LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

Cyber threats against critical infrastructure - Is there a need for national programme?

Mäkinen, Jani

2016 Leppävaara

Laurea University of Applied Sciences
Leppävaara

Cyber threats against critical infrastructure - Is there a need for national programme?

Jani Mäkinen
Degree Programme in
Security Management
Bachelor's Thesis
May, 2016

Laurea University of Applied Sciences **Abstract**
Leppävaara
Degree Programme in Security Management

Jani Mäkinen

Cyber threats against critical infrastructure – Is there a need for national programme?

Year 2016 Pages 62

This thesis was written as part of studies in the Degree Programme in Security Management at LAUREA University of Applied Sciences and this work was commissioned by the National Emergency Supply Agency.

The aim of this thesis is to examine if there is a need for a national cyber security programme for critical infrastructure called KYBER 2020 programme, implemented by the National Emergency Supply Agency with cooperation with the National Emergency Supply Organisation and the Finnish Communications Regulatory Authority. In addition to that this thesis examines what are the major reasons for the implementation of this programme.

Another goal of this thesis was to develop an evaluation framework for the KYBER 2020 programme, by using two evaluation tools, Logic model and Key Performance Indicators. However, the writing process of this thesis does not focus on the development process of the evaluation framework, but it focuses to the reasons behind the implementation of the KYBER 2020 programme.

This thesis is a qualitative research and two research methods were used during the process, literary review and interviews.

The results of this thesis indicate that the cyber threats against critical infrastructure are increasing and becoming more noticeable and therefore there is a need for a national programme, such as KYBER 2020 programme. The main reason for implementing KYBER 2020 programme is that Finland's Cyber Security Strategy and its implementation programme is not taking on consideration the protection of the critical infrastructure against cyber threats sufficiently enough.

Keywords: Critical infrastructure, cyber security, cyber threats, evaluating

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Programme in Security Management

Jani Mäkinen

Kriittiseen infrastruktuuriin kohdistuvat kyberuhkat - Onko tarvetta kansalliselle ohjelmalle?

Vuosi 2016 Sivumäärä 62

Tämä opinnäytetyö on kirjoitettu osana opintoja LAUREA - ammattikorkeakoulun englanninkielisessä turvallisuusalan koulutusohjelmassa ja tämä työ on tehty Huoltovarmuuskeskuksen toimeksiannosta.

Tämän opinnäytetyön tarkoituksena oli tutkia tarpeita kriittiseen infrastruktuuriin kohdistuvalle kansalliselle kyberturvallisuusohjelmalle nimeltään KYBER 2020 – ohjelma, jota toimeenpanee Huoltovarmuuskeskus yhteistyössä Huoltovarmuusorganisaation ja Viestintäviraston kanssa. Näiden lisäksi opinnäytetyö pyrkii selvittämään mitkä ovat suurimmat syyt tämän ohjelman toimeenpanolle.

Tämän opinnäytetyön toisena tavoitteena oli luoda arviointiviitekehys KYBER 2020 – ohjelmalle hyödyntäen kahta työkalua, loogista mallia sekä keskeisiä suorituskykymittareita (Key Performance Indicators). Kuitenkin, tämä opinnäytetyö ei keskity arviointiviitekehyksen luomisprosessiin, vaan keskittyy enemmän tarpeisiin KYBER 2020 – ohjelman toimeenpanolle.

Tämä opinnäytetyö on laadullinen tutkimus jossa käytettiin kahta tutkimusmenetelmää, kirjallisuuskatsausta ja haastatteluja.

Tämän opinnäytetyön tulokset osoittavat, että kyberuhkat kriittistä infrastruktuuria kohtaan kasvavat sekä ovat huomattavia ja KYBER 2020 – ohjelman kaltaiselle kansalliselle ohjelmalle on tarvetta. Pääsyy KYBER 2020 – ohjelman toimeenpanolle on se, että Suomen Kyberturvallisuusstrategia ja sen toimeenpano – ohjelma eivät riittävän voimakkaasti ota huomioon kriittisen infrastruktuurin suojaamista kyberuhkilta.

Asiasanat: Kriittinen infrastruktuuri, kyberturvallisuus, kyberuhkat, arviointi

Table of contents

1 Introduction

It is Friday morning, 1st of February 2016, temperature is approximately -30 degrees Celsius and it is a normal winter day in a small village in Finland. The television is on the news and an elderly woman who lives just outside of the village is preparing lunch for her husband.

Suddenly, lights go out. First thought of the woman is that there is nothing to worry about, this happens from time to time and the lights will come back eventually. Even the weather appears to be normal. As the day turns in to night the elderly couple is still without electricity and it is starting to get cold inside. Even though, there are fireplaces in the house, the couple had decided to not to warm their house with wood anymore due the reason that they are getting older and they simply do not have the strength to chop and carry the wood. Even if they would decide to heat the house, they do not have any wood at the time. The only cell phone that the couple have was supposed to be charged in the evening, but it is not possible anymore. The phone goes dead since there is no electricity coming from the charger. As the day turns in to night, the couple is forced put more clothes on and the temperature keeps getting lower in the house.

The night turns in to morning, still no electricity. The couple is getting worried, but it is impossible to leave the house because the couple is disabled and the car will not start without if not heated first. The house is getting colder and it is now freezing inside the house. According to The Security Committee's publication Sähköriippuvuus modernissa yhteiskunnassa, it takes approximately 30 hours to a small wooden house to reach zero temperature when the heating is cut off, when there is -20 degrees Celsius outside. (The Security Committee. 2015, 55)

Suddenly, the man falls in the kitchen, something snaps in his leg and after that the man feels excruciating pain. The woman gets scared, house is freezing cold, her husband just hurt himself and there is nothing they can do. Saturday is turning in to night and the man is getting weaker, the leg is changing colour and both of them are shivering from cold. In the middle of the night, the woman wakes up from her sleep and she turns to watch her husband. At first, she thinks that he is sleeping peacefully, but then she wonders why there is no steam coming out of his mouth as he sleeps. Woman comes closer to the man and suddenly realizes that he is not breathing. The woman is panicking and she is trying to do something to save her husband, but the temperature and the tiredness are overwhelming and eventually only thing she can do is to sob as she embraces her husband's cold body.

It is Sunday, woman is cold and tired, the whole day goes agonizing slowly by and woman is clearly noticing that her strengths are getting weaker. For a moment she thinks that she

would try going the village, but in this condition it would be lethal. She decides to stay with her dead husband and wait for the same destiny.

Monday morning, suddenly television opens and lights come back on again. There is news that covers the incident that occurred last Friday. Finnish Prime Minister is telling that two days ago, 1st of February 2016, the cyberattacks causing power outages took place in when Finnish electricity distribution company reported that their service is out of order. These outages occurred when a third party illegally entered in to the company's computer systems and remotely controlled the systems. These cyberattacks caused the whole weekend long disconnection in to the distribution of electricity. The Prime Minister is speaking in a soothing voice and convincing that the worst is over and electricity distribution is working as usual now. As the minister continues his speech, two figures are embracing themselves in a still position and there is no living soul in the house that could hear the prime minister's speech anymore.

Naturally, this story was fictional and this incident has never occurred in Finland. However, in the incident which happened in Ukraine in December 2015 this could have been possible. According to the Electricity Information Sharing and Analysis Center's publication Analysis of the Cyber Attack on the Ukrainian Power Grid, the cyberattacks against Ukrainian power grid in December 2015 caused an interruption of electricity supplies to hundreds of thousands of customers. Even though the power cut lasted only a few hours this raises up the worrying dilemma, the physical effects of cyberattacks, as described in the story at the beginning. This cyberattack is considered to be the first publicly acknowledged event that has caused power outages. (Lee, R., Assante, M., Conway, T. 2015, 1-3)

The only different aspect, when comparing this fictional scenario to the cyberattack in Ukraine was that the power outage was shorter, only few hours. However, the scenario is real. Cyber threat is evident and the day when human lives are lost by the cause of cyberattack is getting closer and closer.

The vital functions of the society are hugely dependable of how businesses are protected against the cyber threats. Majority of critical infrastructure is owned or operated by the private sector and disturbances caused by a cyberattack of another nation or a criminal organisation can have a major effect to the society. For instance, this fictional story is related to the electricity distribution which is a vital service for the society and the companies who are providing this service are considered as critical infrastructure.

One can only imagine what kind effects of a successful cyberattack against, for example, Finnish health care systems can have. It is actually estimated that within the next three years cyberattacks against critical infrastructure can cause loss of lives. (The Aspen Institute & Intel

Security. 2015, 3) Cyber security is not only protecting networks from attacks, but it includes the protection of the people whose physical wellbeing is somehow connected to those networks.

This thesis was commissioned by the National Emergency Supply Agency and the focus of this work is to figure out the reasons behind the KYBER 2020 programme and how the activities of this programme can or should be evaluated.

Therefore, this thesis focuses on the protection of the critical infrastructure against cyber threats in Finland and considers if our nation has taken enough measures in this matter. This thesis also introduces new national cyber security programme, called "KYBER 2020", designed and implemented by the National Emergency Supply Agency (NESA) with cooperation with the National Emergency Supply Organisation (NESO) and The Finnish Communications Regulatory Authority (FICORA). This programme is aimed to the critical infrastructure in Finland.

This thesis also suggests two commonly known management tools, Logic model and Key Performance Indicators, in order to successfully evaluate and monitor the activities of the KYBER 2020 programme.

However, this thesis does not concentrate on to the development process of the evaluation framework. The main focus in this thesis is the reasons behind the KYBER 2020 programme. By choosing this approach this thesis will be much more interesting and it also serves the needs of the National Emergency Supply Agency much better.

The research questions for this thesis are:

Is there a need for a national programme, called KYBER 2020 programme, for protecting critical infrastructure against cyber threats in Finland?

How the effectiveness of the KYBER 2020 programme should be evaluated?

1.1 Key concepts and definitions

From the following the key concepts related to this document will be briefly introduced and shortly explained. All the cyber related terms were gathered from Finland's Cyber Security Strategy excluding the term cyberattack, which was not defined in the strategy.

Cyber Attack

The term cyberattack is not defined in Finland's Cyber Security Strategy, therefore the definitions is adopted from the National Information Assurance Glossary of Committee on National Security Systems (CNSS). According to the glossary, cyberattack is an attack through cyber domain which is targeted to the enterprise's usage of the cyber domain in order to disrupt, disable, destroy or controlling the computing environment and infrastructure with malicious manner or stealing information or compromising the integrity of the data. (Committee on National Security Systems. 2010, 22)

Cyber Security

Cyber security means the desired end state in which the cyber domain is reliable and in which its functions are ensured. At this end state the cyber domain does not cause any harm or disturbance to the functions that are dependent on the handling of electronic information in cyber domain. Cyber security contains actions that are targeted to the vital functions of the society and critical infrastructure and the goal of these actions are to reach the ability to proactively control and if necessary tolerate cyber threats and the impacts of those cyber threats on the vital functions of society. (Finland's Cyber Security Strategy. 2013, 12)

Cyber Risk

Cyber risk means a possibility of damage or accident against cyber domain which, if realizes or being utilized, can cause harm, disturbance or damage to the functions dependent on the cyber domain. (Finland's Cyber Security Strategy. 2013, 12)

Cyber Threat

Cyber threat means a possibility of an event or action in cyber domain, when realized, can endanger those functions which are dependent on the cyber domain. (Finland's Cyber Security Strategy. 2013, 12)

Cyber Domain

Cyber domain is an operational environment which is formed by one or more technology infrastructures for electronic information. (Finland's Cyber Security Strategy. 2013, 12)

Critical Infrastructure (CI)

Critical infrastructure includes all the functions and structures that are vital in order to maintain the functions of the society. Critical infrastructure comprises of both, physical facilities

and structures and also digitalized functions and services of the society. (Finland's Cyber Security Strategy. 2013, 12)

Critical Information Infrastructure (CII)

Finland's Cyber Security Strategy defines Critical Information Infrastructure as those structures and functions of information systems that are the basis of vital functions of society. Critical Information Infrastructure comprises electronic functions and physical facilities. (Finland's Cyber Security Strategy. 2013, 12)

Critical Infrastructure Protection (CIP)

Critical infrastructure protection means all the activities which are aimed to confirm the functionality, continuity and integrity of critical infrastructure in order to reduce or mitigate threats, risks and vulnerabilities. (2008/114/EC article 2. 2008, article 2)

Security of Supply

According to Governments Decision on the Security of Supply Goals, security of supply means safeguarding the livelihood of the people, economics, and most critical production for the national military defence, services and infrastructure of society in severe emergency situations. (Valtioneuvoston päätös huoltovarmuuden tavoitteista. 2013, 1)

2 Literary review

In this chapter, key documents related to the subject of the thesis are presented. The focus of the material presented is related to cyber security and critical infrastructure.

2.1 Critical infrastructure & Critical infrastructure protection

There are many definitions of critical infrastructure and almost every country has one of its own. However, the main concept of the critical infrastructure is the same, therefore there is no need to collect different definitions from various sources and in this paragraph the definitions of critical infrastructure are chosen from Finnish and European Union point of view.

According to a European Union's COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, critical infrastructure is "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, secu-

rity, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions;". (2008/114/EC. 2008, article 2)

Finland's Cyber Security Strategy states that critical infrastructure includes all the functions and structures that are vital in order to maintain the functions of the society. Critical infrastructure comprises of both, physical facilities and structures and also digitalized functions and services of the society. (Finland's Cyber Security Strategy. 2013, 12)

According to Hagelstam, critical infrastructure means those structures and functions which are necessary for the continuous functions of the society. Critical infrastructure is comprised of physical facilities and structures, but also electronical functions and services. Securing these functions means finding the individual vulnerabilities and securing them without compromising the functionality of the infrastructure. (Hagelstam. 2005, 16)

The concept of critical infrastructure protection started from the United States in the middle of the 1990's. In the USA it was noticed that different sectors of infrastructure are interconnected with each other even more than before. (Hagelstam. 2005, 14) Technological development in different sectors of society has caused the situation where many sectors critical infrastructures are increasingly dependent on each other. (Hagelstam. 2005, 18)

Critical infrastructure protection has three dimensions. These dimensions are political dimension, economic dimension and technical dimension. The political dimension has emerged from the common interests of different countries to protect infrastructure systems and through that there has been more cooperation between countries. (Hagelstam. 2005)

Political dimension is comprised of national legislation and national needs for the protection of the critical infrastructure and international cooperation around these structures. With international cooperation the countries that have common interests are thriving to make similar solutions and with common security policies and regulations between countries, the countries are able to conduct cooperation especially when the infrastructures are belonging to the both countries. (Hagelstam. 2005)

Economical dimension includes all those companies and economical entities that are involved with constructing, owning and controlling infrastructure systems and facilities. The equitable sharing of the costs of securing the functions between different actors also belongs to the economical dimension. (Hagelstam. 2005)

Technical dimension is comprised of the technical development and the practical solutions and actions which are made by the governments and companies in order to protect the functionality of the critical infrastructure. (Hagelstam. 2005)

In order to protect critical infrastructure all of these dimensions have to be in harmony and the cooperation between different actors has to be smooth. Therefore, the cooperation between public and private sector is crucial. (Hagelstam. 2005, 16)

In Finland the critical infrastructure protection is explained in the Government's Decision on the Security of Supply Goals, which states that the National Emergency Supply Agency with cooperation with the Security Committee, other authorities, businesses and other organisations gathers and maintains up to date information about production, services and infrastructures which is vital for the security of supply.

