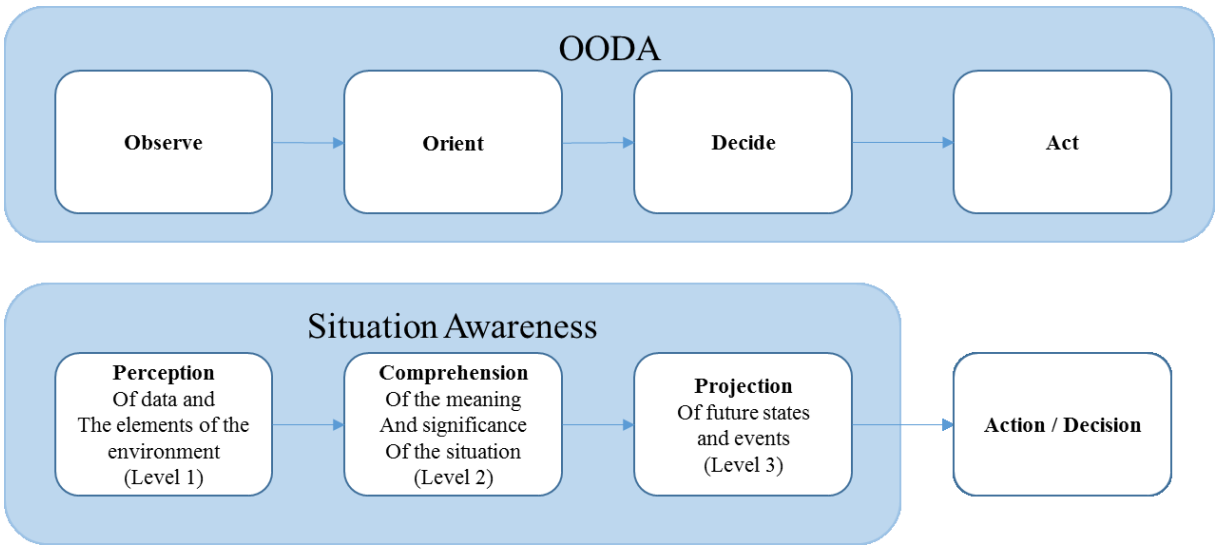


Figure 4. Side-by-side comparison of the two SA-models (adapted from Endsley 1995 & Boyd, 1995).

### 3.2.2 Situation Understanding

Situation Understanding (SU), within the context of SA-process, is the comprehension of the current situation, the observation of the elements within and their elements, the interactions of the elements and the effects of the elements on the observer's goals and objectives. The comprehension phase is interpreting information and creating context and understanding, with projection of what happens next based on the current information. The point of level 2 comprehension, is to be able to derive relevant meaning and significance from data (Level 1 perception). The difference of SA perception and understanding comes from assigning objective significance and importance to collected data. (Endsley 1988 & 1995, Endsley & Garland 2000.)

Alberts et al. (2001, 18-24) look at SA and SU in military context and conclude that situation awareness deals with what can be understood from the situation historically and in the present, whereas the situation understanding deals with analysing how the situation is developing and how it may develop in the future. In similar vein, Cooper (in Johnson & Libcicki, 1995, 103-105) has constructed a view of SA based on levels of information and knowledge. The Cooper model presents the SA as cognitive model, where raw data is turned first into information and through SA-process into SA and SU itself. Endsley (in Kott, 2008, 96-98) states that the second level of SA moves the individual from observing the presence of elements within the situation, to understanding the meaning of the elements and their interactions in relation to their goals and requirements, calling it Situation Understanding.

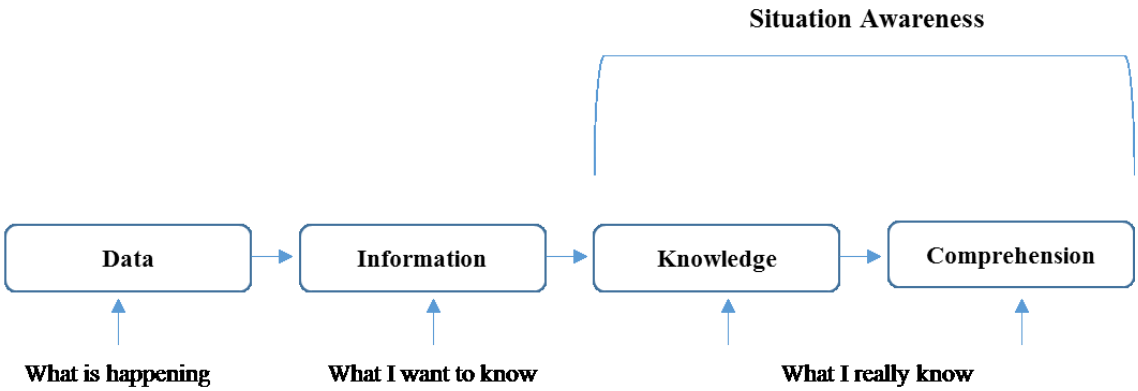


Figure 5. Information in relation to SA-levels (Adapted from Cooper, in Johnson & Libicki 1995, 103-105.)

The emergence of SU is a process, that is based on the ability, of the individual or the system, to receive, gather, analyze and use information. Understanding rising from the analysis of gathered information, leads to decision and action. SU is always situation dependent, based on the internal models, experiences, training and other factors, that combine with the information available and the SA-actor's ability to handle that information. The emergence of SU is presented below in Figure 6. (Sinkkonen, Kuoppala, Parkkinen, & Vastamäki, 2006, 88-89 & Nofi, 2000, 20-22.)

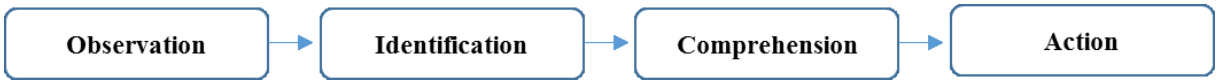


Figure 6. Emergence of Situation Understanding (Adapted from Sinkkonen et al. 2006 & Nofi 2000.)

Boyd (Richards, 2004, Chapter 7) spoke a lot about implicit direction of the loop, as internalized factors mould the process of SA for each unique SA-actor. Boyd's main thesis was that winning comes not from accumulative SA-process to gather a higher SA-balance and gain competitive advantage. Rather he emphasized the implicit over explicit; "to gain a favourable mismatch in friction and time." (Boyd, 1987) This raises the significance of true SU, where the current situation is turned immediately into comprehension and understanding of the options for action. Central to Boyd's OODA is acting on true SU enables the actor to unleash the unexpected, to blindside to adversary and gain an upper hand. Boyd's view is especially valuable in the cyber context, as knowledge of one's own assets, their function and interdependencies has a major effect on cyber incidents.

Understanding is always built on the observer's existing mental models, previous experiences, current analysis and even current mental state. These individual and shared factors can have a major impact on SA-comprehension, and must be considered. Boyd's Orient-phase has a built-in pentagon of elements that must be factored in: (1) cultural traditions, (2) genetic heritage, (3) analyses and synthesis, (4) new information and (5) previous experience. Endsley (1988 & 1995) talks about the effects of ideology and mental models on comprehension. The combined factors form the two writers are presented below, in Figure 7. The different elements affecting the situation awareness result in vastly different interpretations of the SA. For example, two organisations will view the SA through their own lens, based on the history, current situation and capabilities.

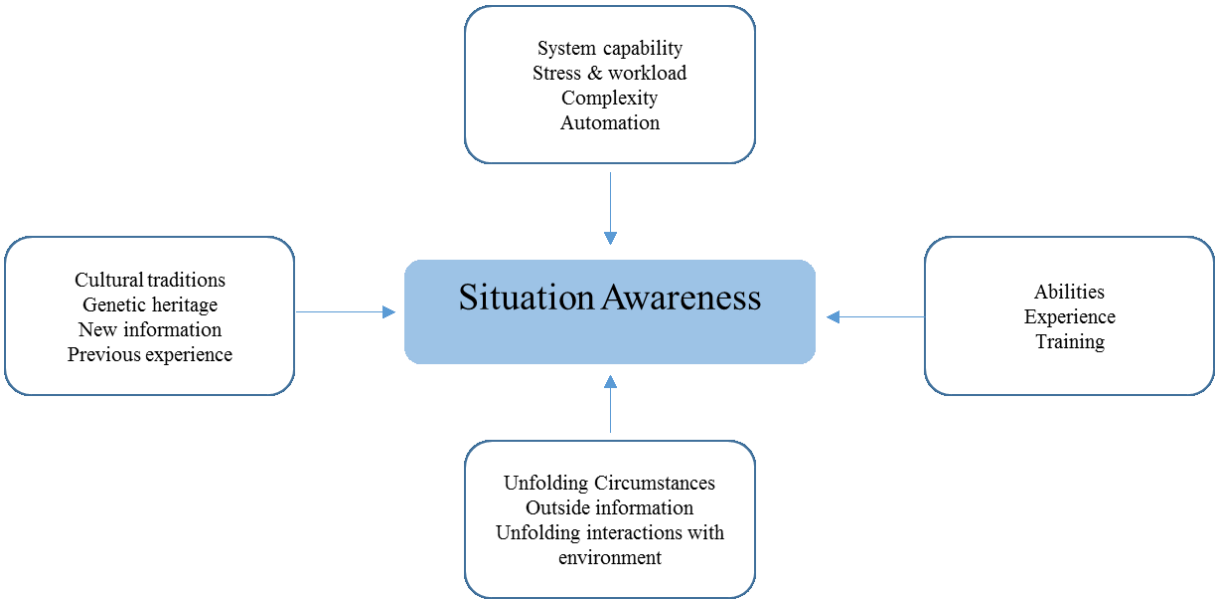


Figure 7. Factors affecting the emergence of SA (adapted from Boyd 1995 & Endsley et al. 2000.)

The sources of information for SA comprehension are various. The value of different sources is clear, with understanding of both the value of observed sources but also the sources of mental models that assist in interpreting the collected information. The true value of SA understanding comes from finding the relevant information within the oceans of data, that we are capable of collecting in today's world. This phenomenon is known as the Information Gap and is described below, as a rule we should always understand that more data does not necessarily mean more information. Rather, the quality of analysis and interpretation gives meaning to data. (Endsley & Garland, 2000.)