The National Emergency Supply Organisation promotes the business continuity of the critical infrastructure and the ability to recognise the critical dependencies, risks and changes. The functions of the security of supply are carried out with cooperation between public authorities and private sector. (Valtioneuvoston päätös huoltovarmuuden tavoitteista. 2013, 1-2)

This Governments decision is defining vital critical functions and dividing them into two sections which are critical infrastructure services and critical production. The critical infrastructure services are comprised of production of energy, data communications systems, networks and services, services in financial field, transport and logistics, supply of water, construction and maintenance of infrastructure and in special conditions waste management. Critical production consists of, food supply, health care and basic services, industry and production and services supporting military defence (Valtioneuvoston päätös huoltovarmuuden tavoitteista. 2013, 1-9)

When considering cyber threats against critical infrastructure, according to this decision critical infrastructure is obligated to take on consideration in their continuity planning the cyber threats which are directed to them and also maintain sufficient protective measures, the National Emergency Supply Agency and National Emergency Supply Organisation will support critical infrastructure in their actions by the means of reporting, instructions and training. (Valtioneuvoston päätös huoltovarmuuden tavoitteista. 2013, 4)

2.2 Cyber threats against critical infrastructure

A survey, called "Critical Infrastructure Readiness Report – Holding the Line Against Cyber Threats", aimed to particularly towards critical infrastructure in United States, Germany,

France and United Kingdom and commissioned by Intel Security and the Aspen Institute reveals what are major trends in the future of cyber security. The participants of this survey were major IT decision makers from 625 public and private critical infrastructure organisations. There were five major findings what the survey is representing.

Firstly, even though data breaches are increasing, the majority of IT executives believed that the defence systems of their organisation were in good or excellent state. Almost 80 % of the respondents are seeing that cyber security in general is either greatly or extremely concerning and the attacks against critical infrastructure shows no decrease, yet all of the respondents are stating that they are feeling less vulnerable than three years ago. The survey however notes that could be only a misconception on behalf of the respondents and IT executives might have too much overconfidence what becomes to their capabilities, despite the fact that cyber incidents has increased lately throughout the world. The major threat seen among the respondents comes from non-nation state actor, such as hacktivists, ransomware, and data thieves.

Secondly, even though, according to the survey, many of the attacks against critical infrastructure can be under way for weeks or even months before initial detection, yet almost 75 % of the respondents were confident that they have the ability to identify cyberattacks and almost 70 % of the respondents were confident that they can mitigate and deflect the attacks as well.

70 % thinks that cyberattacks are becoming more frequent and almost 90 % have experienced at least one severe attack in recent years. What might come as surprise to some readers, 59 % of the attacks caused physical damage to the organisation, 33 % service disruption and 25 % initiated data compromise. According to survey, the amount of increased and successful cyberattacks against critical infrastructure is indicating that the confidence level of the organisations might decrease in the future, at least from those who are experiencing more attacks than the others.

Another interesting fact is that 48 % of the respondents believe that cyberattack against critical infrastructure can indirectly cause loss of life in some point. 64 % believe that this has not happened yet due to the effectiveness of the IT security and 12 % believe that attack methods are not yet to be sophisticated enough.

Due the overwhelming confidence of the respondents, survey is putting on a reminder towards the critical infrastructure that they make sure to live up to expectations by taking all the necessary measures in order to live up to the answers.

Thirdly, businesses are usually reluctant to cooperate with public sector because of the conception businesses have towards public sectors ability to improve process or situation, but when it comes to cyber security, critical infrastructure IT executives are confident that international organisations, governments and national agencies can bring value to the fight against cyber threats. Over 80 % of the respondents believe that key for a successful cyber defence is cooperation between public and private sector. When considering, which are the main obstacles of successful cooperation between public and private sector respondents' stated three things; lack of budget, different perspectives of cyberattacks among the organisations and the lack of other necessary resources. When asked about the forms of cooperation, the respondents were open to all suggestions which the survey provided, such as creating joint public-private councils and sharing network and defence information with other organizations in the same industry or a national or international agency.

Fourth, in next three years a successful cyberattack will take down critical infrastructure and will end up causing a loss of life, especially U.S. and French respondents believed this to be very or extremely likely.

Fifth, IT executives still believe that human factor is still the weakest link and ranked the most potential cause of a successful cyberattack. Even though cyber security companies are warning its customers about the threat of BYOD (Bring your own device) and the diversity of devices can serve as a potential attack vector, respondents still see that the lack of awareness, use of social media and use of unofficial online sites are the three major threats in organisations. (The Aspen Institute & Intel Security. 2015, 3-7)

Like this survey points out, the cyber threats against critical infrastructure are growing and almost every organisation participated in to this survey had experienced cyberattacks. Another interesting fact is the physical effect of the cyberattack. Due the reason that all the fields of critical infrastructure are connected in to networks leaves us the issue that someday a successful cyberattack will cause a loss of life. One relieving fact is that IT executives are feeling confident of their level of cyber security. However, the survey also points out the importance of cooperation between public and private sector and how the respondents are willing to participate in to this kind of collaboration.

According to Europol's publication The Internet Organised Crime Threat Assessment 2015 (IOCTA 2015), cyber threats against critical infrastructure are constantly evolving and needs to be addressed in order to protect societies and economies. Weak network security, lack of knowledge regarding the automated computer systems and difficulties to update systems in critical infrastructure indicates that there will be more efforts to exploit the vulnerabilities of critical infrastructure. The possibilities, which the Internet provides gives attackers a possibil-

ity to operate globally and the characteristics of these threats are increasingly becoming non-state actors, organised groups or individuals. On the other hand, losses of control over its technology, the need for having the accessibility online and foreign ownerships are also factors which can be a threat to the critical infrastructure. Critical infrastructures interdependence on power grid, telecommunications, information systems and electronic data will increase, and alongside the possibilities to conduct cyberattacks to these different structures will increase as well.

This Europol's threat assessment also provides some recommendations in order to tackle the cyber threats against critical infrastructure and one of the main message, like previous survey is also appointing, is that the cooperation between public authorities and private sector is necessary when addressing the vulnerabilities of critical infrastructure. (Europol. 2015, 44-45)

2.2.1 Examples of cyberattacks from the world

As there was a mention in the introduction part of this thesis about the cyberattack against Ukrainian power grid, there are naturally also other examples cyberattacks against critical infrastructure throughout the world. In the following, few examples are presented.

In Germany in year 2014, attackers gain access to the steel plants office production network and through that successfully caused outages to the production machines. These outages caused physical damage to the plant due the reason that the plant was unable to shut down a blast furnace (Eduard Kovacs. 2014)

Once again in Germany in this year, a German hospital's computer systems were planted malicious software by hackers, which eventually caused computer servers to go offline. After the attack all the data in the computer systems were inaccessible and that led in to the situation where hospital staff was forced to rely on pen and paper when exchanging the information about the patients. Also, high risk surgeries were forced post-pone due to this attack. (Sarah Steffen. 2016)

In Bangladesh, a group of hackers planted malicious software to be targeted to Bangladesh Bank officials, in order to gain insights how the bank conducts transactions. After that the hackers stole money from the bank by making series of transfers from banks account at the Federal Reserve Bank of New York. These actions were seized after Deutsche Bank noticed a misspelling in a hackers request to the Federal Bank of New York. Before that, hackers were able to steal 81 million dollars from the bank. (Arafat Kabir. 2016)

In Finland at the end of the year 2014, a Finnish financial services group called OP – Pohjola received distributed denial – of – service attacks that forced OP – Pohjola to shut down its banking services. Group of hackers called CoreSec took the responsibility of the cyberattack and posted to Pohjola's Facebook page and demanded 35000 dollars' worth of bitcoins to call off the attack. (Mathew J. Schwarts. 2015)

As we can see from these few examples, cyber threats are real in many fields of critical infrastructure and Finland is not an exception with these matters.

2.3 Finland's cyber security landscape

In the following subchapters, Finland's cyber security landscape concerning critical infrastructure is presented.

2.3.1 Finland in GCI and EU Cyber Security Dashboard

The Global Cyber Security Index (GCI) is a joint project between ABI research and International Telecommunications Union (ITU) which provides insights of cyber security issues within the nations worldwide. The aim of the index is to reveal in what level countries are in their cyber security and GCI inspects the state of commitment of the nations in cyber security in five different areas. These areas are legal measures, technical measures, organizational measures, capacity building and international cooperation. The results of these five areas appear as country's global ranking and what the country-level index is. (ABI Reseach. 2015,1)

Finland is in eighth position in a GCI, however there are many countries that are ranked in to same position and Finland can be found in a 24th position if the countries are counted for top to bottom. In Europe, Finland is ranked fifth, but again if we count the countries, Finland is actually in 12th position. (ABI Reseach. 2015,2)

Key findings in Finland cyber wellness profile related to private sector are that GCI recognises the National Emergency Supply Agency as organising preparedness of critical infrastructure, but for example Finland does not have any officially identified cyber security programmes or projects that can be applied to public or private sector. Finland does not either have any officially identified national or sector specific programmes in order to share cyber security information and assets between the public and private sector. (ABI research.2015, 194-195)

EU Cyber Security Dashboard, released in year 2015, is a report that gives insights of what is the state of cyber security in European Union member states. The report has chosen five key areas to examine in order to build a comprehensive image of cyber security frameworks and

capabilities of each and every member state. These areas are legal foundations in cyber security, operational capabilities, public-private partnerships and sector specific cyber security plans (BSA. 2015, 1-4)

The key findings of the report regarding private sector in Finland are that once again the National Emergency Supply Agency is recognised as a key player when protecting critical infrastructure and the Governments decision on the Security of Supply Goals is considered as national plan to address the protection of the critical infrastructure. However, when considering does Finland have any defined public – private partnerships, the report only partially recognises the National Emergency Supply Organisation as an entity that defines the public-private partnerships in cyber security and when considering if Finland has any public-private partnerships plans that addresses the cyber security, the report is referring yet again to the Governments Decision on the Security of Supply Goals, but still underlines that Finland does not have public-private sector plans at the moment. (BSA country report)

In general, the report addresses the importance of the public – private partnerships and is referring to the fact that most of the critical infrastructure is owned by the private sector and by increasing the public-private partnerships in member nations can improve the effectiveness of cyber security with better sharing of information, experience and enhancing the perspective in cyber related issues from different entities. This lack of public – private partnerships is widely recognised by the study and it is listed as one of the key findings in the study and only five nations have, according to the study, have succesfully established a formal public-private partnerships for cyber security. (BSA.2015, 3-6)

These studies might leave the reader in to a notion that Finland does not have any cooperation between public authorities and private sector in a field of cyber security. However, the case is not so. For instance, the National Cyber Security Center Finland is providing assistance to the critical infrastructure, which includes also private companies, in a matter of cyber security. One good example of this kind of assistance is HAVARO system, which will be covered shortly in the later parts of this thesis.

And what comes to the National Emergency Supply Agency and National Emergency Supply Organisation, aligning the cooperation between private sector and public authorities is one of the fundamental tasks of NESA and same example serves with this case also, HAVARO. There are also other programmes and recent activities, such as KYBER – TEO, which are aimed to the critical infrastructure. KYBER – TEO initiative will be also covered shortly in this thesis.

2.3.2 Perceptions of cyber threats in Finnish businesses

Taloustutkimus OY conducted a study called Yrityksiin kohdistuvat kyberuhat 2015 on behalf of the Helsinki Chamber of Commerce in year 2015 where 748 Finnish enterprises were approached with issue regarding cyber threats against their businesses. Main focus of the study was to research what kind of impressions businesses had about cyber threats against them and how they should prepare themselves against those threats. The answers for this study were collected from different fields of business, such as industry, construction industry, service industry and commercial industry and most of the answers came from the small and medium size enterprises and 12 % of the answers came from large enterprises comprising 200 or more employees. (Taloustutkimus. 2015, 5)

The study categorizes five major findings. Firstly, the awareness of the businesses needs to be increased. For example, two thirds of the respondents did not know where they can reach information about cyber threats against businesses. According to this study information is available, produced mainly by The National Cyber Security Center Finland, but businesses needs to learn where the information is. Another reason for the lack of information is that businesses do not know the roles of the authorities regarding cyber security. For instance, four out of five respondents do not know or is little aware of the functions of authorities in cyber security scheme.

Secondly, the readiness of the businesses to recognize cyberattacks is weak. For example, one third of the companies would not even notice if they are under cyberattack and only 1 out of ten companies are constantly following and analysing log information. 34 % of the respondents have a capability to detect cyberattacks with their own measures, but there is a substantial amount of companies who are reliable of getting information or warnings about cyberattacks from the National Cyber Security Center Finland or telecommunication companies.

Thirdly, too few companies have full-time information security chief or similar and only six per cents of respondents claimed that they had a person who is fully responsible of information security matters in their company.

Fourth, there is little existence of contingency planning concerning cyber threats in the businesses, only 31 %. Nine out of ten enterprises have not had any exercises against cyber threat situations and four per cent had trained against external advisory, which, according to this study, is the best way to find if company has reliable and effective continuity planning regrading cyber threats.

Last, the training of the staff needs to be increased. According to the study only 10 % of the respondents believed that staff members will notice if the company is under cyberattack and

the biggest obstacle for effective cyber security companies sees the staff's disregard against information security and cyber threats. (Taloustutkimus. 2015, 47-48)

The study raises some worrying dilemmas within the cyber security scheme in Finnish companies. Even though the majority of the respondents were small companies and not necessarily categorized as critical infrastructure, the lack knowledge of the cyber threats and the knowhow of how these threats can avoided or even where to go to if cyber threat incident occurs is alarming. If Finland is aiming to be the global number one country in cyber security there has to be more effort put to the protection of the business life. Nevertheless, businesses, especially those categorized critical infrastructure, are the working backbone of the nation and the functionality of the industry is vital for the society.

One interesting fact is that National Emergency Supply Agency was not even once mentioned in the study, even though NESA is mandated to assist Finnish business life through reporting, instructions and training. Of course, one cannot be sure were there any businesses categorized as critical infrastructure in the study. Still, NESA is supposed to be the link between the private and public sector, including cyber security. For example, NESA has made a cyber security manual for small and medium enterprises, but one can only imagine if Finnish companies have taken the manual in to consideration. The manual for example guides the companies to deal with cyber security from the executive point of view, handles safe procedures of information technologies and how to safely outsource company's websites. This guide also informs where to report when cyber incident occurs and even practical guidelines for building strong passwords. (Huoltovarmuuskeskus. 2013, 11-12)

Even though the study was not specifically targeted only for critical infrastructure it reveals, at some level, in what condition is the awareness of cyber threats in the Finnish business life. Hopefully those companies which are categorized as critical infrastructure are handling their cyber security issues with better understanding than this study lets us to understand.

2.3.3 Finland's National Risk Assessment on cyber threats

According to Finland's National Risk Assessment, Finland is highly developed information society and is extremely dependent on the functions of the information networks and systems. Cyber threats against information systems will be highly significant matter when concerning the security of the society. Global cyber operational environment is comprised of complex information networks which retain information networks of the people, authorities and business entities and also different control systems of the critical infrastructure.