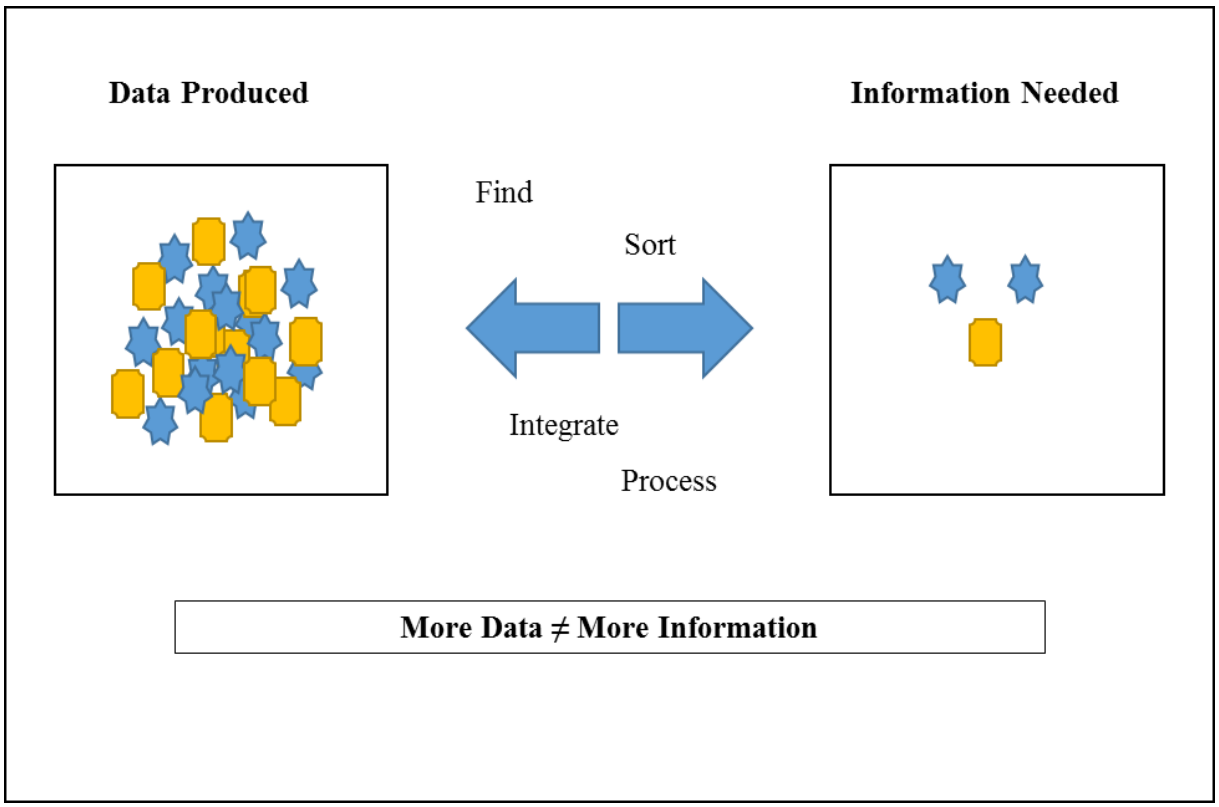


Figure 8. The Information Gap (adapted from Endsley & Garland, 2000, 2.)

Nissinen (in Vankka, 2015, 48) frames the issue of SA breakdown caused by excessive data flow and excess information as common to today's world of digital information and computing power. The purpose of SA is to filter the information from data, through definition of SA requirements and SA processes to provide a framework for all SA actors. Beyond the framework, precedence is given to exchange of information and SA systems that support this communication. This is echoed by Khrons-Välimäki (in Vankka, 2015, 45) and the three issues of design principles for SA: (1) how to organize information, (2) how to process information, and (3) principles for designing user interfaces for SA. Haapanen (in Vankka, 2015, 35-37) treads similar paths by his three groups of design principles for SA: (1) how information should be organized, (2) how information should be processed and (3) how to improve the SA of the operator for SSA. Both views underline the importance of information and open communication for SA is critical. (Vankka, 2015.)

### 3.2.3 Shared Situation Awareness

Nofi (2000, 26-27) furthers the definition of situation awareness to shared SA by simply extending the dynamic mental model to a group dynamic mental model. The aim of Shared Situation Awareness (SSA) is to provide a common view of the situation, based on common goals, requirements and aims. As Sinkkonen et al. (2006, 88-89) points out, it is impossible for a single actor to share their SA completely, as SA is based on internal factors of an SA-actor. The more homogenous the SSA-group is, the beneficial the circumstances for successfully creating SSA. However, the SSA must be based on common ground, the factors that are shared by all the actors within the group: training, employment, similar experiences, assumptions (Nofi, 2000, 49-52). This common ground is essentially the platform that SSA must be built on and in organizational actors can also be based on commonly agreed on goals or requirements. The SSA can differ greatly from individual-SA, as the goal of individual-SA can be vastly different from SSA. However according to Endsley & Jones (1997, 49) common SA requirements are the basis for SSA, where all team members maintain the same SA, based on these common goals and requirements.

Figure 9. below presents the SSA-model by Endsley and Jones (1997), where A, B and C are team members with their own individual SA. AB, AC and BC represent the common SA created by the members of the team, these arise as a by-product of aiming for team SSA. ABC is the team SSA, where you have the shared requirements and the common goal for SSA. Salas, Dickinson, Converse and Tannerbaum (in Sweazy & Salas, 1992) have studied the emergence of SA in military units, where each individual has a defined role and responsibilities. The most important defining factors of SSA in this context was the common goals, interdependency and specialized roles and duties (Sweazy & Salas, 1992). The group SSA can be described as the SA level, that each actor in the team has achieved based on their own role and goal within the group (Endsley & Jones, 1997). The key to successful SSA is a common goal, from which individual duties and requirements are derived for each actor within the group.

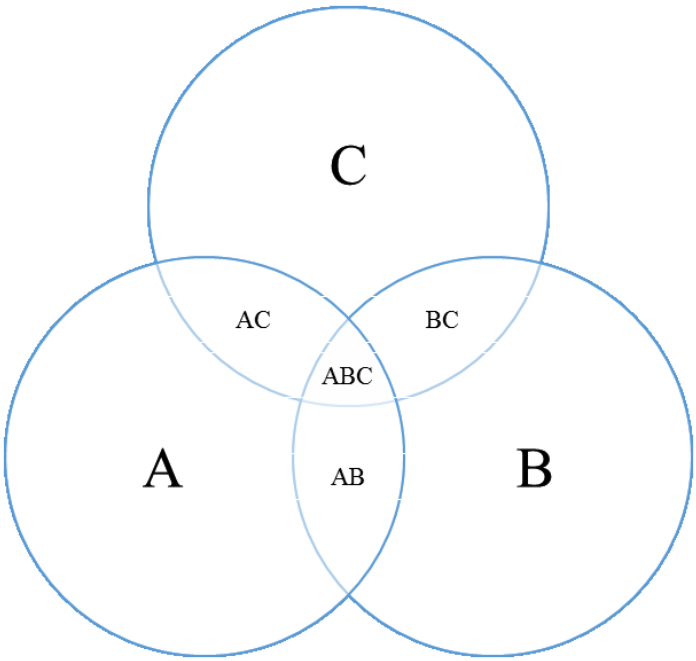


Figure 9. Shared Situation Awareness (adapted from Endsley & Jones, 1997, 47.)

Panteli and Kirschen lay out the requirements for each level of SSA, that are presented in Table 1. below. Level 1 requires the actors to have awareness of the system and environment in addition to being aware of the status of the other team members. On level 2, comprehension, the ask of the actor's is to perceive the goals and requirements of themselves and others in the group, and understanding of the impact of own actions on others and vice versa. Level 3 is simply the foresight of future actions of team members and acting accordingly. (Panteli & Kirschen, 2015, 140-151.)

Table 1. Shared situation awareness requirements (adapted from Panteli & Kirschen 2015, 140-151)

| | |
|---|---|
| Level 1: Perception | System<br>Environment<br>Other team members |
| Level 2: Comprehension | Status relevant to own goals/requirements<br>Status relevant to other's goals/requirements<br>Impact of own actions on others<br>Impact of other's actions on self and overall goal |
| Level 3: Projection | Actions of team members |

### 3.2.4 Situation Awareness in Cyber Context

The view of SA and SU in the previous chapters is universal, not relating to any particular domain. We are, however, interested mostly in cyber space as a domain and national cyber security as a specific target for our view of generating SA and producing SU. Tadda & Salerno (in Jajodia, Liu, Swarup & Wang, 2010, 27-28) state that Cyber SA is dependent on the level of the observer, i.e. network administrator will have different needs compared to a higher level cyber manager in an organization. The issue is that SA as a product may be a single view or system that collates all the SA-relevant information, but SU is much more varied within the organization.

Richard Kugler (in Kramer, Starr & Wentz, 2009, 333) views the cyber situation awareness for deterrence in the case of a national actor (specifically USA) to be based mainly on outside observation of the threat landscape and adversaries, comprising of five types of knowledge:

- identification of cyber threats
- assessment of motives, goals and calculations of adversaries
- appraisal of calculations, judgements and external pressures that might lead to adversary refraining from action
- awareness of potential adversaries' assets, capabilities and vulnerabilities
- all-source intelligence for attribution of crisis situations

The Kugler-view of SA is firmly in the "know your enemy" part of "sun tzunian"-art of war and lacks the internal view of knowing yourself (Sun-Tzu, 2002). SA defined by The Comprehensive National Cyber Security Initiative (2009, 3-4) complements Kugler's view by concluding that shared situation awareness consists of understanding network vulnerabilities, threats and events within the federal government, state, local and tribal governments as well as private sector partners. They make it clear that cyber-SA requires effective maintenance of cyber-capabilities within complex distributed infrastructures in changing cyber landscape (Harrop and Matteson, in Lemieux, 2015, 161). Cyber-SA requires both the understanding of internal situation as well as knowledge of the external situation, there cannot be true SA without both. This leads to concerns over data vs. information and data overload, as Tadda & Salerno (in Jajodia et al. 2010, 27-29) highlight the current situation challenge as lower level, technical SA-data overwhelming the decision makers cognitive ability. The need is to clarify the requirements of SA-data on different (for example operative, tactical and strategic) levels of decision making, that require different type of data as input into the decision-making cycle.