Because of the reason that network management systems, databanks and different kind of components are abroad, it gives Finland challenges in terms of risk management and contingency planning, for example the whole Finnish payment transactions are dependent of functional data network connections to abroad. With corporate acquisitions, the expertise in the field of cyber security might get transferred to abroad and there can be also a possibility that large multinational corporations does not take in consideration national needs in terms of cyber security. Majority of Finland's vital functions are based on the data transmission and the functions of information systems and many services that society provides are interconnected to electrical services. The global markets are changing from traditional methods and structures, and the ability to utilize digital information will define the position of the nations at global markets in significant manner in all fields of industry.

The amount of cybercrimes has also increased and will continue its growth especially when the Internet of Things (IoT) is coming more and more available in the society, this phenomena gives cyber criminals more ways to commit cybercrimes. According to the National Risk Assessment, the ability of the criminals to reach their goals in the target is much more efficient than the targets ability to detect intruders, and it is estimated that with the current resources what police have, the ability to solve cybercrimes will decrease significantly and it will lower the trust against the authorities e.g. from the companies. In severe cybercrimes there is usually strong international dimension, severe threat to society and its vital information systems.

According to the risk assessment, Cyberattacks against Finland can be a part of wider crisis or conflict in Europe and can be caused by another nation or terrorist organisation and one of the means of political pressure against Finland is directing cyberattacks against critical infrastructure. For example cyber threats against social and health care systems can lead in to a loss of lives and threats against financial market information systems can produce serious economic damage. Risk assessment also reminds us that most of the critical infrastructure is in the private sector which means that the activities of the businesses are guided commercial expediency, which again means that there can be challenges in terms of contingency planning towards cyber security.

The Finland's National Risk Assessment is also raising the issue that if a successful cyberattack is targeted against critical infrastructure, there is a possibility that these attacks can cause fatal incidents. (Ministry of Interior. 2015,18-21)

2.3.4 Security Strategy for Society

Security Strategy for Society is decision in principle approved by Finnish government in year 2010 and this strategy comprises the foundation of common contingency planning and crisis management for all the actors in Finland's security landscape. The strategy is drafted from the perspective of the functions that are vital for society and which needs to be secured in every situations. The strategy defines all the vital functions of the society, the threat scenarios which are endangering those functions, strategic duties of the ministries, basics of the crisis management and the principles of monitoring and development of the execution of the strategy. (Ministry of Defence. 2010, 3)

According to strategy, all vital functions of the society will be secured with cooperation between the administration and the goal of the strategy is to avoid overlapping when developing the resources to secure those vital functions. These vital functions of the Finnish society are management of government affairs, international activity, defence capability, internal security, functioning of the economy and infrastructure, income security and population's capability to function in emergency situations and psychological resilience to crisis. (Ministry of Defence. 2010, 15)

The Security Strategy of Society has defined thirteen threat scenarios in order to support different actors when planning contingency and those threat scenarios are designed to be handled within cooperation with different administrative sectors. These threat scenarios are

- Serious disturbances in the power supply
- Cyber threats
- Disturbances in transport logistics
- Serious disruptions in public utilities
- Disturbances in food supply
- Disturbances in the financial sector and in payment systems
- Disruptions in the availability pf public funding
- Disturbances in the welfare and health of the people
- Extreme natural phenomena's, major accidents and environmental threats
- Terrorism and criminality which will endanger social order
- Disturbance in border security
- Political, military and economic pressure
- The use of military against the country. (Ministry of Defence. 2010, 65-78)

As seen above, Security Strategy for Society is defining cyber threats as one of the threat scenarios. Strategy states that the services and functions of the society are mostly connected to networks and majority of the society's critical services are based on data transfer and the usage of the electronical databanks. There are several phenomena's that can threat society's

electrical services, such as natural disasters, human actions and accidents caused by the failure of the technology. According to strategy everyone who is in some way connected to information networks can be target of malicious or non-malicious disturbance, especially cyberattacks can be targeted against network operators and entities involved with electronic commerce, but also industry, communities and public services. (Ministry of Defence. 2010, 66-67) From the next two figures can be seen how different disturbances can be connected into cyber threat scenario.

POSSIBLE DISTURBANCES AND THEIR CONNECTION TO THREAT SCENARIOS IN THE STRATEGY	Serious disturbances in the power supply	Serious disturbances in the telecommunications and information systems – cyber threats	Serious disturbances in transport logistics	Serious disruptions in public utilities	Serious disturbances in food supply
Disruption in the availability, transmission and distribution of electricity	X	X	X	X	X
Disruptions in the functioning of telecommunications and information systems	X	X	X	X	X
Damage in the ICT infrastructure	X	X	X		
Disturbance in the nation-wide radio and television broadcasts	X	X			
Transport disruptions	X		X	X	X
Disruptions in the availability of imported fuels	X		X	X	
Disruption in the fuel supply	X		X	X	
Disruption in the supply of non-durable consumer goods	X	X	X		
Disruption in the water supply (incl. wastewater management)	X	X	X	X	
Disruption in waste management			X	X	
Failure of district heating	X	X		X	
Failure of financial transactions	X	X			
Disruption in the availability of cash		X	X		
Collapse of the credit rating of the state and municipalities					
Downfall of the solvency or reinsurance cover of an insurance company					
A pandemic or other widespread outbreak of serious infectious disease	X	X	X	X	
A serious animal or plant disease outbreak					X
Mass extinction of species					X

Figure 1: Possible disturbances & their connection to threat scenarios in the strategy. (Ministry of Defence.2010, 80)

POSSIBLE DISTURBANCES AND THEIR CONNECTION TO THREAT SCENARIOS IN THE STRATEGY	Serious disturbances in the power supply	Serious disturbances in the telecommunications and information systems – cyber threats	Serious disturbances in transport logistics	Serious disruptions in public utilities	Serious disturbances in food supply
Declining conditions in primary production	X				X
Widespread contamination of soil or waters					X
A storm or flooding and a dam disaster	X	X	X	X	X
An accident relating to CBRNE hazards					
Land, sea or air traffic accident			X		
An accident affecting Finns or action taken against them abroad					
A terrorist attack or a clear threat thereof	X	X		X	
A criminal act that widely endangers the population	X	X		X	X
A criminal act that widely endangers functions in society	X	X	X	X	
Jeopardised border security					
Major influx of asylum seekers					
Adversely influencing the State's capability to function					
Disruption in foreign trade			X		
Threatening with WMD					
Information operation	X	X	X		
Provocative violation of territorial integrity					
An armed incident	X	X			
The use of military force attempting to surprise	X	X	X	X	X
A large-scale use of military force	X	X	X	X	X

Figure 2: Possible disturbances & their connection to threat scenarios in the strategy. (Ministry of Defence. 2010, 82)

When concerning security of supply and protecting critical infrastructure, the Security Strategy for Society is referring to the Government's decision on the security of supply goals and is emphasizing the responsibility of the National Emergency Supply Agency and its duties to enhance and align the capability of public authorities to guide private sector during emergency situations or similar. This strategy also states the main responsibilities of the ministries in the matter of the security of supply for better coordination of the goals of the security of supply. For example, the Ministry of Transport and Communications is responsible of maintaining and developing the operational preconditions of the electric communications infrastructure in matters of the security of supply. (Ministry of Defence. 2010, 63-64)

2.3.5 Finland's Cyber Security Strategy

Finland published its first cyber security strategy in year 2013 and this strategy is defining all the essential goals and policies which are aimed to answer all to the challenges regarding cyber domain and also securing the functions of the cyber domain. This cyber security strategy is a part of the Security Strategy for Society and cyber security strategy is following the same principles and definitions that are in the Security Strategy for Society and in the Governments Decision on the Security of Supply Goals. Finland's Cyber Security Strategy provides the vision, operational model and strategic alignments. According to strategy, the highest authority in cyber security falls in to the Prime Minister's Office. Each and every ministry has their own strategic tasks and they are responsible of the cyber security and disturbances caused by cyber threats within their administrative branch. (The Security Committee. 2013, 1-4)

According to the strategy, Finland as a small, capable and cooperative country have all the possibilities to become one of the leading countries when regarding cyber security issues and the vision of this strategy is that

- Finland is able to protect its vital functions in all situations concerning cyber threats
- Authorities, citizens and companies has a possibility to efficiently utilize safe cyber domain
- Finland will be a worldwide pioneer in contingency planning and in controlling cyber threats by the year 2016 (The Security Committee. 2013, 3)

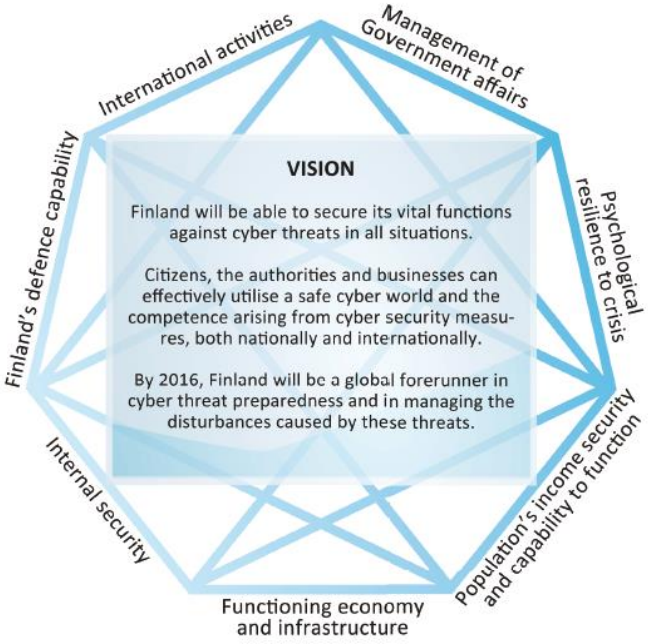

Figure 3: Vision of Cyber Security (The Security Committee. 2013, 3)

Finland's Cyber Strategy background dossier states that a global cyber domain is comprised of complex worldwide information networks which contain players from national security authorities to critical infrastructure and its controlling systems. Global cyber domain has brought the people closer to each other and has made life much easier in many ways. However, it has also brought new problems and risks. If information technology is not working properly or cyberattacks are affecting to society it can reduce people's trust to public services, business life and government. Cyber domain has also changed traditional international power arrangements and it gives possibilities to the smaller actors to function in a global cyber domain.

Cyberattacks can paralyse or create massive disturbances to the critical infrastructure and through cyberattacks nations can be pressured into political, military or economic concessions. The openness of cyber domain gives the possibility to attack from every corner of the world and Finland as one of the most advanced information societies is greatly affected by the cyber domain. According to a dossier Finland has already been a target of cyberattacks and the constant development of the cyber domain will increase the threat to be under more severe attacks. (The Security Committee. 2013, 17-18)

According to the dossier, year 2010 was a beginning of the new era when Stuxnet worm was exposed. With this worm it was confirmed that cyberattacks can produce physical damage also when with the help of this worm Iranian nuclear plant was attacked and physically damaged the centrifuges which were used to enrich uranium. It is estimated that this cyberattack delayed Iranian nuclear programme for years. This raised the concern of the possibility to the attacks against the industry using automatization and with this new era of cyber security this type industry might be the first ones to attack when the goal is ultimately to harm and affect the vital functions of the society. (The Security Committee. 2013, 18)

Finland's cyber threat scenario is comprised of five elements. These elements are cyber activism, cybercrime, cyber espionage, cyber terrorism and cyber operations. Cyber threat scenario means the description of the disturbance caused by the cyber threats and the mechanism, source, target and the impact it have to the target. Threats can fall upon directly or indirectly against the vital functions of the society such as critical infrastructure and it can come whether from inside or outside of the nation's borders. (The Security Committee. 2013, 18)

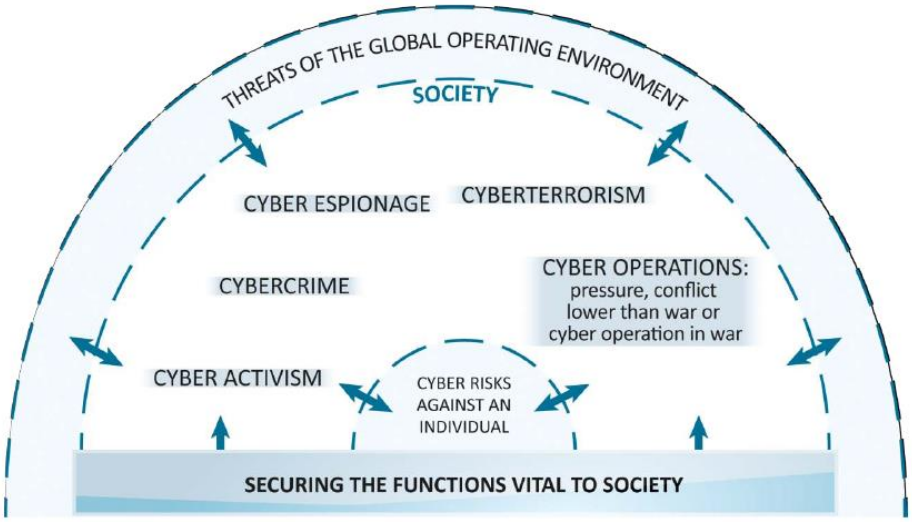

Figure 4: Finland's cyber threat scenario (The Security Committee. 2013, 19)

Finland's Cyber Security Strategy has defined ten strategic alignments in order to develop national cyber security. These alignments will create the preconditions to the realization of strategy's vision and through the Finland's Cyber Security Strategy implementation programme where these alignments are put in concrete level. These ten alignments are

1. Creating an effective cooperation model between authorities and other actors in order to enhance cyber security and preventing cyber threats
2. Improving the comprehensive understanding of the cyber security of those actors who are involved with securing the most vital functions of the society
3. Maintaining and developing the ability of detecting, eliminating and recovering from cyber threats and malfunctions against the organisations and companies who are essential for the vital functions of the society
4. Making sure that the police has effective preconditions to prevent, uncover and solve crimes that fall upon cyber domain
5. The Finnish Defence Forces will create a comprehensive cyber defence ability
6. Reinforcing national cyber security capability by actively and efficiently participating to the functions of the focal international organisations
7. Improving the cyber capabilities and understanding of all the essential actors in the society
8. Making sure of an effective cyber security functions with national legislation
9. Defining the tasks and service models to authorities and business life and common foundation to manage the requirements of cyber security
10. Monitoring the implementation of the strategy (The Security Committee. 2013, 7-11)

When considering critical infrastructure the Finland's Cyber Security Strategy is, similar as Security Strategy for Society, emphasizing the role of the National Emergency Supply Organi-

sation in whole. For example, the third strategic alignment is aimed for the critical infrastructure and the goal of the alignment is to secure continuity of the most vital businesses in a case of a cyber disturbance situation. NESO has a vital role in ensuring the functions of the critical infrastructure and critical production in all situations with correct contingency planning. (The Security Committee. 2013, 8)

After Finland's Cyber Security Strategy came its implementation programme in year 2014, which is listing 74 proposals that needs to be addressed in order to achieve the goals what Finland has set in its strategy. This implementation programme is also defining six central targets of development and these main targets of development of the programme are

- Establishing the National Cyber Security Center Finland
- Nations round-the-clock information security activity
- Encrypted data transfer and management of network security service integration project
- Police capability in cybercrime prevention
- Development of the legislation concerning cyber domain
- Cyber security and research, education and other methods of competence development (The Security Committee. 2014, 2)

These 74 proposals are divided into two major themes, "Effective and secure public administration" and "The wellbeing of the citizens and the success of the companies", the first theme is comprised of 18 main proposals with sub proposals attached to some of them and the second theme is comprised of 13 main proposals, all of these proposals are connected to the strategic alignments of the cyber security strategy.