Tadda & Salerno (in Jajodia et al., 2010, 27-28) stress the importance of understanding an organizations field of operations, that will bring its own requirements and threats. Trying to understand the national requirements; an organization that is critical to societal functions will have a wholly different view to cyber security than a firm with no obligations towards the functioning of national infrastructure. Even if Tadda & Salerno (in Jajodia et al., 2010, 28.) define environmental information as network topology and the collection of data associated with this topology, we will need to look at SA and SU in a wider scope. Especially looking at the strategic level SU, the importance of local, technical understanding is limited and needs to be interpreted through the meaning of such information to the bigger organisational picture of cyber security.

Bradford, Dacier, Dietterich, Fredrikson, Giffin, Jajodia, Jha, Li, Liu, Ning, Ou, Song, Strater, Swarup, Tadda, Wang & Yen (in Jajodia et al., 2010, 4-6) view the internal situation as critical to SA, with internal infrastructure information, attack vector, anomaly detection and attack detection as especially important. They provide seven aspects, that at least must be present for cyber SA: (1) Awareness of current situation (perception), (2) Impact of the Attack, (3) Awareness of how the situation evolves, (4) Awareness of adversary behaviour, (5) Awareness of why and how the current situation was caused, (6) Awareness of the quality of perception and knowledge-intelligence-decision relating to the situation and (7) Assessment of possible futures of the current situation. For one to be able to build and maintain SU in cyber context a thorough understanding of oneself must be in place, otherwise understanding the possible attack vectors, vulnerabilities and consequences of attacks is impossible. This, however, is not enough: there must also be an understanding of the outside forces, means and motivations. Low level SU within an organization might be reachable by understanding the systems, processes and people within it, but to reach a high level of SU this rudimentary information must be complemented by the understanding of internal complexities and dependencies within, the criticality of information and systems and the outside attackers and their motivations and means (Jajodia et al. 2010, 3-7).

As both Boyd and Endsley (2000) view time as a critical part of SA and especially SU, in the cyber SU time must also be of critical importance. This emphasizes the ability to monitor and react to detected anomalies, and at the same time understand that every second allowed to the adversary to act makes detection and reaction more challenging. Lehto & Limnéll (2017, 199) stress the same view with emphasis on a real-time SA that supports Shared-SA in the network of critical actors. Their conclusion is that by providing real-time SA and understanding adversary operations, capabilities and goals will one reach a decision-making ability to outmaneuver the opponent.

### 3.2.5 Conclusion

Situation Awareness as a concept has been defined from multiple angles, the two main views of this thesis are the SA-process oriented view by Endsley and the more decision making oriented view of Boyd's OODA-loop. Both views provide insight into the definition of Situation Understanding, which can be summarized as the understanding of the current situation and the projection of its future status. The three dimensions of SA-as-a-concept (vs- the SA-as-a-process) need to be kept in mind as they support each other: (1) level 1 Situation Awareness, (2) level 2 Situation Comprehension and (3) level 3 Situation Understanding.

The complexities within the SA-process need to be considered when trying to identify prerequisites to Situation Understanding. A view of the operating environment, required information and capability to analyse the collected information are all vital. Similarly, the factors affecting the building of Situation Understanding, both inherent and external, are relevant. The true value of Situation Understanding comes through identification, collection and analysis of the truly important information, hidden in oceans of data that are available in our modern, interconnected computerized world.

Shared Situation Awareness is more complex than just combining the SA of the individuals of the group. Rather, you need to consider the factor affecting the group dynamic, i.e. the differences of the individuals, be it cultural, educational or geographical. At the same time, it is essential for the group to have shared interests in building the SA. These include commonly agreed goals or common defined requirements, as well as the aims of the SA. Shared Situation Awareness needs to benefit the individual parties as well.

In the cyber context, SA is very dependent on the level of the observer, a low level technical SA is completely different from organizational strategic SA. Similarly, in cyber context the mapping of essential information is critical, operative level systems produce streams on data that need to be analysed and broken down into actionable inputs to the cyber SA-process. The cyber SA requires understanding of both internal and external information, internal situation and system knowledge is essential to provide framework and context for actionable information, but there also needs to be an understanding of external threats and actors.

# 4 EMPIRICAL RESEARCH

This chapter will present the empirical research portion of this thesis, mainly the interviews and analysis of the interview content. First the interview methodology is presented as well as the interviewees to provide an overview of the research. Then analysis methods are presented, based on the abductive research method. Finally, the results of the interviews are presented in a similar structure as our guiding principles in the previous chapter.

## 4.1 Interviews

The themes of the interviews were based on the research questions and the two main guiding principles of cyber security and situation understanding. The interview themes were bound to a hypothetical situation of strategic level threat intelligence exchange within the network to provide concrete context and basis for the interview discussions. Strategic level threat intelligence also provided leeway to stay clear of security operations or even incident management processes within the interviewee organizations, as these processes may over-ride the situation awareness function. On a strategic level they enable us to have a separation from technical level, which provides an opportunity to look at true Situation Understanding and the usage of that understanding. Strategic communication will not be high priority in terms of speed, but rather will provide the study with an actual view of cooperation between the organizations in the study. (Rantapelkonen & Koistinen, 2016.)

The data collected through the interviews was broken down in the themes created for the interviews and analysed through the prism of the theoretical understanding of the issues laid out in the previous chapter. The data was analysed using critical logic, which looks at the relation of the theoretical premises and the collected facts (Peirce 1931-1958 & 1958). The validity of the study is based on the soundness of the researchers use of the data and the ways it is presented, using abductive analysis the assumption is that the data is always valid, even the internal contradictions within it (Grönfors, 2011, 20). The credibility of the study will be based on multiple factors: (1) the credibility of used sources and their coverage of the research topic, (2) the use of the sources by the student and (3) the credibility of analysis of the data (Rantapelkonen & Koistinen, 2016).

The interviewees were selected to provide a sub-section of the whole national security network of actors, to maintain a manageable sample but at the same time provide a large enough group to provide valid conclusions. The interviewees were also selected to operationalize the view of national cyber security, in so far as the network of national cyber security is based on a numerous of organizations, private and public. No one actor has a holistic, all-encompassing picture of national cyber security, but rather the situation awareness is built on numerous pieces of the bigger puzzle, all the responsibility of different organizations.

Interviewees were selected based on the model of national cyber security presented in the previous chapters. The governmental actors are explicitly in the governmental documents and their cyber security responsibilities are based on legislation, as we shall see form the analysis of the interviews. The private actors are a different case, with their cyber security functions are based on a mix of the need to support and upkeep business functions and different regulations posed on them by different actors.

Interviews were conducted with representatives from the following actors:

- Government:
    - Communications Regulatory Authority (NCSC-FI)
    - Government Situation Awareness Office
    - National Emergency Supply Agency
- Infrastructure provider: Energy infrastructure Provider
- Infrastructure provider: Telecommunications Provider
- A preparedness critical firm: Banking Group

The interviews were conducted with the representatives of the actors. The interviewees were provided with the interview themes beforehand, but only on a high level. The interviews were taped and transcribed. The transcribed interviews were then sent to the interviewees, who validated them to ensure the content was representative of the interview discussion. The interviews were conducted in Finnish, where possible a direct translation is used. If no direct translation was available, there was considerable effort to preserve the spirit of the quote.

## 4.2 Analysis

This chapter will present the interview findings as per the guiding principles presented in the previous chapter. First there is an analysis of how the different parties view cyber security and how they are connected to the national cyber security network. Then the situation understanding is assessed, how the parties analyse and draw conclusions from situation awareness to build situation understanding. The following chapters are based on the interviews, unless a specific source is denoted. Direct quotes from the interviews are presented in italics and contain source information of the which interview the quote is from.

### 4.2.1 Actors

The actors interviewed are presented shortly in this chapter. Included is a short background information on why they need to address cyber security and what are the main drivers for each actor.

**NCSC-FI**

The National Cyber Security Centre of Finland (NCSC-FI) is the main operative cyber security actor of the Finnish government, situated within the Finnish Communications Regulatory Authority (FICORA). FICORA is tasked with developing and monitoring the operational reliability and security of communications networks and services (FICORA, 2018) and NCSC-FI is the specialist organization within the authority responsible for cyber security situation awareness within the communications network and services. NCSC-FIs mandate is based on legislation, which explicitly frames the functions scope as the de facto cyber security regulatory authority within Finland. According to the interviews, the role of the NCSC-FI is twofold: (1) to act as the Governmental Computer Emergency Response Team (CERT) with the responsibility to monitor, respond to and solving different security incidents, violations and threats, and (2) cyber security regulatory authority with the mandate to produce binding guidance and policies within the scope of FICORA (i.e. the communications networks and services, so the binding guidance is usually pointed towards the telecommunications providers within Finland). This role is unique to Finland, according to the interview there aren't many similar mandates, where the operative function also has a mandate to create binding guidance.

The ability to provide binding guidance, especially expedited through established networks, is a huge enabler for the NCSC-FIs functions, as the authority can respond quickly to cyber security threats within the national communications infrastructure. This enables NCSC-FI to for example instruct telecommunications providers to enable certain filtering functions within their networks, to counter certain threats. In cases, where NCSC-FI can identify distinct technical solutions to a threat, they can roll out the deployment very quickly to their network of organizations and set up mitigation efforts. This is based mainly on Finnish legislation (Information Society Code) and the NCSC-FI status as a regulatory authority, where the authority acts as the situation awareness centrality and identificatory of incidents. When solutions arise, they can bind different actors to roll them out.

The NCSC-FI functions mostly on an operative level, building situation awareness and providing insight to different actors within their networks. They mostly cooperate with organizations related to the communications network and services, but as the communications infrastructure is key to the functioning of different public and private organizations, these networks are extensive within the national realm. However, their expertise and insight is mainly limited to communications related issues and their mitigation. They do provide some higher-level guidance and reporting, but this is limited to few times per year, most of NCSC-FI focus is on daily functions and operative actions.

**Government Situation Awareness Office (VNK SA-office)**

The VNK SA-office is a governmental actor tasked with providing situation understanding to governmental leadership, mostly to the prime minister and the cabinet. Their mandate is based on law and their aim is to produce wide-scope SU-information on all topics that may affect the country and may need governmental actions. The goal is to collect a lot of information from different sources (governmental, NCSC-FI, police agencies, the defence forces, foreign sources etc.) and provide objective analysis for governmental decision making. Cyber security is one topic, but its role is limited, as one topic among many. VNK SA-office acts as a central node for governmental SA and SU, co-operating with many different actors and exchanging information within this network.

VNK SA-office functions mostly on tactical and strategic level, providing SU-information for decision making. The office stays out of the decision making itself, providing as objective information as possible, basing the collection and analysis on expert sources. The office itself tries to stay away from interpretation of the results, rather looking to be the provider of information. The governmental entities will make their own conclusions and decide on the actions required. Cyber security is just one topic the SA-office is monitoring, so it uses a lot of the other governmental functions to provider deeper understanding into the issues. For cyber, NCSC-FI is close collaborator, providing deep understanding and analysis in cyber incidents. Overall, the SA-office is a broad monitor of issues, but does not delve deep into any particular subject. That in depth analysis is left to the specialist organizations.

**National Emergency Supply Agency**

The National Emergency Supply Agency (NESA) tasks include providing support for National Emergency Supply Organisation (NESO) individual sector and pool organisations in security of supply activities. The sectors steer, co-ordinate and monitor preparedness in their respective fields and pools are responsible for monitoring, analysing, planning and preparing measures for the development of security of supply within their respective industries. NESA acts as the central planning and directing agency within the whole field of preparedness in Finland. (NESA, 2018.)

NESA's role within national cyber security is twofold: (1) supporting the cyber security preparedness of governmental sector and (2) supporting the cyber security preparedness of private sector. The functions supporting the private sector differ in two ways, the regulated industries are directed mainly through the regulatory means, while the non-regulated industries are directed through softer means, i.e. facilitating co-operation and providing voluntary support. As the NESA functions mainly as a fund, providing monetary support to security of supply and preparedness functions, it's role in the cyber security field is similar: providing support to different initiatives, facilitating co-operation and monitoring preparedness level.

**Energy Infrastructure Provider**

For an energy infrastructure provider, the physical view of cyber security is the strongest: functioning of the infrastructure is their main goal. Over the last few years, the logical layer has risen in importance and long history of workplace safety operations has enabled the organisation to leverage their awareness work for cyber security as well. The infrastructure provider seems to have a strong history in criticality and preparedness operations, reaching back maybe even a hundred years. This legacy is still visible today in the networks and preparedness work that is done.

The drivers for the infrastructure industry are largely regulatory, as the functions of the energy infrastructure are critical to the functions of society. This is evident in the structure of the whole industry, where the organizations are mostly involved in local monopolies, left to function as the sole provider for a certain geographic area. This fact combined with heavy preparedness and criticality regulation means that cyber security and other security functions are central to daily operations for the infrastructure provider. For them, the role is a mandatory player within the national cyber security context.

In terms of national cyber security, the field of energy infrastructure is highly networked and has many working networks around preparedness and cyber security. There is even strong co-operation internationally, with neighbours to all directions: Sweden, Estonia, Russia etc. The enabler for this strong co-operation is the fact that there is very limited competition between these operators. The international relations are important enough to side-step effects of international crisis, the operative work continues even, when diplomatic relations are frozen between countries.

**Telecommunications Provider**

Telecommunications is key for the interconnected society running on computing power, so for a telecom provider, cyber security is very important. The main aspect driving cyber for a telecom is the production of services, even though the regulatory burden is also large. The telecom operator needs to look at its production environment beyond the national borders, as its functions for cyber security encompass the Nordics as well. For our telecom the challenge of information exchange is not limited to external networks, but internal organization as well: how do the different country organizations interact. The cyber organization is a virtual one, encompassing experts from all geographies and supporting local businesses.

For the telecom provider the value of cyber security comes mostly through enabling the continuity and resilience of its production systems, while they are closely regulated by NCSC-FI, the main value realised by the organizations comes through their own business. Customer trust and functioning services are primary drivers for the organizations cyber security actions. This view makes the information exchange tricky, as it contains potentially critical business information. However, this is resolved by how the telecom network operates within the national cyber security context, most information is passed to other telecom operators via the NCSC-FI.

The telecom operators carry a large burden in national cyber security, as central cogs in the cyber network, they have the ability to direct web traffic and even suppress certain connections. They rely on fast actions and require it to be supported by up-to-date SA. The telecommunications industry in Finland works in very close co-operation with the NCSC-FI, as the FICORA is the regulatory authority for the industry. The telecom industry has close co-operation in cyber issues as well, although mindful of the competition, there is openness when it comes to disclosing large issues that may have wide effects. The NCSC-FI is the central node in the information exchange, the operators trust that it will not disclose critical business information to the other operators, while also maintaining usable information of the cyber issues and possible mitigations.

**Banking Organization**

A banking organization that in the modern world offers its services to customers via digitized channels is very reliant on cyber security to ensure continuity and resilience of its services. The continuity of business functions is a major driver of security overall within the organization, the benefits of effective cyber security operations has been realised from a business perspective.

The main connections to national cyber security, however, are regulatory. When looking at a large enough banking organization, it will be declared critical to functioning of the society and as such will be under the mandate if the NESA. In addition to NESA regulations, the banking industry is highly regulated for cyber security issues as well. The main parties are the European Central Bank, which handles the regulatory supervision of banks deemed large enough on a European scale. and the local financial regulator. Both provide ample amounts of regulation and auditing of an organizations cyber security, in addition to business, risk management and other internal functions. Upon all this, the banking organizations is liable for guidance regulating certain services, for example credit card industry has its own cyber security provisions.

### 4.2.2 Cyber Security and National Cyber Security

In this chapter we reflect on the interviews based on our guiding principles. The interview material is analysed through the prism of the theoretical background with the aim of understanding how the theoretical concepts found relate to the situation on the ground.

**Cyber Security**

> *"Cyber Security is just one topic we focus on, but at the same time you need to keep in mind that in the modern society everything ties to everything else.*
> (VNK SA-office interview.)

All the interviewed parties approach towards cyber security are quite similar, all the layers of the Libicki (2007) and US Army (2010) models are represented, although usually not packaged quite as neatly. The physical and logical layers are quite a lot more established, than that of the social which is mostly reduced to the security awareness of the personnel. Depending on the industry of the organization, the emphasis on each layer differs. The infrastructure organization puts a big emphasis on the physical side of things, whereas the more software based organizations, i.e. the banking organization and NCSC-FI, emphasize the logical layer. The social layer seems to be the least in focus, as especially the infrastructure focused organization seems to hold it in quite a small regard. During the interviews, one gets a feeling that the awareness level and the culture of the organization mostly affects the focus based on the social level (i.e. the actions of people). In comparison, an organization with a higher level of maturity in security awareness, for example the NCSC-FI or the banking organization (where phishing for example has been a long-time issue), the social aspects of cyber security are more pronounced. Although, in the case of the infrastructure provider the interviewed person was not directly responsible for security awareness, and this might explain the focus more on physical and logical layers of cyber security.

Cyber security as a concept is understood in similar terms, even though the approach is a little different whether you look at it more from a logical layer (as an expansion of traditional information security), physical layer (as expansion of traditional (physical) security management). Within the interviewed organizations there isn't any organizations whose outlook is founded on the social layer, which of the aspects seems to be the least emphasized. This maybe the least understood part of cyber security, especially when dealing with internet personas, information operations and manipulation, concepts that have risen to the public consciousness over the last few years. However, overall the cyber security framework is very similar between all the actors, which should provide a solid footing for national cyber security networks and processes.

**National Cyber Security**

> *"The benefits from national cyber security networks and information exchange are difficult to show, especially in the language business uses: euros. The benefits, especially in the long run, reliability and trust are definitely among them."*
> (NESA interview.)

Quite obviously, the governmental organizations and private organizations base their national cyber security co-operation on different drivers. The governmental organizations functions are based on legislative mandate, which covers their legislative basis, responsibilities and even prescribes resources. The mandates and responsibilities are derived mainly from the national security and cyber security related documents analysed in chapter 3.1.2. The private organizations, however, look at cyber security from two very distinct points of view: (1) supporting and ensuring resilience for their business functions and (2) regulations based on them from different regulative authorities. In the case of the banking organizations the continuity of their business functions and problem-free services to their clients are probably the biggest driver of cyber security, however on the other hand they need to consider regulations from banking authorities (both domestic and European), payment service regulators and National Emergency Supply Authority.

For the private organizations the size and industry makes a big difference how they are integrated into the national cyber security network: if the industry is a part of the functions vital to society makes an organization a concrete part of the national cyber security network, similarly the organizational size, if big enough to be critical, makes it a vital actor within the national context. Governmental entities base their functions relating to cyber security on their mandates, mostly form legislation. NESA derives its mandate form the Cyber Security Strategy and NCSC-FI from the relevant legislation relating to the Communications Regulatory Authority. The private organisations relationship to national cyber security is based on the operations and regulations relating to said organizations. The telecom industry works very closely with the NCSC-FI, who as both the regulatory authority and cyber security authority investigates issues and mandates actions based on the results. This is central to information exchange, but requires trust, as all the telecom operators need to be able to trust in NCSC-FI to not divulge business critical information. The interviewed telecom operator describes the process: *"Major threats are not hidden, but we openly inform FICORA and NCSC-FI, who process and deliver the information to all the operators, if it has implications for them. It helps information exchange, to know that NCSC-FI sanitizes the information on the way."*

The interaction between private organisations depends greatly on the field of the business and the customer – service provider relationship. That is, organizations that provide one another services, tend to interact a great deal more, than organizations that have no business functions between them. Companies within the same industries co-operate somewhat, especially if they belong to highly regulated industries, such as financial or infrastructure provider (physical or telecommunications). The client-customer relationship establishes strong interaction and information exchange between the parties. In the case of the banking organization *"...to the individual customer a lot of training and guidance is provided, but for the corporate customer, especially in the insurance business, almost a hands-on role has developed, where risk assessments and binding guidelines are part and parcel of everyday business."*

However, much of the networks that function within the national cyber security context are based on governmental actor's initiative, either regulation based co-operation or government incentivised groups. Regulated industries are forced to exchange information and complete certain cyber security related tasks, such as audits (for example The European Central Bank has audited at least some of the financial sector organizations in Finland recently). Best example is the telecom industry, which is networked strictly around FICORA and NCSC-FI, and their mandate to regulate the industry actors. According to the interview with the telecom provider, it is quite clear that information exchange on the level that is done through the NCSC-FI, would not happen directly between the competing operators: *"... you must always evaluate rigorously what information to share, especially the business related."* Information that has gone through the NCSC-FI analysis is a smaller risk of giving up anything business related.