Every proposal is comprised of the name of the proposal, the main responsible party, possible requirements of reforming or renewal of the legislation and in what strategic alignment the proposal is connected. NESA is named the main responsible party in seven proposals which some of them are not in operation anymore, such as previously mentioned KYBER-TEO initiative which ended in its current form in at the end of the year 2015, but continues its existence, as one of the themes, in the KYBER 2020 programme. (The Security Committee. 2014, 24-55)

In the following chapter some criticism over the strategy and its implementation programme is presented.

2.3.6 Criticism over Finland's Cyber Security Strategy and its implementation programme

As the Finland's Cyber Security Strategy serves as a fundamental guiding security strategy in Finland and serves also as a framework for the KYBER 2020 programme, the strategy and its implementation programme has been receiving some criticism over the effectiveness of it.

According to the study Cyber security competencies in Finland – Current state and roadmap for the future published by Finland's Prime Minister Office at February 2016, Finland's Cyber Security Strategy has been claimed to be too authority oriented and it is missing the identifications of such factors which truly would make Finland a worldwide pioneer in cyber security matters. The strategy is concerned as some form of compromise and there has also been criticism over its implementation programme and the slender resources allocated to these 74 proposals. It seems that Finland's Cyber Security Strategy has not been able create common strong vision and the spirit of cooperation between different actors within cyber security field. (Prime Minister's Office. 2016, 34)

The same study also stating that Finland is lacking a cooperative operations model, whereby confidential and profound exchange of information can be shared between actors who are involved with cyber security. The study is suggesting that Finland needs a Cyber Security Committee, a national cooperation body which reinforces the coordination between public sector, scientific community and private sector. (Prime Minister's Office. 2016, 70)

Aalto University's professor of cyber security Jarno Limnell is also questioning if Finland's Cyber Security Strategy has reached one of its targets to be one of worldwide pioneers in cyber security. According to Limnell, Finland cannot pronounce itself as a pioneer in these matters and to back up his thoughts Limnell is referring worldwide studies conducted by European Union and United Nations, even though Finland has succeed relatively well in this studies. Limnell is also adding that it is difficult to compare nations between each other due the reason that there are no established measurements and not all the necessary information is available. When concerning nation's maturity level in cyber security, there are several factors to consider, for example, legislation, public-private cooperation and the level of common understanding. There has been positive advance in the development of Finland's cyber security and Limnell is mentioning that there has been improvement in international cooperation, development of cyber defence capabilities, the readiness to detect and repel cyber threats and general knowledge of cyber security has been increased. In order to improve Finland's cyber security Limnell is highlighting six different issues in which should be taken on consideration.

Firstly, the leadership of national cyber security is too widespread to the different actors in society, therefore there has to be comprehensive leadership between government, business life and science world.

Secondly, Finland has to decide what is its ambition in national cyber security issues and allocate the right amount of resources to it in order become the worldwide pioneer. According to Limnell, Finland have all the capabilities to achieve that status.

Thirdly, there is a shortage of skilled persons in cyber security, even though education and research has increased, but the level of knowhow has to be increased too. There has to be better coordination between educational establishments and the research of cyber security needs to be more versatile.

Fourth, even though one strategic alignment of Finland's Cyber Security Strategy was to improve national legislation, according to Limnell, Finland has not been effective enough in that matter. Modernity of legislation is one of the key criteria when estimating the level cyber security in international comparison and clear legislation will secure the basic rights of individuals and gives business life better possibility to design its functions and making investments.

Fifth, the transportation of successful Finnish companies to foreign ownership is compromising Finland's cyber self- sufficiency and there has to be, if necessary, government measures taken in order to keep the top expertise in Finland and therefore Finland's export markets needs to be more supported.

Sixth, it is important that common knowledge about cyber security issues reaches each and every citizen because the cyber knowhow of the people serves also as one the criteria when measuring the level of nation's maturity in cyber security. (Jarno Limnéll. 2016)

Even the members of Finnish parliament do not believe in the Finland's Cyber Security Strategy. In Limnélls study, Kansanedustajien arvioita Suomen kyberturvallisuuden nykytilasta ja tulevaisuudesta which is was aimed to the members of Finnish parliament in order to figure out what are their perceptions on the current status and the future cyber security in Finland. As one of the conclusions, the study is highlighting the lack of efficiency of Finland's Cyber Security Strategy. For example, even though there has been good work done after the Finland's Cyber Security Strategy the members of parliament still do not believe that Finland has achieved the status of being one of the leading countries in cyber security, like it is stated in the strategy's vision. (Limnéll. 2016, 16)

When the members of parliament were asked in a scale of one to ten, how likely they consider a scenario that within the next three years there will be a cyberattack against critical infrastructure almost fifty percent considered the possibility to be high. Limnéll is estimating

that this answer is indicating that there is a political need to take more on consideration the protection of critical infrastructure against cyber threats. (Limnell. 2016, 10-11)

Earlier of this thesis presented study about perceptions of cyber threats in Finnish business life, conducted by Taloustutkimus OY, is also giving its own contribution to the criticism against Finland's Cyber Security Strategy. According to the study, the highest level of the national leadership in cyber security is represented by the government. However, there is no clear reference what body is in charge of leading and coordinating every day activities of the authorities in reality. There is National Cyber Security Center Finland which is giving information about cyber threats and attacks but does not have; according the study, clear leadership mandate in cyber security seems to be missing. (Taloustutkimus. 2015, 28)

On behalf of National Cyber Security Center Finland one can argue that, according to the implementation programme of the Finland's Cyber Security Strategy, there is no authority given to the National Cyber Security Center Finland, but rather act as a service element to those government authorities who are responsible of the cyber security in Finland. (The Security Committee. 2013, 37)

The former Chief Executive Officer of the National Emergency Supply Agency Ilkka Kananen is also reminding us about the defects of the Finland's Cyber Security Strategy and especially the making process of it. According to Kananen, the ten strategic alignments of the strategy was an outcome of compromise and the preparing process of the strategy was agonising and frustrating. Kananen is estimating that probably not all of the participants acknowledged that cyber security cannot be only governmental project.

Kananen states that there were only little alignments that were concerning the preparedness of the critical infrastructure. The third alignment, maintaining and developing the ability of detecting, eliminating and recovering from cyber threats and malfunctions in the organisations and companies who are essential for the vital functions of the society was aimed to the critical infrastructure. Through that alignment NESO was given the task to support critical infrastructure by reporting, guiding and training in order to enhance the cyber resilience of the vital businesses and organisations. However, according to Kananen this task did not brought anything new to the table and NESO has been doing similar tasks through its organisation for years.

The National Emergency Supply Agency took part in to the preparation process of the implementation programme of the Finland's Cyber Security Strategy and the preparation work was time consuming and full of conflicts, but when the implementation programme was complete

NESA launched cyber security related activities such as KYBER TEO initiative and cyber security manual for small and medium enterprises. (Kananen.2015, 275-276)

It is also clearly said in the Finland Cyber Security Strategy's implementation programme that this strategy is in fact intended to be authority orientated. This authority orientated approach is justified by the Security Committee in a way that with this approach Finland's central administration has the best conditions to co-ordinately launch these proposals in the matters which are significant in a national context. (The Security Committee. 2013, 3) One can only estimate that, in what point of the making process of the implementation programme this statement was written and what were the reasons that led in to this, sense there has been substantial amount of criticism over the programme's inability to take on consideration cyber security issues of critical infrastructure.

Then again, the Security Committee is concerned that many of these proposals from the implementation programme of the strategy are still in at planning stage and according to Kananen, the vision of the strategy is not enough, but resources are needed too. (Kananen. 2015, 278)

This wide range of criticism which Finland's Cyber Security Strategy and its implementation programme are receiving is noticeable and this should even more accelerate the need for generating structures in order to better take on consideration critical infrastructure.

2.4 International examples of cyber security activities

In the following two examples of cyber security activities from other countries are presented. These countries are the Netherlands and Estonia. One thing common with these two countries is that they have both revised their cyber security strategy. The Netherlands released its first strategy in year 2011 and published its second strategy in year 2013. Estonia, in other hand released its first cyber security strategy in year 2008 and the second one came 2014. (Prime Minister's Office. 2015, 59-60) The Netherlands and Estonia are considered to be in the top countries worldwide regarding cyber security, for example, according to the Global Cyber Security Index, the Netherlands is in a sixth place and Estonia in fifth place. Therefore, it is suitable to use these countries as examples. (ABI Research.2015, 1-2)

2.4.1 The Hague Security Delta, the Netherlands

The Hague Security Delta is the European largest security cluster and it operates in three different cities in the Netherlands, Hague, Twente and Brabant. This cluster is comprised of businesses, government organisations and educational institutions and these entities are

working closely within cooperation in specific fields of cyber security, protection of the critical infrastructure, national and urban security and forensics. Cyber security issues are handled in Hague. (thehaguesecuritydelta. 2016)

The starting point of HSD dates back in the year 2010 when a project called Pieken in de Delta project was established by some educational and governmental institutes. The purpose of this project was to get Netherlands' security network professionalised, explore the possibilities for developmental organisation or financial fund and to generate innovation establishments within the four fields of interest. Like KYBER 2020 programme is now, the Hague Security Delta was officially initiated as a project in 2012. Nowadays the Hague Security Delta is the largest security cluster in the Europe. (thehaguesecuritydelta. 2016)

One of the recent activities of HSD in order to enhance the cyber security in critical infrastructure in Netherlands was to develop a national multi-sector testbed for critical infrastructure. Testbed is a platform where hardware and software can be tested in a protected environment. The report Securing Critical Infrastructures in the Netherlands – Towards National Testbed is rationalising the importance of the testbed by stating that industry is becoming more and more automatized and the society is increasingly adopting digital technologies, but the security behind those technologies are coming behind. Attacks against critical infrastructure have massive influence towards society, therefore, it is important that critical infrastructure have a possibility to test their system and share the information. Being multi-sector testbed gives the different sectors of critical infrastructure a possibility to test their cooperation because different sectors of critical infrastructure often rely on each other, for example, food industry is reliable of transportation. (Castellon & Frinkin. 2015, 6-19)

When considering the fact that HSD was initially a two year project in order to enhance the security field in Netherlands and considering the fact what HSD is now, the growth has been enormous when regarding the statement that HSD is the biggest security cluster in Europe.

2.4.2 Estonian Defence League's Cyber Unit, Estonia

Estonia adopted its first cyber security strategy in year 2008 and the attacks against Estonia were one of the trigger points of emphasizing the importance of cooperation between public authorities and private sector. (Kaska, Osula, Stinissen. 2013, 7)

Estonian Defence League's Cyber Unit is a part of the Estonian Defence League and it was also established in the aftermath of the 2007 cyberattacks against Estonia and this cyber unit focuses on enhancing the cyber security capabilities of Estonia and it is voluntary based. EDL CU

aims to promote public-private cooperation and strengthening the awareness of cyber security.

Estonian Defence League was founded in year 1918 and it is a voluntary military organisation which later became a foundation of the establishment of the Estonian armed forces, border guard and prison service. During the Soviet occupation Estonian Defence League was dismissed in 1940 and restored back again in year 1990. The purpose of Estonian Defence League is to defend the independence of Estonia and enhance the preparedness of the Estonian people.

The proposal of establishing cyber security unit came after the cyberattacks in year 2007 and after those attacks it was recognised that the cooperation between public and private sector is essential in order to successfully handle the attacks. After the proposal was widely accepted by Estonian cyber security community it started as a project which ended to the establishment of the Estonian Defence League's Cyber Unit in January 2011. (Kaska et.al. 2013, 7–9)

The mission of the EDL CU is to protect the high-tech way of life in Estonia by the means of protecting critical information infrastructure and supporting national objectives of Estonian's national defence. There are three identified objectives of EDL CU, which are

- Developing a network of cooperation between public and private cyber security expertise
- Improving the security of critical information infrastructure by sharing the knowledge and awareness of cyber threats and handing out the best practices
- Promoting awareness, education and training by establishing information security training and education and by participating in, international and national, cyber security exercises. (Kaska, Osula, Stinissen. 2013, 11)

Basically, the functions of EDL CU can be comprised in to two major themes. Firstly, strong cooperation between public and private sectors in a field of a cyber security, secondly, the strong Estonian tradition of volunteering in to national defence. (Kaska, Osula, Stinissen. 2013, 37)

Even though EDL CU structurally integrated into paramilitary organisation let us not be fooled by that. The main message of this kind of establishment is that cyber security experts are gathering a forum in which cyber security issues can be handled with the cooperation of public and private sector, in order to serve a bigger purpose; defending the nation, in which critical infrastructure is major part of it, against constantly evolving cyber threats. Estonia has also experienced a massive cyberattack in year 2007 and it was after that when this cyber

unit was established, meaning there was a national ambition, both in private and public sector, to prevent such incidents to occur again.

2.5 Tools for the evaluation of the programme's activities

This part of this thesis introduces two commonly known management tools. These tools were adapted from European Union Agency for Network and Information Security (ENISA) evaluation framework for cyber security strategies. These same tools will be adapted to the KYBER 2020 programme and writer during this thesis process has made an evaluation framework for one of the themes of the programme, however the content of the evaluation framework for the programme will be classified information, therefore it will not be presented in this thesis.

2.5.1 ENISA's evaluation framework

European Union Agency for Network and Information Security (ENISA) is a centre of expertise of cyber security matters within European Union and its main objectives is to prevent, address and respond problems related to information and network security. The main tasks of ENISA is counselling member states on information security, gathering and analysing information on incidents related to security throughout Europe, advance the capability to handle information security threats through risk assessment and risk management and cooperation with various actors who are involved in information security especially building up public private partnerships in the industry. (ENISA. 2016)

An Evaluation framework for Cyber Security Strategies is ENISA produced report which suggests two commonly known management tools for building an evaluation framework. These tools are Logic model and Key Performance Indicators. The evaluation framework produced by ENISA is based on the several interviews of cyber security experts, systematic review of existing cyber security strategies and the feedback what ENISA received from the Logic model from member states. (European Union Agency for Network and Information Security (ENISA). 2014, 25) In the following subparagraphs these two management tools are presented.

2.5.2 Logic model and key performance indicators

First tool which ENISA is using in its evaluation framework for cyber security strategies is Logic model. From the following this widely used management tool is defined and the principles of how to use the tool shortly explained.

Logic model is, deceivingly simple, programme management tool which aims to explain to various stakeholders how to address acknowledged problems and how the programme that is

implemented is supposed to attack the problems in order to solve them. This tool is especially developed for those who are responsible of designing, conducting programmes and also for those who are reporting and using programme evaluations. The model itself has been in use from the 1960's and have become more and more popular because of the demanding need for measuring performance in programmes. Logic model has various forms, but Wholey in his book presents a basic model which consists of inputs, activities, outputs, and short –term outcomes, intermediate outcomes and long – term outcomes.