Looking at the links to national cyber security networks, a big difference-maker is the history that the industry has of preparedness operations. A distinct difference can be noted between the banking organisation and the energy infrastructure provider, main reason seems to be the history of working within a regulatory context. The infrastructure industry has been wrestling with these continuity issues for over a hundred years, whereas the banking organisation has been dealing with ICT and cyber security issues for little over 20 years. How established the links are makes a big difference in the level of trust and information exchange. The infrastructure provider explains: *"... culture of preparedness comes from history, long history of preparing for power grid problems, snowy winters etc. We have been preparing for a hundred years."*

A lack of competition seems to be a major enabler for trust and communications within the national cyber security networks. Organizations that have nothing to lose by giving out information have a very low threshold for doing so. The difference to a competitive industry is pronounced: banking organisations have a lower level of interaction, even if one wouldn't consider cyber security a big area of competition between the different actors in the industry. The banking organization articulates the challenge form their point of view: *"The challenge is how to exchange information between competitors without divulging business critical information? And on the other hand, how much of the information can be sanitized for it to still be useful?"*

The private organizations show a presence of personal connections of their cyber security personnel, who in the courses of their career have built confidential relationships or even set up confidential networks between same industry peers. These networks are interpersonal and function on a strict confidentiality and anonymity basis: whatever is disclosed will not be made public. The penalty would most likely be loss of these valuable connections and reputation. These connections are not a major part of cyber security organization or operations, but provide a network of confidential connections, where even confidential vulnerability information can be exchanged. These personal connections seem to function in industries with high competition between actors, as such seem to compensate for the lack of formal networks. They may be a function of filling up vacuums, where there isn't any formalized framework for co-operation.

### 4.2.3 Situation Understanding

> *"...a malware by itself may not be very interesting, but understanding how it has penetrated the system is very interesting."*
> (NCSC-FI interview)

How does Situation Understanding emerge in the interviewed organizations and how are they able to exchange information on a national level? These questions are looked at in this chapter focusing on the guiding principle of SU.

**Situation Awareness**

> *"If there is no situation awareness, NCSC-FI is useless."*
> (NCSC-FI interview)

Practically all the interviewed organization had some type of SA-implementation in place, whether a SA-system that collects and displays the information directly or a process that collects information throughout the organization and provides a SA-picture to the personnel and leadership. These SA-processes align with the Endsley (e.g. 1995) SA-model, with three phases, while the OODA-loop (e.g. Boyd, 1987) Orient-phase points distinctly to the SU-processes of the studied organizations. The operative SA and analytical SU processes are more separated according to the interviews for the studied organizations than our theoretical model would presume. This may be caused by the separation of operative cyber security and more strategic cyber security functions within these organizations, especially the private ones.

The SA-models of the studied organizations are based mainly on technical solutions and their monitoring, there is a definite bias towards internal and technical information, and most implementations are rather technology based dashboard-type solutions. Outside SA-information, e.g. threat feeds and actor information, seems to be very qualitative, i.e. it is added to the SA-picture during analysis. The SA-implementation is connected to internal processes, that monitor the SA-indicators and launch internal processes as required. This also shows, that for the SA-processes the internal view is of more importance, than the outside sources of threats and vulnerabilities. This may be an issue of the incident management processes, that mainly deal with looking at the internal infrastructure and problems within it. Only later in the processes do external considerations come into consideration, if the internal actions are no effective to solve the issues or finally after the issues have been resolved with study of root causes and lessons-learned-processes.

Most SA-processes for the interviewed parties are concerned with the perception and comprehension phases, the main tasks are collection and analysis of information to determine the current status of cyber security. There is very little formalized SU-action within the SA-processes. However, the SU-functions are mainly built within certain reporting and planning processes. For example, the NCSC-FI offers SU information: *"…currently our SA is tasked with the collection of passive SA-picture and the projection is accomplished through annual or semi-annual reports to our stakeholders."* Similarly, the private organizations interviewed take the SA-information, process it through reporting and provide SU-information via expert analysis and planning of development actions. This seems to be a distinct characteristic of the private organizations, where the SA-process seems to consist two separate cycles: (1) SA-process runs as an operative cyber security process that provides information for operative actions, and (2) SU-process where the data from SA-process is combined with different intelligence feeds and fed into the reporting and planning processes of the organizations, through which it is refined into development actions (The SU-process for these organizations).

Two of the governmental actors' whole purpose is almost based on providing Situation Awareness: NCSC-FI and the Governmental Situation Awareness Office. These two functions are focused on very different views on SA: (1) NCSC-FI focuses solely on network related SA, (2) the SA-office looks at SA more on government functions point of view, the political situation around the world and special incidents, additionally the SA-office is also focused on analysis and provides SU to governmental actors, rather than pure SA-picture. These actors mission brief mandates them to be very SA-oriented, which clearly shows in the interviews.

**Situation Understanding**

> *"…Situation Understanding links closely with operative actions and goals in preserving smooth and reliable business functions, looking at more at the longer term."*
> (Banking organization interview.)

As noted in the Situation Awareness above: the SU is not really a part of SA-process for the interviewed actors, especially the private organizations. Situation Understanding emerges within these organizations either through reporting and planning processes or organically through the cyber security experts analysing and interacting within the organizations. The infrastructure organization explains: *"First we get a notification of a threat scenario through our networks. The information is passed on to our security experts, who analyse it internally. Then through internal reporting and analysis, it finally leads to the desks of our c-level who take in the conclusions and decide on the recommended actions."* This is a common route of an incident or threat information flowing through the interviewed organizations, finally being digested into conclusions, recommendations and development actions. The bureaucracy takes hold.

During the process of turning SA into SU, the organizations collect a lot of data to complement their SA-picture: governmental information, different threat intelligence sources, OSINT and networks (official and unofficial, even personal) are leveraged to better provide understanding of what the SA means and how the situation may develop in the future. The infrastructure provider elaborated their information collection to include: *"…we look at the attackers and their motivations. This gives us priceless insight into the severity of the threat, whether we can handle it ourselves or if we need to contact outside actors, for example the governmental ones."* Lots of different resources are leveraged, mainly as qualitative additions to largely quantitative data of the SA-picture.

For the private organizations, moving from SA and SC-operations towards SU brings business understanding and functions into the conversation. Looking at the longer term cyber security goals, one needs to consider the goals and requirements of the business, rather than looking only at the security or It-operations. The responsibility for cyber security: *"…it's separated threefold: (1) operative information security that handles the SA-process and related actions, (2) cyber security development that handles policy and development plans and (3) cyber architecture that handles the development of secure architecture and architecting the security solutions",* a structure that emphasizes the different views of cyber security, the needs of operative information security as well as the needs of the business functions. This requires the cyber security organisation to provide insight into the cyber security situation and incidents, so that these issues can be evaluated within the business scope and conclusions can be drawn.

The SA process in turning SA into SU for many of the organizations is about proactively managing future threats and risks. This fits well into the theoretical view of SU as the projection of future status, even though most organizations do not regard this as a part of the SA-process. Rather, it is seen more as a part of the internal reporting and planning processes. Most of the interviewed organizations look at the SA-process as purely operative cyber security, in this view the SU-phase of the process is a different one and may even be the responsibility of another organization altogether, as our example of the banking organization above, where the SA-process is divided to the turfs of three different internal organizations. Interestingly the long-term view brings the external considerations more into the evaluation: the threats, risks and adversaries feature more heavily in the SU-process than they do in the SA-process. This may be the result of the division of SA- and SU-processes to the different levels of organization and the separation of the operative and strategic.

Looking at SU through the lens of OODA-loops Orient-phase (Boyd, 1995), some conclusions can be drawn of the importance of cultural tradition and previous experience to the emergence of SU-process:

- Within the infrastructure industry has a long history of preparedness and continuity planning, that provides strong frameworks not only to the networks within the industry, but also for the SU-process of the firms. As these frameworks give structure and previous experience makes understanding cause and effect easier, the SU-framework for these actors is very mature. Under these conditions, combining new threats (cyber) into the framework is easier and as such the SU-process to provide insight into these threats is also easier.
- Compared to less mature industries (e.g. banking that has been dealing with cyber threats for only 20 years, or the NCSC-FI that has been around for less than 10 years), there are less ready frameworks to build SU on. Even as these actors are able to create a functionable SA-picture, the SU-functions are less established and function more on an ad hoc basis, combining with normal reporting and planning structures within the organizations.

This existence of established ways of working, networks and tradition in preparing for emergency situations is a huge benefit in emergence of SU. For example, the infrastructure industry manages quite a lot of scenario based planning and exercises, where the scenarios are based on very high impact incidents. This provides deep understanding of what can happen and how one responds to these worst-case scenarios. During normal operations one rarely meets these kinds of incidents, where everything seems to go wrong. So, planning and preparing for them makes it easier to respond to so called normal incidents, that at least hopefully are not as severe as the worst outcomes planned and trained for.

**Shared Situation Understanding**

> *"…all actors feel like they are the only ones with their specific problems. We try to facilitate information exchange to break this misunderstanding, as most issues are not unique, but affect plenty of organizations."*
> (NCSC-FI interview.)

The issue of a lack of functionable networks makes production of a shared situation understanding very difficult within the national context. As the networks function is very much based on central nodes that tend to be governmental actors, the only real national SU-view is within these actors. The effectiveness of these networks a hampered by two factors: (1) information exchange is muchly one-way, there is very little or no feedback to enrich the usually very technical information collected and sent (i.e. technical SA information collected by a private organization and sent to NCSC-FI, or threat information sent by NCSC-FI to different actors) and (2) the central nodes are key in information exchange, there has not emerged information exchange between the different actors connected to this central node (i.e. private organizations in a network haven't started to exchange information between themselves, without the governmental actor facilitating the exchange).