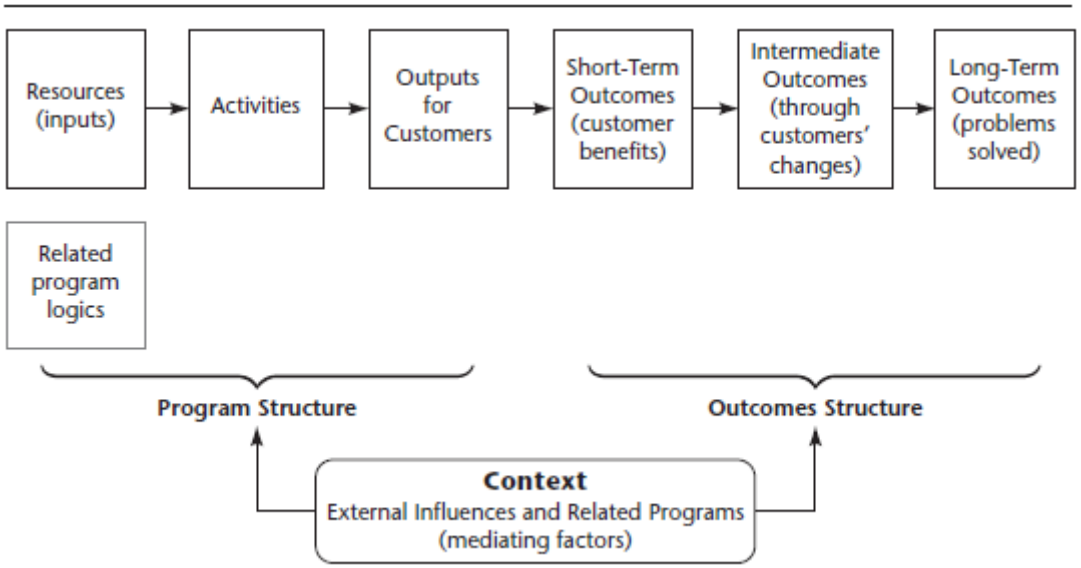

Figure 5: Basic Logic Model (Wholey et al. 2010, 57)

Inputs are resources put in the programme; these resources can be human and financial but also other elements which are supportive to the programme, such as, partnerships. The problem which the programme is attacking is also resource and there should be the type and level of that particular problem. ***Activities*** are the steps that need to be taken in order to produce the next step of the model, which is the programme output. Activities present the idea what the programme does. ***Outputs*** are the elements produced and manufactured to the programme participants, these elements can be products, goods and services.

After the outputs comes the outcomes which are the benefits to whom the programme is targeted and these outcomes are usually divided into three sections. Firstly, ***short – term outcomes***, which are the changes that are caused directly by programme's outputs. Secondly, i***ntermediate outcomes***, which are the outcomes what programme is supposed to produce from the short – term outcomes. Thirdly, ***Long – Term Outcomes***, or ***programme impacts***, which are expected to follow from the intermediate outcomes.

There are also external ***contextual*** factors which can influence the programme and is not under the control of the programme, these external factors can produce either negative or

positive affect to the programme. According to Wholey et. al, there are two types factors that affect the programme, antecedent and mediating factors. Antecedent factors are at the beginning of the programme and can be such as economic factors, client characteristics and geographical variables. In other hand, mediating factors are taking place when the programme is in progress and these factors can be for example new policies, change in staff, change in the economy and other similar programmes which can there for competition or for support. It is important to programme planners to take on consideration what are those uncontrolled factors that influences to the programme.

According to Wholey et.al, there are five steps when building a logic model for programme, these steps are collecting the right information, defining the problem what the programme is supposed to solve, defining the elements for the logic model, making the logic model and getting assurance of the logic model from the stakeholders. (Wholey et.al. 2010, 56-58)

Collecting the right information means involving all the persons who are working the programme in to the process in order to avoid the possibility that some essential parts of the programme are left out form the consideration. This gives the possibility to create much more coherent vision about how the programme is supposed to work. It is important to collect the information from various sources, such as documents related to the functions of the programme and by interviewing the key stakeholders, internal and external, of the programme.

By clearly defining the problem which the programme is supposed to affect positively gives the foundation to the development of the logic model. This means defining all the factors which are causing the problem and defining the factors that the programme is addressing. It is also important to consider what is the context in which the programme is operating and how it might affect to the programme outcomes. Even though, there might be several factors that need to be addressed before finding all the problems which programme is trying to affect, it is recommendable that all of these factors needs to be found. If failing to found all the factors, it might negatively affect to the long-term outcomes of the programme.

The next step of building the logic model is defining the elements by categorizing the information gathered and tagging it into programme's resources, activities, outputs, outcomes or external factors and placing these elements in to logic model table presented in figure 10. There should be continuous check-ups of the accuracy and relevance of the information in the table and a good way to get assured that all the right elements are in place is to engage stakeholders. Meaning, if stakeholders can understand the logical flow from resources to long-term outcomes there is possibility that all the elements are defined and there is clear sequence from one column to the next.

There are several different forms of logic models, but one shown in the figure five is the most basic one. The outlook of logic model depends on the complexity of the programme and if necessary there can be several different logic models showing different relevant aspects of the programme from the point of view of different stakeholders. It is better to start with the easiest form of logic model and then, if necessary, modify that model in to a more complex design. This step takes patience, even though drawing logic model can be seen as a simple task, it is hard work behind the model what makes it appear simple. Nevertheless, logic model is should be simple and understandable graphic representation, making the stakeholders to understand the hypothesized linkages of the model.

As the logic model is complete, there should be continuous evaluation of the programme logic and how it is functioning with the respect of the programmes goals and how the programme works in order to achieve its short-term, intermediate and long-term outcomes. The verification process of the logic model should engage all the relevant stakeholders. (Wholey et.al. 2010, 62 – 72)

According to ENISA, logic model is a tool that can show the logic behind the actions taken by the program and this tool is used to inspect the relationship between the inputs, outputs and outcomes. (European Union Agency for Network and Information Security (ENISA). 2014, 28)

Another tool that is suggested by ENISA, alongside Logic model, is Key Performance Indicators. From the following the concept of KPI's are shortly explained.

According to Parmenter (Parmenter. 2010) key performance indicators are the measures that focus on the most critical aspects of organisational performance that are vital for the success of the organisation. In order to clarify what Key Performance Indicators are Parmenter is dividing KPI's in to different fundamental characteristics in which he is also aiming to differentiate KPI's from Key Result Indicators. These characteristics are

- KPI's are not measured financially
- KPI's needs to be measured frequently
- KPI's has to have the attention of the highest level of the organisation and the relevant staff members
- KPI's have to indicate what actions needs to be done if something is wrong
- KPI's has to be tied to a person or a team in order to clarify the responsibilities
- KPI has to have an effect. Don't measure something what does not have impact
- KPI's have to encourage the people to make relevant procedures (Parmenter 2010, 4 – 8)

Parmenter continues with Key Performance Indicators that there are four foundation stones in order to have ultimate success when implementing KPI's. These foundation stones are, creating partnerships with all the relevant stakeholders, transferring the power of influence from high level organisation to working staff, in other words, transfer the power to the frontline, measure those matters only which are relevant for the success and link performance measurement to existing critical success factors and strategic objectives. (Parmenter 2010, 29-36)

Accroding to ENISA, key performance indicators are criteria which can be chosen to measure the performance or advancement of a policy, strategy or, in NESA's case, a programme. KPI's can be qualitative or quantitative depending on the purpose and because ENISA is focusing on the long term outcomes it has chosen to use qualitative measures. Accroding to ENISA, by selecting the correct key performance indicators at the beginning of the strategy's implementation, it gives to the stakeholders a possibility to track the advancement of the strategy, but also during the evaluation phase of the program KPI's can offer information if there is a need for revision of the program. (European Union Agency for Network and Information Security (ENISA). 2014, 29) When designing key performance indicators ENISA is emphasizing some basic characteristics which KPI's need to have in order to them become valuable. These characteristics are specific, measurable, attainable, relevant, time – related, governable and KPI's should have impact. (European Union Agency for Network and Information Security (ENISA). 2014, 2-3)

3 Methodology

In the following the methodology of this thesis will be presented.

3.1 Qualitative research

This thesis aims to understand the importance of protecting critical infrastructure against cyber threats through interviews and review of relevant documents. Therefore, a qualitative research is suitable for the research method.

Conducting a qualitative research is suitable when there is no information, theory or prior research on the subject, researcher wants to have a deep vision about the phenomena, triangulation is used or there is need to have good description about the phenomena.

Qualitative research enables the understanding of the phenomena, in other words understanding what the phenomena is all about. According to Kananen (Kananen 2015), there are four different aspects when conducting a qualitative research and in which the researcher should embrace himself

- Commitment in to time consuming field work
- Commitment in to analysing the collected data
- Commitment in to time consuming writing process
- Tolerance of uncertainty (Kananen J. 2015, 70-73)

For this thesis, all the above mentioned characteristics were realized.

According to Hirsjärvi et.al (Hirsjärvi et.al 1997 12th edition) there are seven characteristics of qualitative research

1. By nature research is a comprehensive acquisition of information and the material is collected in natural and realistic conditions
2. Preferring human beings as an instrument of information gathering. Researcher is relying more to his ability to observe rather than using measuring instruments to get the information
3. Usage of inductive analysis. The aim of the researcher is to reveal unexpected factors; therefore it is not important to test theories or hypothesis, but to inspect the data with detail.
4. The usage of qualitative methods in the acquisition of the data. Preferring the methods where the points of views of those who are the target of the research are revealed. For example, theme interviews is one the methods.
5. Choosing the target group deliberately, not using random sample.
6. The research plan is shaped as the research is proceeding. Research is flexible and the plans will be changed if necessary.
7. Handling the cases as they are unique and the data is interpreted accordingly. (Hirsijärvi et.al 1997, 155)

3.2 Interviews

According to Kananen (Kananen 2015) interviews are very flexible methods where interviewer can guide the interviewee and if necessary make new questions about the subject in hand. The forms of interviews can change from open discussion to very strict questions which are presented in the same order to each every interviewee.

Theme interviews is the most common way to conduct interviews when collecting information to qualitative research, however the most common mistake with theme interviews is that the interviewer has readymade specific questions for each specific theme. This indicates that the interviewer already knows the phenomenon so clearly that by conducting only theme interview is the wrong research method. (Kananen J. 2015, 143-146)

According to Hirsijärvi et.al (Hirsijärvi et.al 1997 12th edition, 197) theme interview is intermediate form of questionnaire and open interview, and with theme interviews it is typical that the subject areas are known but there is no strict formulated questions and the order of the questions are unknown. (Hirsijärvi et.al 1997, 197)

For this thesis, three different persons were interviewed. Two of the persons are working for the National Emergency Supply Agency and one of the interviewees for the National Cyber Security Center Finland. Two of the interviews were conducted in the premises of the National Emergency Supply Agency in Helsinki during early spring of the year 2016 and the third interview was conducted in the premises of Finland's Communications and Regulatory Authority in Helsinki as well. All of the interviewees are experts in a field cyber security and are closely working within the KYBER 2020 programme and all of them have prior experience in the field of protecting critical infrastructure against cyber threats. From every interview there is a memo written which can be found from the writer.

Persons who were interviewed for this thesis were

- Director, Sauli Savisalo, National Emergency Supply Agency
- Business Continuity Manager, Erkki Räsänen, National Emergency Supply Agency
- Special advisor, Miikka Salonen, National Cyber Security Center Finland.

All of the interviewees agreed to appear in this thesis by their own name.

4 Results of the interviews

This chapter represents the results of the interviews and also introduces the organisations behind the KYBER 2020 programme. These Interviews had three themes in it. Firstly, because of the reason that there is no public information of the KYBER 2020 programme, the information about this programme was gathered via interviews. Secondly, the reason why this programme is implemented was discussed and thirdly there was discussion about the need for monitoring and evaluating the programme's activities. Before the results of the interviews, the organisations behind the KYBER 2020 program are briefly introduced.

4.1 Organisations behind KYBER 2020

In the following subchapters the organisations behind the KYBER 2020 programme are shortly presented. These organisations are National Emergency Supply Organisation, National Emergency Supply Agency, Finnish Communications Regulatory Authority and National Cyber Security Center Finland.

4.2 The National Emergency Supply Organisation (NESO)

The National Emergency Supply Organisation is a network organisation which maintains and develops the security of supply in Finland. Main goal of NESO is to secure the operational pre-conditions of those organisations which are vital for the security of supply and through that secure the functions of the whole nation. Within NESO hundreds of entities, authorities and associations from various sectors of the nation are working towards the common goals. NESO is comprised of National Emergency Supply Agency, National Emergency Supply Council and Sectors and Pools from different aspects of society. (Huoltovarmuus. 2016)

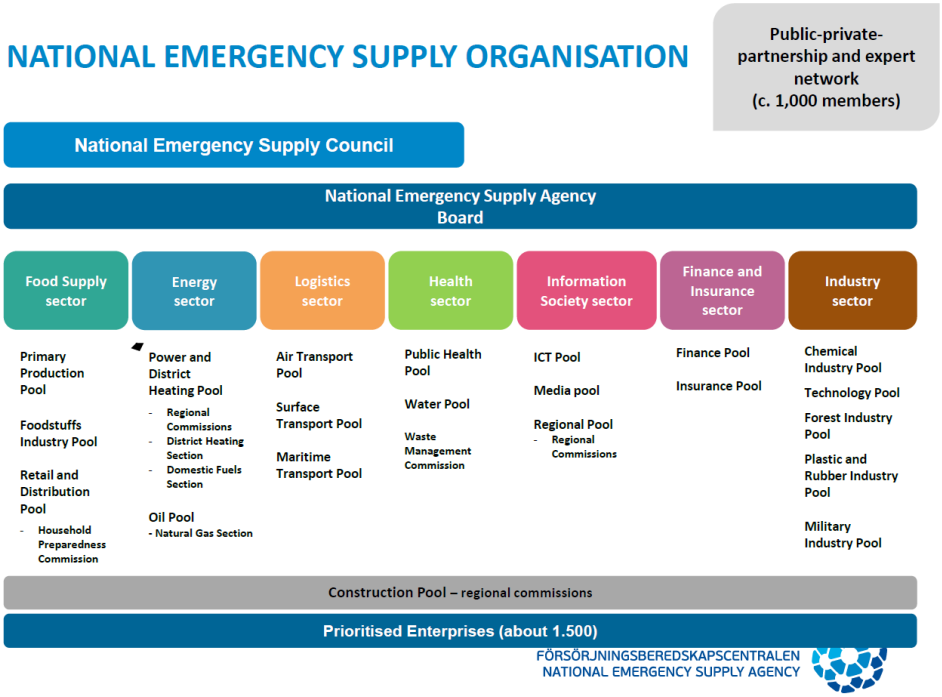

Figure 6: NESO (Huoltovarmuus 2016)

4.3 The National Emergency Supply Agency (NESA)

The National Emergency Supply Agency is an organisation under the Ministry of Employment and Economy with main objective to develop and maintain security of supply in Finland. The Degree on the National Emergency Supply Agency has defined more specific tasks to NESA which are

- Acting as secretariat for the National Board of Economic Defence
- Maintaining security of supply stockpiles
- Promoting and coordinating public authorities' readiness to manage and guide the national economy in emergency situations
- Promoting the readiness planning of companies
- Ensuring the functioning of the national technical infrastructures

- Safeguarding the production of necessary goods and services under emergency conditions
- Analysing threats against security of supply and drawing up plans for countermeasures
- Maintaining relations to similar bodies and agencies in other countries.