Even if the overall networks are not functioning as well as one would hope, there are certain industry networks that provide robust information exchange and even SU-functionalities. Within the interviewed organizations, at least energy infrastructure and telecommunications industries function as a network when it comes to cyber incidents. There are different drivers for these two industries: (1) the energy infrastructure industry is not in direct competition between the different parties, the industry consists of local monopolies, so information sharing is not a risk to the businesses, (2) the telecommunications industry is extremely critical to the functions of society and as such is very closely monitored and regulated, this regulation provides a central node to the industry as the NCSC-FI is a trusted central information sharing node. Compared for example to the banking industry, there doesn't seem to be a similar level of trust within the industry, even though it is quite heavily regulated. The issue may be, that there is a very high level of competition and a lot of organizations that are international, this may make building trust difficult. One issue may also be the fact that the largest financial organizations in Finland are overseen by the European Central Bank, instead of a local authority.

A lack of common goals is a big issue in creating shared SU within the context of national cyber security. Although many high-level goals are articulated in the governmental documents, there are very few common goals between the actors. The interviews provided no such goals, that would act as Boyd's (1987) schwerpunkt – the shared, common objective of actions that would direct the actors – but rather the goals were very individualized: the governmental actors viewed the cyber world through their own mandate and legislation, whereas the private actors were driven by their business goals and regulatory requirements.

Shared SU is made harder by a lack of common framework for information and data sharing: there are no guidelines for what type and in what form information should be shared. The NCSC-FI has some technical data gathering solutions, which automate the data collections and provide some analysis by the NCSC-FI, but other than that there are no formalized frameworks. If this information collection is unstructured, there is a risk of data overload, as organizations may be tempted to overshare, especially if regulated to do so. This issue with regulation came up in all the private organization interviews, where the actors suffer under tremendous amounts of regulation from different parties. The banking organization, for example, is regulated by the Financial Supervisory Authority, The European Central Bank and NESA as the main regulators, in addition to this they have certain service related regulation (e.g. PCI-DSS), and guidelines from the NCSC-FI and different laws, such as GDPR. These regulations are often contradictory, with no central authority to consult on them. Co-ordination between the authorities is required.

One major missing point of view, that makes shared SU that much harder to achieve, is the lack of focus on business operations and needs within the governmental actors. Based on the interviews, one gets the feeling that the governmental actors view cyber security almost as separate from the everyday business of the private actors. In the NESA interview, there was a realisation of the problems of attracting private actors out of the scope of regulation to the national networks, but this was the only interview where this dichotomy was articulated. And even then, the solutions were few in forthcoming: how to incentivise the private actors into attending the national cyber security networks if they did not have a regulatory or legislative must?

**Situation Understanding in Cyber Context**

> *"...you always have to keep in mind, that cyber is only one aspect of the whole. We live in an age where everything affects everything else, and cyber is just one of those things."* (VNK SA-office interview.)

The main view of SU in cyber context in the interviews is the reminder, that cyber is just one of the issues affecting these actors. A stark reminder that cyber security is not the sole issue that these organizations are dealing with, the only exception being the NCSC-FI. However, all in all, even as cyber security has gained in importance over the last 10 years, it is still a support function to other organizational operations, be it business or governmental. The organizations always function as wholes and look to fulfil the main goals, which for the private organizations are based on business needs. So, understanding the cyber security situation needs to be framed in the larger context of organizational goals and requirements.

From the interviews, one is tempted to conclude that the external view prevails: it seems to be easier to deal with understanding threats and threat actors, rather than the nitty-gritty of internal ICT-solutions and -operations. This aligns somewhat with Kugler (in Kramer, Starr & Wentz, 2009, 333), who emphasizes the understanding of adversary goals, capabilities and tools. Even if this external view is important, what may be even more important for true SU is the knowledge of an organizations internal functions and technological solutions that support them. This is the message that Tadda & Salerno (in Jajodia et al., 2010, 28.) emphasize, but from the interviews it seems that this aspect is not centralized within the organizations, but rather information is distributed among the experts in charge of these functionalities. When knowledge of these functions or solutions is required, rather than having documentation or understanding of them, an expert is consulted.

Similarly, this same dichotomy of external-vs-internal seems to hold for national level cyber SU as well: the threat environment is followed in almost real-time with different sources and even automatic feeds, threat actors, vulnerabilities etc. are communicated and acted upon. However, the understanding of cyber infrastructure is mainly built either through annual or semi-annual regulatory reporting or built ad hoc relating to an incident or crisis situation. The difficulty in having a strong internal view of infrastructure to base SU on is the complexities involved. Internal situations and infrastructures can range wildly from one another and every organization is different.

For shared SU in a cyber context one would have to sanitize the specifics that might reveal business critical issues or other major vulnerabilities. The level of shared SU information would have to be carefully assessed and sharing guidelines, especially for the governmental actors, would have to be mutually agreed. This is critical to foster trust into the network and its information exchange practices, so that organizations can be sure that no critical information will be shared unnecessarily. A framework, guidelines and implicit trust are some of the basic qualities that a shared SU network requires to be able to function. These issues have been raised by all the private organizations and even mentioned by the governmental ones, even though for them business critical information is not as big an issue as for the private firms.

# 5 CONCLUSIONS AND DISCUSSION

This chapter presents the conclusions based on the guiding principles and empirical study analysis. The research questions are answered in the next chapter and discussion on the study results is presented below as well. Finally, study reliability and validity is discussed.

## 5.1 Conclusions

**Research question:** What does situation understanding comprise within the context of national cyber security?

Cyber security as understood by the studied organizations closely resembles the Libicki (2007) and US Army (2010) three-layered model. Emphasis is on the physical and logical layers; the social layer being reduced to personnel security awareness and not the wider encompassing concept of cyber personas and information warfare. All the studied organizations look at the cyber security field very similarly as the guiding principle cyber security is defined in this study, especially as Andress and Winterfield (2014, 30-32) define cyber defence as a collection of information assurance, computer network defence, incident response and critical infrastructure protection, with the aim of preventing, detecting and responding to outside actor's attempts to deny or manipulate information and/or infrastructure. This is frame of cyber security for all the studied parties: a mix of governance and policy, awareness and technical protections.

National cyber security is defined by the governmental documents analysed in chapter 3.1.2. and is mostly built on the functions vital for society. In modern world, these functions rely on functioning ICT-infrastructure, which brings the studied private organizations into the framework. National cyber security is built on the functions of certain governmental actors and upon the private organizations deemed critical to the functioning of the infrastructure. These include the three industries which were chosen for this study: energy infrastructure, telecommunications and banking. The national cyber security on one hand is the co-operation and co-ordination of these organizations that are deemed critical and on the other hand the cyber security of each of these organizations.

**Research question:** How does situation understanding arise from situation awareness?

Situation Awareness is a key function of overall cyber security for the studied organizations, all are working on SA-systems or -processes to provide insight into their cyber security situation. All the solutions map well against the Endsley (e.g. 1995) SA-process, with the observation- and comprehension-phases present for all actors. The biggest difference comes looking at the comprehension phase, where differences emerge and it is more of a co-operative function in the organizations. The fact is all of these organizations rely on their SA-capabilities to keep them up to date regarding their cyber security. The SA-processes function within the cyber security scope defined in the paragraph above and for all studied organizations this structure seems to be similar.

Situation Understanding and its emergence in these organization diverges between the governmental actors and private organizations: (1) for the governmental organizations SU is a key part of their SA-process, where their SA-process continues beyond the comprehension phase and into projecting the future status and making conclusions based on this projection, (2) for the private actors the SA-process is the responsibility of the cyber security organizations, but the SU emerges through reporting and planning-processes, where the SA-information becomes one part of background information for business and development planning. This may be the reason why the drivers for national cyber security differ so much between governmental and private organizations: business point of view becomes a heavy part of the discussion, even in cyber security SU.

**Research question:** How does situation understanding form in a network of national cyber security actors, through shared situation awareness and understanding?

For shared SU the conclusions are difficult to make: there doesn't seem to be a framework for this level of information within the national cyber security context. The SU-processes seem to diverge between the governmental and private organizations, and after this divergence there are a lot of inhibiting factors to the information exchange. For the private organizations the SU information potentially includes a lot of business insight, which makes sharing very sensitive. This highlights the quality of SU as very context bound and hard to transfer. The national level shared-SU seems to be enabled rather by shared-SA, rather than sharing SU-information. This shared-SA can be facilitated by the governmental actors, as we have seen through the interviews. The telecom example highlights how a trusted intermediary, in this case a governmental agency, funnelling and sanitizing shared information to competitors, can facilitate information exchange. More effort should be afforded by the governmental organizations into building a common information sharing framework, with focus on security and privacy of the information, business benefits for the participants and defined ways of working.

The national cyber security context deals mainly in shared-SA and is quite effective in those areas that are under direct governmental cyber security mandate: in this study the telecommunications industry working in close co-operation with the NCSC-FI and the infrastructure industry has close co-operation within its own field. The banking industry co-ordinates with the regulatory authorities and has co-operation with the NCSC-FI, but the industry cyber security functions are less formalized than the two other industries that were studied. Some of these effects are evaluated in the Discussion-chapter below.

These findings align with the theoretical views on the prerequisites for shared-SA or -SU, for example the factors highlighted by Sweazy and Salas (1992): common goals, interdependency and specialized roles and duties seem to be mostly lacking in the National Cyber context. Endsley & Jones (1997) of defined roles within a group can be seen at least somewhat in the infrastructure and telecommunications industries, where the government has used its heavy hand to regulate and mandate preparedness networks. These issues point towards the lacking structure for both network building and organizational roles within those networks, as well as a lack of framework for information sharing.

To conclude a reminder from one of the interviews, why cyber security needs to be a priority initiative for the national security:

*"Cyberwar is cheap, easy and you cannot be caught"*

## 5.2 Discussion

Based upon a small sample of national cyber security actors drawing concrete conclusions is difficult. The conclusions that arise from abductive research and the interviews are inherently true, but making generalisations based on this thesis only is something that must be done apprehensively. The results from this study point to some factors and influences regarding emergence of shared situation understanding, but to make generalisations would require further study and validation.

The frame of reference between the organizations is consistent, the studied organizations have similar understanding of the studied concepts. Cyber security and national cyber security concepts were similar between all the interviewed actors, in addition all were operating some kind of Situation Awareness system or process. Situation Understanding was understood little differently at the different organizations, this difference and its meaning to this study is elaborated in the next paragraph. Overall, the similarity is a factor that will provide reliability for the results, as we can trust that organizations studied understand the framework of cyber security and national cyber security and view Situation Awareness in a comparable way.

When evaluating the results regarding SA and SU, there is a distinct divergence between them: (1) SA is a concept understood, accepted and practice by all the studied organizations in a very similar way, (2) SU, however, while a concept that is understood and practiced, is not as uniform as the SA functions and emerges very differently between the organizations. The biggest difference seems to be between the governmental and private organizations, due maybe to the required view through business goals and requirements. It may be beneficial for the governmental actors to build a better understanding of the business context of each industry and even each organization. This may be difficult to achieve, especially on an organizational level, but would benefit the national cyber security. One thing is clear: the government must look at co-operation more through the lens of business benefits for the private organizations, rather than through the scope of regulation. Lemieux (2015, 144-147) highlights three major incentives for a company to join cyber security information sharing networks: (1) social approval for co-operative behaviour, (2) reduced costs through increased cyber resilience and (3) access to high-quality information to serve decision-making and operational capabilities. Out of these, number 1 would be fairly easy to produce within the national context, however 2 and 3 require framework for information sharing and high-quality analytical capabilities. These are, however, clearly manageable by the governmental organizations and may be the kind of initiatives that will provide enhanced national cyber security.

There are best practices in place around the world, that could be leveraged in Finland. Moulton, Stavridis and Uthoff (in Lemieux, 2015, 122-125) outline a public-private partnership-based "Federal Cyber Board", that would promote not only cyber security, but the cyber space and related issues as well. Included within the charter for the FCB would be the understanding and fostering of business opportunities within the cyber space as well, this would combine strong business initiatives with the burden of enforcing strong cyber security together. A balance struck between mandatory burdens and business benefits would act as a strong enhancer of trust and co-operation. A similar approach might be beneficial for Finland (or even EU) as well.

The interviews point to some factors that inhibit and benefit information sharing within the national cyber security networks. Factors that seem to benefit information sharing for shared SU:

- Lack of competition
- Trust in confidentiality of information shared
- Confidential governmental authority acting as central node in sharing network
- Confidential personal relationship between experts
- History of preparedness co-operation within industry

Factors that seem to inhibit information sharing for shared SU

- Strong competition between organizations
- International operations
- Lack of regulation and central regulatory authority
- Lack of framework and guidelines for information sharing (what to share and how)

The first factor of inhibiting information exchange, i.e. competition between organizations, seems to point towards the need for stronger governmental requirement to act as a facilitator in the information exchange. The telecommunications industry example backs up this conclusion, as a central node providing trust, privacy and security to the information exchange has enabled a functioning network for cyber security within the industry.

You could also look at the results through dichotomies; where two distinctly opposite choices both bring their own advantages and disadvantages. One might even understand them through Clausewitz's concept of friction (von Clausewitz, 1997, 66-69.), where it is said that: "Activity in war is a movement in resistant medium." It certainly seems to hold true in cyber security as well, where dichotomies of separate choices bring their own frictions and advantages-disadvantages for both ends of the spectrum:

**Private - public**

A private company strives to produce wealth to its owners. All actions are subsidiary to this aim and if a large enough crisis falls upon a private company, it always has the option of liquidating its assets and calling it quits. The public actors have no such option, but rather must keep up the fight until the bitter end. This dichotomy brings distinctly different drivers and possibilities in directing and running cyber security.

**Regulated – Unregulated**

A dichotomy which concerns mostly the private companies, where the ones that are under government regulation through either business functions (e.g. banking) or have been deemed critical for the functions of society and as such are under preparedness regulation (e.g. infrastructure or telecom provider) can be brought under the national cyber security umbrella by government decree. Compare that to businesses that are under no such obligations, free to base their cyber security functions to serve their business functions and those alone. If cyber security is a function that is as strong as its weakest link, then these unregulated actors need to ensure their cyber security at least to a functionable level. How does the government ensure this? There needs to be some combination of the carrot and stick: benefits need to be realized in taking part to national cyber security actions.

**Centralized – Distributed**

One must consider the system to lead the cyber security on a national level: do you push for a centralized bureaucracy or try to build a distributed system, where smaller networks (based around industries for example) are the central unit? For this dichotomy the governments answer seems to lie somewhere in the middle, where governmental and regulated organizations are run through a somewhat centralized system, but for the others a distributed system is in place. The NESA interview highlights the need for cluster intelligence, akin to a school of fish responding to a predator. This dichotomy has been understood within the governmental actors and a lot of though is going to the building of networks, fostering trust and facilitating information sharing.

**National – International**

As modern world becomes more interconnected the national borders mean less each passing day, especially in cyber space. One is drawn towards the conclusion that national level networking, however important, is not enough in the modern world. This seems to be true not only to companies, but governmental actors as well. Cyber-crime is distinctly cross-border activity, information warfare pays little heed to borders and even regulation is becoming increasingly regional, instead of national. An important dichotomy to keep in mind, although mostly out of the scope of this thesis.

## 5.3 Reliability and validity

The scope of the empirical research is limited, so making of sweeping conclusions is risky. Are you able to draw far reaching conclusions from a group of six organizations within a field that includes thousands of actors? One must be careful in generalizing findings from such a scope, but within abductive research method the assumption of validity for the interview material still holds (Grönfors, 2011, 20). However, we must ask how valid are the conclusions made based on the source materials are? And here we should be careful, as the interviews were conducted with a limited amount of organizations.

The issues with the interviewed organizations are real and as such bring valuable insight into the cyber security networks on a national level. As we can see similarities between the theoretical models of the guiding principles and the concepts and frameworks arising from the interviews, we can conclude at least some validity in the results. The fact that the concepts are understood similarly, gives the research and conclusions at least some merit. The issue is rather in making generalizations and wider rules based on the small sample size. This similarity speaks for the reliability of the study as well, even if the information from the interviews will prove to be hard to repeat, the framework that we are working in seems to hold.

Overall, the selected study method of abductive research has been shown to be beneficial with a research topic such as Situation Understanding. The ability to use induction for a topic such as SU, which differs greatly from organization and application to the next, might be limited. Abduction, however, gives the study some leeway in interpreting the results based on guiding principles. The fact that the findings from the interviews must be logical and understood in the context of the guiding principles, give the researcher ability to pose conclusions that seem to be true. The generalizations done based on the conclusions of this study must be limited, and ideally should be supported by further study. (Grönfors, 2011, 17-18.)

Picking the people for the interviews, compromises had to be made, as especially in the private organizations it is very hard to pinpoint persons with a complete, in-depth view to cyber security. Excluding the governmental organizations, the interviewed people oversaw cyber security in some capacity, but the exact responsibilities differ very much in each organization. This fact makes definite conclusions on some issues difficult to make, for example which layer of cyber security is emphasized within each organization. If the person interviewed was in charge of physical infrastructure, then quite obviously, in his answers this aspect will be highlighted. However, overall the interviewees were able in the interview situation look at the issues beyond their own duties, but still some bias may remain.

Overall, the insights and conclusions form this study point towards issues and benefits within the national cyber security framework. The study also has pointed to some factors benefitting and hampering the information exchange and dichotomies in place. To make definite rules or firm generalizations, however, more research is required. But this may be the biggest contribution of this thesis: to highlight issues within the national cyber security to further the understanding and provide ideas as seeds for further study.

## 5.4 Further Research

One major contribution of this thesis is the highlighting of national cyber security and the related networks of public and private actors as a fairly immature field of study, especially in Finland. While making sweeping generalizations and policy initiatives based on this one study would be nonsensical, this thesis has produced quite a few points of view for further study:

- Facilitating co-operation between industry competitors for national cyber security
- Establishing trust between competitors to disclose and share cyber security related info
- Looking at the networks of a single actor, especially a private organization: how and what kind of networks is the organization involved in (customers, service providers etc.)
- Studying a set network of actors that reside within a single network (i.e. organizations that actually co-operate together regarding national cyber security)
- Studying an industry as a national cyber security network
- Looking at the international aspect, how do international business operations affect taking part in national cyber security?
- Evaluating the effect of the dichotomies listed above in the Discussion-chapter
- Building a framework for effective cyber security information sharing network

**SOURCES**

Alasuutari, P., (1999). Laadullinen tutkimus. Vastapaino: Tampere.

Alberts, D. S., Gartska, J. J., Hayes, R. E. & Signori, D. A., (2001). Understanding Information Age Warfare. Washington D.C.: CCRP Publication Series 147.

Andress J. and Winterfeld S., (2014). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Waltham: Elsevier Inc.

Baldwin, D. A., (1997). The Concept of Security. Review of International Studies, Vol. 23, pp. 5-26. Available: http://www.princeton.edu/~dbaldwin/selected_articles/Baldwin_(1997)_The Concept of Security.pdf [Accessed 08.04.2018].

Boyd, J., (1986). Patterns of Conflict. Briefing slides, reproduced by Defence and National Interest, dnipogo.org. Available: http://www.dnipogo.org/boyd/pdf/poc.pdf [Accessed 08.04.2018].

Boyd, J., (1987). Organic Design for Command and Control. Briefing slides, reproduced by Defence and National Interest, dnipogo.org. Available: http://www.dnipogo.org/boyd [Accessed 08.04.2018]

Boyd, J., (1995). The Essence of Winning and Losing. Briefing slides, reproduced by Defence and National Interest, dnipogo.org. Available: http://pogoarchives.org/m/dni/john_boyd_compendium/essence_of_winning_losing.pdf [Accessed 08.04.2018].

Chapple, M. & Seidl, D. (2015). Cyberwarfare: Information Operations in a Connected World. Jones & Bartlett Learning: Burlington, MA.

von Clausewitz, C. (1997). On War. Wordsworth Editions Limited: London.

The Comprehensive National Cyber Security Initiative, (2009). Available: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf [Accessed: 08.04.2018]

The Constitution of Finland 1999/731. Enacted in Helsinki 11.6.1999. Available: http://www.finlex.fi/en/laki/kaannokset/1999/en19990731

Coram, R. (2002). Boyd: The Fighter Pilot Who Changed the Art of War. Back Bay Books: New York, NY.