The operations of NESA are headed by the chief executive officer with the guidelines given by the National Emergency Supply Council and the functions of NESA are funded by an extra-budgetary fund. (Huoltovarmuus. 2016)

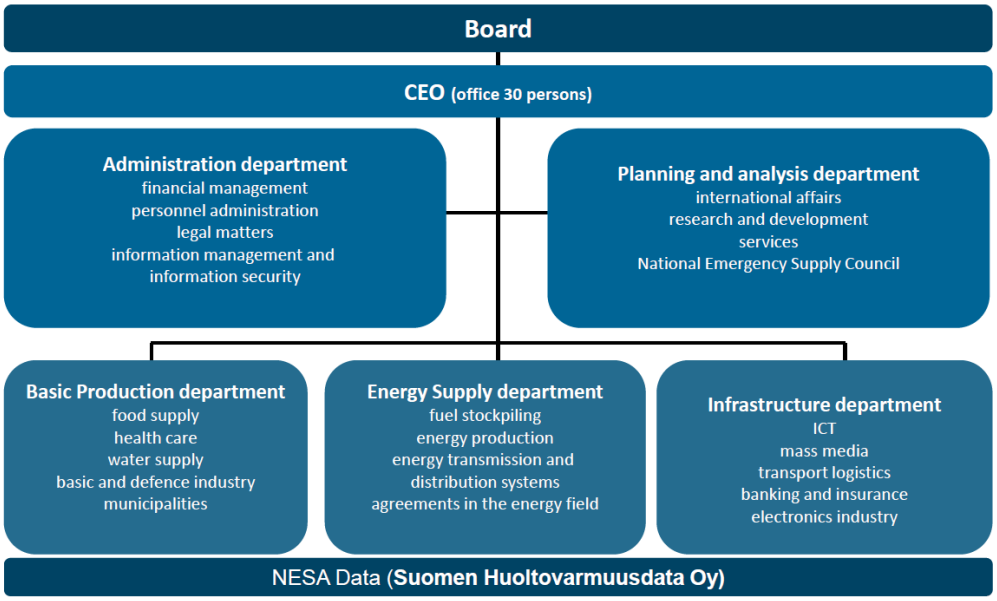

Figure 7: NESA (Huoltovarmuus 2016)

4.3.1 Examples of NESA's cyber security activities

KYBER 2020 programme is not the first effort in which the National Emergency Supply Agency is trying face the constantly evolving cyber threats against critical infrastructure. From the following, few examples of NESA's activities in a field of cyber security are presented.

In order to improve cyber security of critical industry the National Emergency Supply Agency, with cooperation with its partners, launched KYBER-TEO initiative in year 2014 where new services were tested and provided to the critical industry which are utilizing automatization in their operations in order to enhance the cyber security and business continuity of these entities. With this initiative Finland's critical industry has improved its capabilities against cyberattacks and the work done during this initiative will benefit also other organisations that are involved with the security of supply more or less. (Emma Karki. 2014)

Suomen Huoltovarmuusdata (SHVD) is a data centre established by the National Emergency Supply Agency and its aim is to be top secure service operator for the most critical information technology in Finland. Reason for establishing SVHD came from the Governments decision on the security of supply goals from year 2008, which states that the functions of society's most critical information technology needs to be secured during emergency conditions. In year 2008 established data centre is service provider for the most critical information systems and aims to ensure that the functions of information systems will operate in all conditions. (Huoltovarmuus. 2016)

HAVARO is an observation and warning system of information security breaches designed especially to the critical infrastructure in Finland. HAVARO is one of the products of Cyber Security Center Finland and it is result of the long term development work between National Emergency Supply Agency and Finnish Communications Regulatory Authority and it is comprised of versatile technical solutions and it is designed only to monitor information security breaches, not communication of an individual persons. There are approximately 20 to 40 organisations involved with HAVARO, but the identities of the organisations are kept secret. Joining the HAVARO system is based on voluntariness, but if an organisation decides to join HAVARO system it has to have already high standards in information security and the ability to utilize the observation data provided by HAVARO system. Systematic deviations detected by HAVARO is analysed by the National Cyber Security Center Finland and then the information about the critical attacks against the system is sent to the organisations. (Varmuuden vuoksi. 2016)

HUOVI–portal is a designed to support municipalities, authorities and critical infrastructure in preparedness of severe malfunctions. HUOVI–portal serves as information channel and databank to the organisations and it provides instructions, publications and articles related preparedness and business continuity and the portal enables the exchange of confidential information between different actors inside the portal. One of the tools of the portal is a maturity assessment tool for business continuity. With the help of this tool organisations can estimate the level of the business continuity within the organisation. With the answers what this assessment tool provides organisations can get useful pointers to preparedness and an overview of the organisations position compared to general level of business continuity in a specific field. The usage of HUOVI–portal is safe and the data between the system and the user is secured in a way that no outsider can get access to the information. (Huoltovarmuus. 2016)

4.4 The Finnish Communications Regulatory Authority (FICORA)

The Finnish Communications Regulatory Authority is an organisation under the Ministry of Transport and Communications and through its activities FICORA is developing reliable infor-

mation society and ensuring that Finnish society has a secure access to different electronic services. FICORA is maintaining an overview of the functionality of electronic communications networks and information security and will inform society from possible information security threats. FICORA's organisation consists of seven divisions which are Administration, Information Management, Communications, Stakeholders, National Cyber Security Centre, Markets, Spectrum Management and the head of Ficora is Director-General. (Viestintävirasto. 2016)

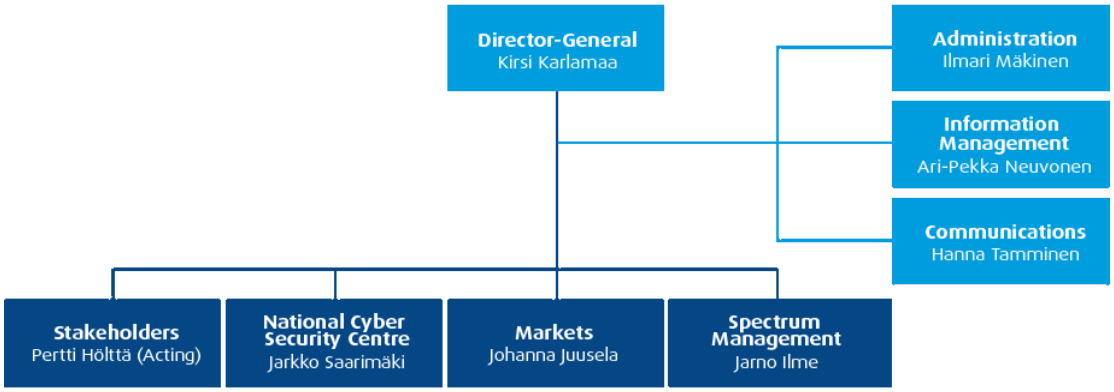

Figure 8: FICORA (Viestintävirasto. 2016)

4.5 The National Cyber Security Center (NCSC-FI)

The National Cyber Security Center Finland has been operating under FICORA since 1 January 2014 and is a national information security authority in Finland. The focus of NCSC-FI is to ensure secure and undisturbed functions of the common public communications networks and communication services and securing the vital functions of the society and through an agreement made with NESA, NCSC-FI will in its part make sure that the functioning of vital technical systems that are essential for the security of supply are protected. (Viestintävirasto 2016)

The National Cyber Security Center Finland was established to function as to service authorities, business life and other actors in order to enhance national cyber security and according to Finland's Cyber Security Strategy, the main tasks of the NCSC-FI are

1. "Compile and disseminate the cyber security situation picture"
2. "Compile and maintain a cyber threat risk analysis, in conjunction with different administrative branches and actors"
3. "Support the competent authorities and actors in the private sector in the management of widespread cyber incidents"
4. "Intensify cooperation and support the development of expertise."

According to the Finland's Cyber Security Strategy's background dossier, the main task of the NCSC-FI is creating, compiling, maintaining and distributing the cyber security situation picture and providing it to those who need it. NCSC-FI is mainly acting as a supportive body in cyber incidents by assisting the authority in charge. (The Security Committee. 2013, 23-24)

4.6 KYBER 2020 programme

According to the interviews, KYBER 2020 programme is a comprehensive cyber security programme designed by National Emergency Supply Agency with cooperation of National Emergency Supply Organisation and Finnish Communications Regulatory Authority (FICORA). The main goal of the KYBER 2020 programme is to enhance the cyber security of the most critical infrastructure in Finland. (Savisalo, Räsänen, Salonen)

KYBER 2020 programme has eight themes in it. However, the first theme, "theme zero", serves only as in a supervisory role to all other themes, which are aiming to represent concrete actions in which NESA and its cooperative partners are aiming to improve the cyber security of the critical infrastructure in Finland. According to Räsänen, these themes were selected and designed by the experts working with the programme after a wide sampling of interviews in which wide variety of distinguished cyber security experts underlined the needs and hopes of how critical infrastructure should be protected against cyber threats. In the following these themes are shortly introduced. (Savisalo, Räsänen, Salonen)

The aim of the ***"theme zero"*** is to adapt this cyber security programme with other existing national programmes and strategies and also making sure that programme will achieve its ultimate goal. According to Savisalo, this theme is intended to serve as overseeing body which monitors the implementation and success of the other themes. Therefore it does not have similar functions than the other themes have. (Savisalo, Räsänen, Salonen)

Theme one is concentrating in to the trust issues of digital methods and abilities to control cyber threats. Throughout this theme KYBER 2020 programme is aiming to enhance the business continuity of the critical infrastructure and making sure that businesses has better knowledge of the their critical dependences. (Savisalo, Räsänen, Salonen)

Theme two focuses on enhancing the preparedness of the critical infrastructure by the means of designing and conducting cyber security exercises and developing specific consultation services where companies can get support and consultation in cyber security matters. With this theme KYBER 2020 programme is seeking to increase the operational capabilities of the criti-

cal infrastructure and preparedness to tolerate and to react against severe cyber threats. (Savisalo, Räsänen, Salonen)

Theme three is focusing on to the development of the ability to recognise information security threats and making the exchange of vital information between companies more effective and to cover the whole value chain of the critical infrastructure. In order to reach these issues KYBER 2020 programme will focus on developing already existing observation and warning systems by drawing up a development strategy to these systems. One of these systems is HAVARO system, which is shortly introduced in this thesis. (Savisalo, Räsänen, Salonen)

Theme four is compiled of three elements which are communications, situation awareness and exchange of information. Within this theme, there are several measures taken but the main measure is that NESA with cooperation with National Cyber Security Center Finland is aiming to develop a common platform for communications and exchange of information where critical infrastructure can get the information they need in order to perform information security measures quickly and efficiently. (Savisalo, Räsänen, Salonen)

Theme five focuses on international cooperation and it aims to recognise possible cyber threats that are wide ranging and long lasting in an international scale, and which can produce severe losses to the businesses. Also, to develop the cyber resilience of the critical infrastructure with cooperation of certain international organisations by the means of changing information and best practises. With this theme KYBER 2020 programme will try to hasten the development of cyber security capabilities of critical infrastructure by utilizing those best practices. (Savisalo, Räsänen, Salonen)

Theme six concentrates on the observation of the future by developing novel means and methods to recognise new threat models and by developing better defence mechanisms against cyber threats. Throughout this theme the programme is focusing on to create networks where these cyber security trends can be observed and recognised efficiently and through that creating conditions where the understanding of a changing business environment can be understood. (Savisalo, Räsänen, Salonen)

Theme seven is focusing on the cyber security of the critical industry which is utilizing automatization in their operations. This theme has adopted one already existing initiative, which is KYBER – TEO initiative and throughout the KYBER 2020 programme, continue the efforts if the KYBER – TEO. More information about KYBER – TEO can be found in chapter 4.3.1. (Savisalo, Räsänen, Salonen)

The implementation of the KYBER 2020 programme is on its way and some concrete work towards the themes of this programme has already been done. According to Räsänen, NESA is aiming to appoint so called “theme supervisor” to each and every theme and these supervisors are intended to represent the highest expertise of knowledge regarding each theme. For example, for theme six it could suitable to appoint supervisors from academic field, but NESA is only at the starting point of considering suitable entities for every theme and only two themes has had its own “supervisor” appointed at this point. Savisalo also emphasizes that these theme supervisors are meant to be organisations or institutes, not individual persons. (Savisalo, Räsänen, Salonen)

From the figure below the basic structures of the KYBER 2020 programme are presented.