Endsley, M. R. (1988). Design and Evaluation for Situation Awareness Enhancement. Proceedings of the Human Factors and Ergonomics Society Annual Meeting. Vol 32, Issue 2.

Endsley, M. R., (1993). Situation Awareness and workload: Flip sides of the same coin. Proceedings of the 7th International 212 Symposium on Aviation Psychology.

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors. Vol 37 (1), 32-64.

Endsley, M. R. & Garland, D. J. (2000). Situation Awareness Analysis and Measurement. Mahwah, NJ: Lawrence Erlbaum Associates.

Endsley, M. R, & Jones, W. M., (1997). Situation Awareness, Information Dominance and Information Warfare. Wright-Patterson AFB, OH: United States Air Force Armstrong Laboratory.

Feibelman, J. K., (1960). An Introduction to Peirce's Philosophy. London: George Allen & Urwin.

FICORA, (2018). Cyber security. Available: https://www.viestintavirasto.fi/en/cybersecurity.html [Accessed: 08.04.2018].

Finnish Government, (2006). The Strategy for Securing the Functions Vital to Society. Government Resolution 23.11.2006. Available: http://www.defmin.fi/files/858/06_12_12_YETTS__in_english.pdf [Accessed 08.04.2018].

Finnish Government, (2010). Security Strategy for Society. Government Resolution 16.12.2010. Available: http://www.defmin.fi/files/1883/PDF.SecurityStrategy.pdf [Accessed 08.04.2018].

Finnish Government, (2013). Finland's Cybersecurity Strategy. Government Resolution 24.1.2013. Available: http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf [Accessed 08.04.2018].

Finnish Government, (2017). Security Strategy for Society – Update 2017. Government Resolution 2.11.2017. Available: https://www.turvallisuuskomitea.fi/index.php/files/35/YTS2017%20materiaalit/80/YTS_2017_suomi.pdf [Accessed: 08.04.2018]

Friis, K. & Ringsmose, J. (eds.), (2016). Conflict in Cyber Space - Theoretical, strategic and legal perspectives. New York: Routledge.

Gibson, W., (1984). Neuromancer. New York, New York: Ace Books.

Garland, D. J, Wise, J. A. & Hopkins, V. D. (eds.), (1999). Handbook of Aviation Human Factors. Mahwah, NJ: Lawrence Erlbaum Associates.

Grönfors, M., (2011). Laadullisen tutkimuksen kenttätyömenetelmät. SoFia – Sosiologi-Filosofiapu Vilkka: Hämeenlinna.

Hirsjärvi, S., Remes, P. & Sajavaara, P., (2015). Tutki ja kirjoita. Porvoo: Bookwell Oy.

ITU-T Study Group. (2008). Overview of cybersecurity, Series X: Data Networks and Open System Communications and Security. ITU-T Recommendation X.1205, April 2008.

Jajodia, S., Liu, P., Swaruo, W. & Wang, C., (2010). Cyber Situational Awareness – Issues and Research. New York: Springer US.

Johnson, S. & Libicki, M. (eds.), (1995). Dominant Battlespace Knowledge: The Winning Edge. Washington D.C.: NDU.

Kaufmann M., (2013). Emergent self-organization in emergencies: Resilience rationales in interconnected societies. Resilience: International Policies, Practices and Discourses 1(1), 53-68.

Klimburg, A. (ed), (2012). National Cyber Security – Framework Manual. Tallin: NATO CCD COE Publication.

Kosola, J. & Solante, T., (2013). Digitaalinen taistelukenttä – Informaatioajan sotakoneen tekniikka. National Defence University: Department of Military Technology. Publishing series 1, No. 35.

Kott, A. (ed.), (2008). Battle for Cognition – The Future Information-rich Warfare and the Mind of the Commander. Westport: Greenwood publishing.

Kramer, F. D., Starr, S. H. & Wentz, L. K. (eds.), (2009). Cyberpower and National Security. Dulles: Potomac Books.

Lehto, M. & Limnéll, J., (2017). Kybersodankäynnin kehityksestä ja tulevaisuudesta. Tiede ja ase. Vol 75 (2017): pp. 179-212. Available: https://journal.fi/ta/article/view/67730 [Accessed: 08.04.2018].

Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, T. & Salminen, M., (2018). Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018.

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T. & Salminen, M., (2017). Suomen kyberturvallisuuden tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017.

Lemieux, F. (ed.), (2015). Current and Emerging Trends in Cyber Operations. Houndmills: Palgrave Macmillan.

Libicki, M. C., (2007). Conquest in Cyberspace: National Security and Information Warfare. New York: Cambridge University Press.

Limnéll, J., Majewski, K. & Salminen, M, (2015). Cyber Security for Decision Makers. Jyväskylä: Docendo.

National Security Presidential Directive / NSPD 54, Cyber Security and Monitoring. The White House. Available: https://fas.org/irp/offdocs/nspd/nspd-54.pdf [Accessed: 08.04.2018]

NESA, (2018). National Emergency Supply Agency – Organization. Available: https://www.nesa.fi/organisation/ [Accessed: 08.04.2018].

Nofi, A. A., (2000). Defining and Measuring Shared Situation Awareness. Centre for Naval Analysis. November 2000: The CNA Corporation.

Panteli, M. & Kirschen, D, (2015). Situation awareness in power systems: Theory, challenges and applications. Electric Power Systems Research 122.

Peirce, C. S., (1931-1958). Collected Papers, Vols. 1-8. Cambridge Mass.:Harvard University Press.

Peirce, C. S., (1958). Values in a Universe of Change: selected writings of Charles S. Peirce. Stanford: Stanford University Press.

Rantapelkonen, J. & Koistinen, L., (2016). Pohdintoja sotatieteellisistä käsitteistä. National Defence University: Department of Warfare. Publishing Series 2: Research Reports No. 1.

Rantapelkonen, J. & Salminen, M. (ed.), (2013). The Fog of Cyber Defence. National Defence University: Department of Leadership and Military Pedagogy. Series 2: Article Collection n:o 10.

Richards, C., (2004). Certain to Win: The strategy of John Boyd, Applied to Business. Xlibris Corporation.

Robinson, N., Disley, E., Potoglu, D., Reding, A., Culley, D., Penny, M., Botterman, M., Carpenter, G., Blackman, C. & Millard, J., (2012). Feasibility Study for a European Cybercrime Center. RAND Europe. Available: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre_en.pdf [Accessed: 08.04.2018].

Rothschild, E., (1995). What is Security?. Daedalus, Vol. 124, No 3, pp. 53-98. Available: https://www.peacepalacelibrary.nl/ebooks/files/Rothschild_What-is-security.pdf [Accessed 08.04.2018].

Security Committee, (2017a). Implementation Programme for Finland's Cyber Security Strategy. Available: https://www.turvallisuuskomitea.fi/index.php/en/component/k2/132-implementation-programme-for-finland-s-cyber-security-strategy-for-2017-2020. [Accessed: 08.04.2018]

Security Committee, (2017b). Security Committee. Available: https://www.turvallisuuskomitea.fi/index.php/en/security-committee. [Accessed 08.04.2018].

Sinkkonen, I., Kuoppala, H., Parkkinen, J., & Vastamäki, R., (2006). Käytettävyyden psykologia. Helsinki: IT Press.

Sirén, T. (Ed.), (2011). Strateginen kommunikaatio ja informaatio-operaatiot. National Defence University: Department of Leadership and Military Pedagogy. Publishing Series 2: Article Collection 7.

Sun-Tzu, (2002). The Art of War. Penguin Books. London: England.

Sweazy, R. & Salas E. (eds.), (1992). Teams: Their Training and Performance. Norwood, NJ: Abex, 3-29.

Tuomi, J. & Sarajärvi, A., (2002). Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Tammi.

United Kingdom Cabinet Office, (2011). The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf [Accessed: 08.04.2018]

United Kingdom Ministry of Defence, (2016a). Cyber Primer 2nd edition. Development, Concepts and Doctrine Center. Available: https://www.gov.uk/government/publications/cyber-primer [Accessed 08.04.2018].

United Kingdom Ministry of Defence, (2016b). Understanding and Decision-making. Development, Concepts and Doctrine Center. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/584177/doctrine_uk_understanding_jdp_04.pdf [Accessed 08.04.2018].

US Army, (2010). Cyberspace Operations Concept Capability Plan 2016-2028. Tradoc Pamphlet 525-7.8. Available: https://fas.org/irp/doddir/army/pam525-7-8.pdf [Accessed 08.04.2018].

Vankka, J. (ed.), (2013). Cyber Warfare. National Defence University: Department of Military Technology. Series 1: No. 34 Helsinki.

Vankka, J. (ed.), (2015). Situation Awareness for Critical Infrastructure Protection. National Defence University: Department of Military Technology. Series 3, Working papers No:1.

Wickens, C. D., (2008). Situation Awareness: Review of Mica Endsley's 1995 Articles on Situation Awareness Theory and Measurement. Human Factors. The Journal of the Human Factors and Ergonomics Society. Vol. 50, p. 397-403.

Wolfers, A., (1952). 'National Security' as an Ambiguous Symbol. Political Science Quarterly: 67, pp. 481-502.

**APPENDIX**

**APPENDIX 1: List of governmental actors and their designation in Finnish**

The governmental actors related to national cyber security and mentioned within the thesis. Listed is the current organizations title and abbreviation in English and their Finnish title (as of 04/2018).

**FICORA – Finnish Communications Regulatory Authority** - Viestintävirasto
**Financial Supervisory Authority** - Finanssivalvonta
**Government ICT Centre** - Valtori
**Governmental Situation Awareness Office** – Valtioneuvoston Tilannekuvatoimisto
**Ministry of Defence** - Puolustusministeriö
**NCSC-FI – National Cyber Security Center Finland** - Kyberturvallisuuskeskus
**NESA – National Emergency Supply Authority** - Huoltovarmuuskeskus
**NESO - National Emergency Supply Organisation** - Huoltovarmuusorganisaatio
**The Secretariat of the Security Committee** – Turvallisuuskomitean sihteeristö
**The Security Committee** - Turvallisuuskomitea