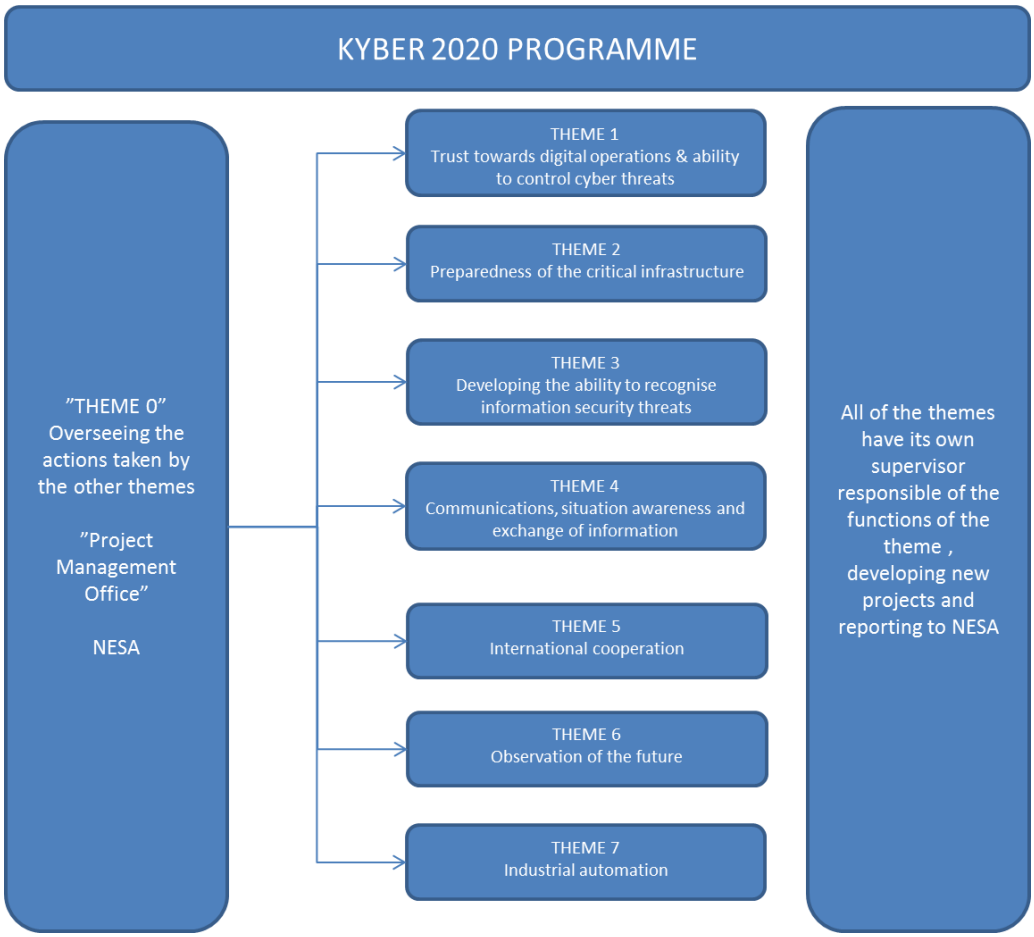

Figure 9: KYBER 2020 programme (Writer)

As seen, one of the themes is focusing on the monitoring of the implementation and success of the other themes. National Emergency Supply Agency is aiming to create so called “Project Management Office” to theme zero, in which the activities of the programme are supervised. With these arrangements the focus is to create smaller projects in to the themes as the pro-

gramme continues its existence and NESA's primary task is to oversee and fund these projects, if they turn out to be effective, relevant and serves the common goal of the programme. (Savisalo, Räsänen, Salonen)

Like the name KYBER 2020 let us presume, this programme is intended to be a five year programme and at the end of the programme, critical infrastructure in Finland is supposed to be more protected against cyber threats than it is currently. However, according to Savisalo, through this programme NESA aiming to create much more permanent status of creating cyber security in critical infrastructure. Räsänen adds that this programme is only meant to be an initiation stage and after year 2020 the structures of this programme are embedded in to Finland's cyber security scheme in a way that it becomes self-sufficient with positive effects on critical infrastructure. Savisalo also points out that establishing this kind of programme requires cooperation. Therefore this programme is a joint initiative with above mentioned organisations. (Savisalo, Räsänen, Salonen)

From the following figure, the framework of the KYBER 2020 programme is introduced. As we can see the Security Strategy of Society is defining the most vital functions of the society and Finland's Cyber Security Strategy is giving the vision, operations model and strategic alignments of cyber security. (Savisalo, Räsänen, Salonen)

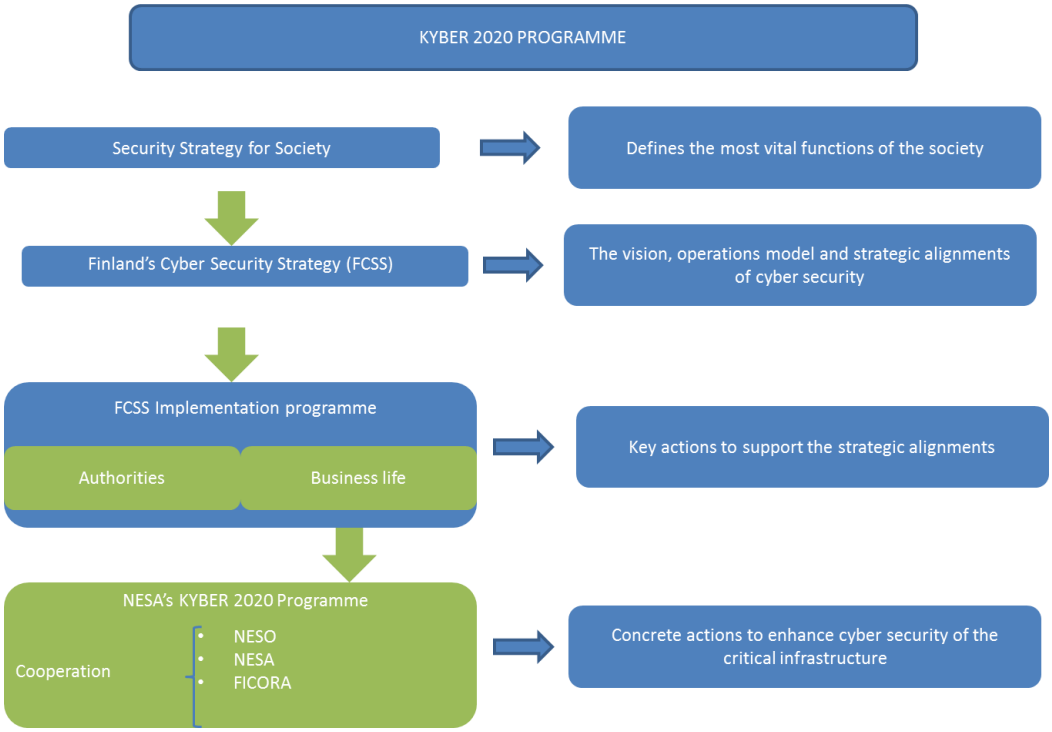

Figure 10: Framework of KYBER 2020 Programme (Writer)

4.7 Reasons behind the KYBER 2020 programme

All of the interviewees stressed the fact that there is a cyber shortfall in Finland's cyber security landscape and there is an order for taking more actions towards the protection of the critical infrastructure. According to Savisalo, the functions of the society are reliant of the critical infrastructure's ability to tolerate cyber threats and if this ability is compromised it can have negative impacts on the society. (Savisalo, Räsänen, Salonen)

Finland's most critical infrastructure is doing well against the cyber threats, but there is a need for new approach in order to assist the efforts of the critical infrastructure. However, according to Salonen, even though critical infrastructure is accomplishing well against cyber threats, there can be significant variations between the skills in different organisations and that is why there is a need for this kind of approach. Therefore, one of the targets of the KYBER 2020 programme is to enhance the change of information between the critical infrastructure and authorities and through that enhance the cyber capabilities of the organisations. (Savisalo, Räsänen, Salonen)

Another fact which Räsänen stressed was that Finland's Cyber Security Strategy's implementation programme is too authority orientated and it does not have specific and comprehensive actions towards the protection of the critical infrastructure in Finland. According to Räsänen, the KYBER 2020 programme is in some ways an answer to the implementation programme of the Finland's Cyber Security Strategy. This issue was agreed by Savisalo and Salonen also. However, Salonen is reminding that there was a need for Finland's Cyber Security Strategy and it came at the right time and it is taking stand on the protection of the critical infrastructure against cyber threats, but the measures were not adequate enough. Therefore, there are reasons to take concrete actions. According to Savisalo, Finland's Cyber Security Strategy and its implementation programme is successfully defining the responsibilities of different actors, including NESA, but Savisalo is also stating that the lack of concrete actions is the main reasons for this KYBER 2020 programme. (Savisalo, Räsänen, Salonen)

According to Savisalo, even though NESA has already done work towards the cyber threats against critical infrastructure, for instance HAVARO system and Huoltovarmuusdata OY, the comprehensive structure of the KYBER 2020 programme will do its part by filling the hole in Finland's cyber security pitfall. Savisalo also reminds that one of the tasks of NESA is connected to the protection of the information society and cyber security issues needs to be essential part of it.

All the interviewees also stressed the issue that NESA is mandated to assist critical infrastructure in continuity management and cyber security naturally falls into this category as con-

stantly evolving issue in Finland's security landscape. According to Salonen, due the reason that critical infrastructure is mainly owned by the private sector there is also a need for a better linkage between public authorities and private sector also in matters of cyber security and NESA is an organisation which serves as an entity aligning the cooperation between these two sectors. (Savisalo, Räsänen, Salonen)

4.8 Monitoring and evaluation of the KYBER 2020 programme

All of the interviewees of the NESA and NCSC-FI experts acknowledged that there is a need to monitor the progress of the programme. According to Räsänen, one of the main reasons is to assure that this programme has real positive affect to the critical infrastructures struggle against cyber threats and Räsänen continues, whenever there is public money used the responsible parties' who are involved with programme needs to make sure that the money is used in a proper and visible manner. (Savisalo, Räsänen, Salonen)

According to Savisalo, as this programme continues its growth and become more active, the amount of stakeholders will increase also, therefore it is essential to NESA have control over the activities inside the programme. Savisalo also reminds that, like the other initiatives that NESA has launched, and the aim of this programme, is to gradually diminish the activities of NESA inside the programme and become more of a background organisation which only funds and supervises the functions of the KYBER 2020 programme. Therefore, it is important that there is a tool or method of how these functions can be supervised. (Savisalo, Räsänen, Salonen)

Another important fact which Salonen notes is that this programme is voluntary on behalf of the critical infrastructure. Therefore it is important to show the effectiveness of the programme. By monitoring and evaluating the actions taken by the programme it provides NESA and its cooperative partners a possibility to demonstrate how the programme is supposed to work and how the measures that are taken will improve the cyber security of critical infrastructure. This issue was agreed by other interviewees also. (Savisalo, Räsänen, Salonen)

5 Analysis

The functionality of critical infrastructure is essential for the society and cyberattacks against critical infrastructure can have a remarkable affect to the vital functions of the society and through that people's lives. For instance, major disturbance in power supply can have catastrophic consequences and can cause indirectly loss of lives. One scenario was presented in the beginning of this thesis. One of the differences between this fictional scenario and real life incident which occurred in Ukraine was that it has not happened in Finland, yet. Another

difference was that no fatal accidents occurred in the Ukrainian case, but if the cyberattack in Ukraine would have prolonged there might have been. There are studies presented in this thesis which are implicating the fact that the cyber threats against private sector, including critical infrastructure, are growing and becoming more frequent. For example, the study made by Intel Security reveals that cyber threats against critical infrastructure will continue its growth and there is a possibility that within the next three years there will be a cyberattack against critical infrastructure that can indirectly cause loss of lives. The same study also reveals that 90 % of the respondents have experienced a severe cyberattack against their organisation. Europol is also estimating that cyber threats against critical infrastructure are increasing.

The study, conducted by Taloustutkimus OY also reveals some worrying issues of the perceptions of cyber threats in Finnish companies. The study in a way implicates that cyber threats are taken seriously, but yet no pre-emptive measures were taken by the companies. The study mostly sets the responsibility towards the authorities. However, the urge for the comprehensive cyber security should come from the companies themselves, but it is in some ways understandable that if the companies do not know where to get information and assistance regarding cyber security.

Almost all of the studies presented in this thesis are also emphasizing the need of cooperation between public authorities and private sector. In Finland, the National Emergency Supply Organisation and the National Emergency Supply Agency are the entities which are mainly responsible of aligning the cooperation between public authorities and private sector and it is clearly stated in the Governments Decision on the Security of Supply Goals that that the National Emergency Supply Agency has a mandate to assist critical infrastructure in various issues. In this modern world and due the reason that everything is connected to the information networks, cyber security should be one the main areas of NESA's interest and activities.

Another issue what came up in this thesis was the lack of leadership in cyber security issues. One explanatory thing could be the way how leadership in emergency situation are organised and explained in the Security Strategy for Society. Like said in this strategy, the highest authority is in the hands of Prime Minister's Office and all the ministries have strategic duties in their field. For example, one of the strategic tasks of the Ministry of Social Affairs and Health is to secure the social and health care services and environmental health care services (Ministry of Defence. 2010, 86). If there are disturbances in that field, the Ministry of Social Affairs and Health is the main responsible ministry before the Prime Minister's Office. Finland's Cyber Security Strategy is a part of Security Strategy for Society and follows the same principles of leadership that are defined in the Security Strategy for Society. For this reason, in cyber security incidents as well, it is the ministry which is taking over the control of the is-

sues and, for example, if there is a cyberattack against hospital, the Ministry of Social Affairs and Health is the ministry in lead when handling that cyber security incident.

Finland is ranked high in international studies regarding cyber security and was one of the first countries which published its own cyber security strategy in year 2013. However, according to the Global Cyber Security Index and EU Cyber Security Dashboard Finland does not have any sector specific plans or programs in a matter of cyber security. Like explained in the earlier parts of this thesis, this is not completely true and there has been cooperation between the public authorities and private sector in Finland. However, this notion made by these studies only gives NESA and its partners more valid reason to implement and promote the KYBER 2020 programme.

There are two main reasons why NESA and its cooperative partners are implementing the KYBER 2020 programme. Firstly, like earlier explained, cyber threats against critical infrastructure are real and we can almost in monthly bases read news of cyberattacks against vital functions of the society throughout the world. Also, the recognised need to enhance the cooperation between the private and public sector is one of the reasons that implicates to the need for this kind of approach.

Secondly, Finland's Cyber Security Strategy and its implementation programme are failing to take in to consideration critical infrastructure in a way that it is sufficient enough and there can be a variety of reasons why the implementation programme is too authority orientated. This issue came up with the interviews and the information presented in this thesis. Maybe, one of the reasons could be that Finland has done only one cyber security strategy and there were not enough understanding how cyber security issues really are concerning the nation as a whole, not only authorities. Yet again, the strategy and its implementation programme identifies the need of protecting critical infrastructure against cyber threats and the National Emergency Supply Organisation and the National Emergency Supply Agency as entities which are providing support to the critical infrastructure, but as we can see from the main development targets of cyber security strategy's implementation programme, there is only one issue where business life is acknowledged. All the others were authority orientated. Even though, this authority orientated approach is acknowledged by the implementation programme itself, this fact only accelerates the need for making adjustments towards more protection of the critical infrastructure against cyber threats. Like said earlier in this thesis, one can only guess in what point of the implementation programme's writing process the idea of adding authority orientated approach to the implementation programme came.

In a way, the KYBER 2020 programme is serving as a counterweight to the Finland's Cyber Security Strategy's implementation programme's authority orientated approach. From the fol-

lowing figure the main development targets of Finland's Cyber Security Strategy's implementation programme can be seen on the left side and on the right side are the themes of NESA's KYBER 2020 programme.

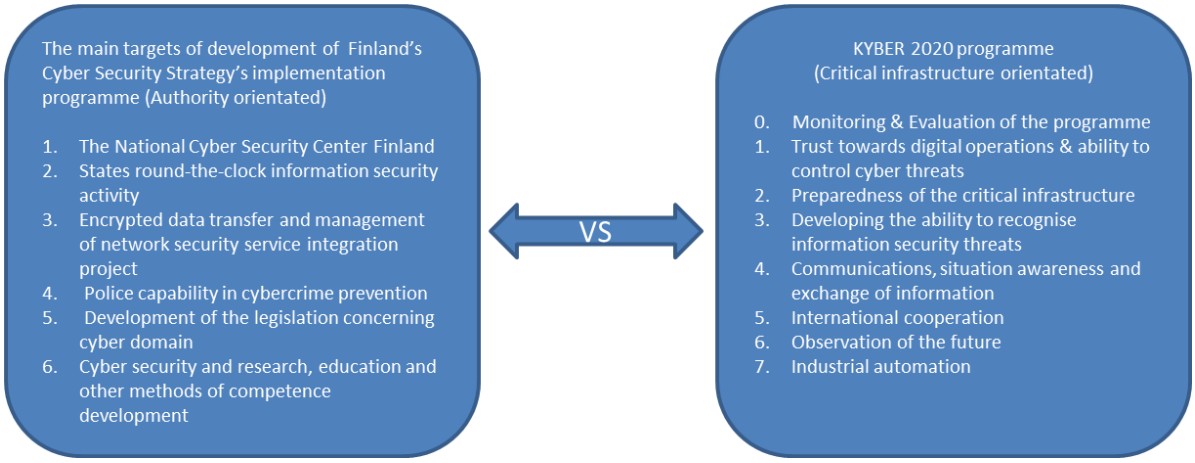

Figure 11: Finland's Cyber Security Strategy's implementation programme vs. KYBER 2020 programme (Writer)

However, if Finland in some point is revising its strategy, it would suitable to implement the activities of the KYBER 2020 programme into the new strategy, like KYBER – TEO was recognised in the implementation programme. That way the KYBER 2020 programme will get more credibility if government is acknowledging the programme and it might also deepen much needed cooperation between public and private sector in matters of cyber security. As this thesis is presenting the cooperation between these two sectors are essential in cyber security and one of the main reason for that is that Finland is highly developed information society and is extremely dependent on the functions of the information networks and systems and this includes also critical infrastructure. Since the critical infrastructure is mainly owned by the private sector, the cooperation is essential.

Two international examples presented in this thesis can serve as an example how other countries are aligning the cooperation between public and private sector. For example, the Hague Security Cluster in Netherlands serves as an example how different actors from various fields come together in order to establish a network of professionals and creating new innovations. Estonia on the other hand relies on the strong patriotism and through that enhances the cooperation in cyber security. Surely, there are many other examples of how the cooperation between public and private sector are organised, but these two countries can serve as fine examples in that field and maybe NESA can adopt some good practices from these countries.

In order to avoid the same what has happened to the implementation programme of Finland's Cyber Security Strategy, there is a need for monitoring and evaluating the implementation

and actions of the KYBER 2020 programme. The evaluation framework provided by ENISA and KYBER 2020 programme has a common denominator, which is cyber security. Therefore the utilization of this evaluation framework could be justified. Since the KYBER 2020 programme is meant to be dynamic programme and the functions within KYBER 2020 can vary and change during the existence of the programme, it would suitable for NESA to implement these suggested tools in to themes. Since, one of the basic ideas of logic model is that it is supposed to be dynamic as well. One possible approach would be that, as soon as, there will be smaller projects created into to themes and in order to NESA monitor and evaluate those projects, NESA would demand from those appointed theme supervisors to develop an evaluation framework by using these two tools, which are presented in this thesis.

Like the interviewees said, KYBER 2020 programme intends to serve as much more permanent solution than just a five year programme and NESA's intentions to nominate "supervisors" to each and every theme leads to the conclusion that this programme needs to be monitored in a way or another. By utilizing Logic model and Key Performance Indicators in project management, it gives NESA and all the stakeholders who are involved in the programme a possibility to see how the different smaller projects inside the programme is supposed to assist the main goal of the programme, which was to enhance the cyber security of the critical infrastructure and creating more permanent structures in the fight against rapidly evolving and growing cyber threats.

6 Conclusion

Through the expert interviews and relevant literature this thesis attempted to explain the cyber security scheme in Finland. During the writing of this thesis, it came clear that there is a growing need to protect critical infrastructure against cyber threats and Finland's Cyber Security Strategy's implementation programme is not focusing enough on the protection of the critical infrastructure. Like said in the beginning of this thesis, critical infrastructure is mainly owned by the private sector and the functionality of the private sector, especially critical infrastructure, is vital for the society. Therefore, there is a need for putting more focus on the cyber security issues in critical infrastructure.

Another part of this thesis was to make an evaluation framework for the KYBER 2020 programme. This framework utilized two commonly known management tools, logic mode and key performance indicators, and with this framework NESA can have a possibility to monitor and evaluate the progress of the programme.

This thesis process is the writer's last contribution to the National Emergency Supply Agency and hopefully the effort has not been futile, but this thesis has brought value to the National

Emergency Supply Agency and its work as securing the functions of the critical infrastructure and through that protecting the vital functions of the society.

6.1 Answering the research questions

Is there a need for a national programme called KYBER 2020 programme for protecting critical infrastructure against cyber threats in Finland?

There are two main reasons why there should be national preparedness against cyber threats. Firstly, cyber threats and cyberattacks against the vital functions of society, including critical infrastructure are increasing. Secondly, Finland's Cyber Security Strategy and its implementation programme is too authority orientated, therefore there is a need to approach the cyber security issues of critical infrastructure in a new manner.

The reason that critical infrastructure is mainly owned and operated by the private sector there is a clear reason for more cooperation between public authorities and private companies. The National Emergency Supply Agency as an organisation mandated to serve as a link between public and private sector in order to align the cooperation between these sectors is the right entity to deal with the problems which critical infrastructure is facing in a field of cyber security.

How the effectiveness of the KYBER 2020 programme should be evaluated?

This thesis is suggesting two commonly known management tools for the evaluation and monitoring of the KYBER 2020 programme, logic model and key performance indicators. The usage of these tools is also recommended by the European Union Agency for Network and Information Security (ENISA) to serve as building blocks of an evaluation framework for cyber security strategies in member states. Due the reason that this ENISA provided evaluation framework for cyber security strategies and KYBER 2020 programme has common denominator, cyber security, the utilization of this evaluation framework could be justified. In addition to this, during the writing process of this thesis writer has made an evaluation framework for the one of the themes of the KYBER 2020 programme. However, due the reason that this evaluation framework is classified material, it will be not presented in this thesis.

7 Validity & Reliability of the research

According to Kananen (Kananen 2015) the research process is always exposed to mistakes, these mistakes can come from the researcher himself or the material he is researching and the mistakes can be either conscious or subconscious. With inspection of the validity & relia-

bility of the research some of these mistakes can be eliminated, however the researcher himself is the biggest influencer to validity and reliability of his research. For example, researcher can with different selections to choose such theories and models which are supporting his results or the material is collected in a way that it is supporting the chosen theories, according to Kananen, this is a common strategy in scientific world.

In qualitative research, researcher always has influence to subject he is studying and this influence cannot be removed but it can be acknowledged, however researcher is never allowed to influence the phenomenon because it might distort the results. Scientifically this is called reactivity which means same as contamination of the material. (Kananen J. 2015, 338-339)

This thesis intends to be neutral and follow the existing guidelines. However, it is evident that writer working closely within the organisation which is implementing the KYBER 2020 programme and aiming to find justification to it might have, conscious or subconscious, agenda in order to find the right information that would suitable for the benefit of NESA's ambitions. Though, writer is working his best to not to get influenced too much.

The results of this research are gathered from the interviews and most recent studies in the field of cyber security. The results indicate that there is a growing need to assist critical infrastructure against cyber threats. One the main reason for this is that Finland's Cyber Security Strategy's implementation programme does not take on consideration the private sector and critical infrastructure in its actions. This fact has been verified by all of the interviewees and some of the documents presented in this thesis.

8 Suggestions for further research

For further research the answer seems obvious. After the KYBER 2020 programme has been implemented and is running, it would suitable to conduct research which is evaluating the success of the programme. If NESA adapt the suggested management tools, Logic model and Key Performance Indicators, it would suitable to use the same tools for the evaluation of the programme's activities.

References

LITERATURE

Wholey, J.S, Hatry, H.P & Newcomer, K.E. 2010. Handbook of practical program evaluation. San Fransisco: Wiley Imprint.

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas. Jyväskylä: Jyväskylän ammattikorkeakoulu (Juvenes Print).

Hirsjärvi, S. Remes, P. & Sajavaara, P. 2006. Tutki ja kirjoita. 12th edition. Jyväskylä: Gummerus Kirjapaino.

Parmenter, D. 2010. Key performance indicators: developing, implementing, and using winning KPIs. 2nd edition. New Jersey: John Wiley & Sons, Inc.

Kananen, I. 2015. Suomen Huoltovarmuus. Riittääkö energia ja ruoka, toimiiko tiedonkulku? Juva: Bookwell Oy.

INTERNET

Enisa. 2016. Organisaatio. Accessed 15 March 2016
https://www.enisa.europa.eu/about-enisa/activities

Enisa.2016. An Evaluation Framework for National Cyber Security Strategies. Accessed 15 March 2016
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies

Enisa.2016. An Evaluation Framework for National Cyber Security Strategies-Annex B Methodology. Accessed 5 April 2016
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies

Huoltovarmuuskeskus. 2013. PK – yrityksen kyberturvallisuuden kehittäminen. Accessed 20 May 2016
http://www.huoltovarmuus.fi/static/pdf/754.pdf

Huoltovarmuus. 2016. Organisaatio. Accessed 16 March 2016
http://www.huoltovarmuus.fi/organisaatio/huoltovarmuuskeskus/

Huoltovarmuus. 2016. Organisaatio. Accessed 16 March 2016
http://www.huoltovarmuus.fi/organisaatio/hv-organisaatio/

VTT. 2015. Emma Karki. Teollisuuden kyberturvallisuutta parannetaan yhteistyöllä Accessed 5 April 2016
http://www.huoltovarmuus.fi/static/pdf/871.pdf

Huoltovarmuus. 2016. Suomen Huoltovarmuusdata OY. Accessed 19 March 2016
http://www.huoltovarmuus.fi/organisaatio/shvd/

Huoltovarmuus. 2016. HUOVI.portaali. Accessed 18 March 2016
http://www.huoltovarmuus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta/huovi/

Hagelstam, A. 2005. CIP – kriittisen infrastruktuurin turvaaminen - Käsiteanalyysi ja kansainvälinen vertailu. Accessed 21 April 2016
http://www.huoltovarmuus.fi/static/pdf/243.pdf

Limnéll, J. 2016. Kansanedustajien arvioita Suomen kyberturvallisuuden nykytilasta ja tulevaisuudesta. Accessed 16 May 2016
https://aaltodoc.aalto.fi/bitstream/handle/123456789/19815/isbn9789526066875.pdf?sequence=1

Varmuuden vuoksi. 2016. HAVARO turvaa yhteiskunnan huoltovarmuuskriittisiä toimintoja. Accessed 18 March 2016
http://www.varmuudenvuoksi.fi/aihe/huoltovarmuuden_toteutuksia/106/havaro_turvaa_yhteiskunnan_huoltovarmuuskriittisia_toimintoja

Viestintävirasto. 2016. Organisaatio. Accessed 17 March 2016
https://www.viestintavirasto.fi/viestintavirasto/virastonesittelyjatehtavat.html

Viestintävirasto. 2016. Organisaatio. Accessed 17 March 2016
https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut.html

Verkkouutiset.2016. Blogi. Limnell, J. Kyberosaaminen pidettävä suomalaisissa käsissä. Accessed 25 April 2016
http://www.verkkouutiset.fi/blogit/limnell_kyber-45624

Ministry of defence. 2016. Security Strategy for Society. Accessed 24 March 2016
http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit

The Security Committee. 2016. Finland's Cyber Security Strategy. Accessed 23 April 2016
http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit

The Security Committee. 2016. The implementation programme of Finland's Cyber Security Strategy. Accessed 23 April 2016
http://www.turvallisuuskomitea.fi/index.php/fi/component/k2/15-kyberturvallisuusstrategian-toimeenpano-ohjelma

The Security Committee. 2016. Finland's Cyber Security Strategy – background dossier. Accessed 24 April 2016
http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit

The Security Committee. 2015. Sähköriippuvuus modernissa yhteiskunnassa. Accessed 3 May 2016.
http://www.defmin.fi/files/3070/sahkoriippuvuus_modernissa_yhteiskunnassa_verkkojulkaisu.pdf

Finland. 2013. Valtionneuvoston päätös huoltovarmuuden tavoitteista. 5.12.2013 . Accessed 20 April 2016
http://www.finlex.fi/fi/laki/alkup/2013/20130857?search%5Btype%5D=pika&search%5Bpika%5D=857%2F2013

European Union. 2008. COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Accessed March 29 2016
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

Intermin. 2016. Suomen kansallinen riskiarvio 2015. Accessed 5 April 2016
https://www.intermin.fi/julkaisu/032016

Valtioneuvoston kanslia. 2016. Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen. Accessed 6 April 2016
http://tietokayttoon.fi/documents/10616/2009122/9_Kyberosaaminen+Suomessa.pdf/29c8f675-0790-4c2f-91c2-69187b34b37e?version=1.0

Taloustutkimus. 2016. Yrityksiin kohdistuvat kyberuhat 2015. Accessed 14 April 2016

http://helsinki.chamber.fi/media/filer_public/36/0f/360fddcd-4cfe-41a6-ab89-c028aa0bf15c/kyberturvallisuus_2015.pdf

Mcafee. 2016.Critical Infrastructure Readiness Report – Holding the Line Against Cyber Threats Accessed 14 April 2016
http://www.mcafee.com/us/resources/reports/rp-aspen-holding-line-cyberthreats.pdf

Europol. 2015. The Internet Organised Crime Threat Assessment 2015 (IOCTA). Accessed 10 May 2016
https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015

Committee on National Security Systems. 2010. National Information Assurance (IA) Glossary. Accessed 18 May 2016
https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf

Kaska, K. Osula, A-M. Stinissen, J. 2013. The Cyber Defence Unit of the Estonian Defence League - Legal, Policy and Organisational Analysis. Accessed 28 April 2016
https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf

Castellon, N. Frinking, E. 2016. Securing Critical Infrastructures in the Netherlands – Towards National Testbed. 2015. Accessed 29 April 2016
https://www.thehaguesecuritydelta.com/images/HSD_rapport_Testbed_EN.pdf

The Hague Security Delta. 2016. The Hague Security Delta. Accessed 27 April 2016
https://www.thehaguesecuritydelta.com/about

International Telecommunications Union. Global Cybersecurity Index & Cyberwellness Profiles 2015. Accessed 9 May 2016
http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

Bsa.2016. EU Cybersecurity Dashboard - A Path to a Secure European Cyberspace. Accessed 9 May 2016
http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf

Bsa. 2016. EU Cybersecurity Dashboard – Country Report Finland. Accessed 9 May 2016
http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_finland.pdf

Lee, R. Assante, M. Conway, T. 2016. Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case. Accessed 10 May 2016
http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

Security Week 2014. Eduard Kovacs. Cyberattack on German Steel Plant Caused Significant Damage: Report. Accessed 11 May 2016
http://www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report

Deutsche Welle 2016. Sarah Steffen. Hackers hold German hospital data hostage. Accessed 11 May 2016
http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030

Forbes 2016. Arafat Kabir. After Hackers Steal $81 Million, What Now For Bangladesh Central Bank? Accessed 11 May 2016
http://www.forbes.com/sites/arafatkabir/2016/03/16/after-hackers-steal-81-million-what-now-for-bangladesh-central-bank/#2cc614774a83

Bankinfosecurity 2015. Mathew J. Schwarts. DDoS Attacks Slam Finnish Bank. Accessed 11 May 2016
http://www.bankinfosecurity.com/ddos-attacks-slam-finnish-bank-a-7761

INTERVIEWS

Savisalo, S. Director. National Emergency Supply Agency. Interview with the author. 16 March 2016. Helsinki. Personal communication.

Räsänen, E. Business Continuity Manager. National Emergency Supply Agency. Interview with the author. 14 March 2016. Helsinki. Personal communication.

Salonen, M. Special Advisor. The National Cyber Security Center Finland. Interview with the author. 18 March 2016. Helsinki. Personal communication.

Figures