Joining NATO: Effects on Finland's Cyber Security

Aleksi Helin & Paula Himanen

2023 Laurea & Jamk

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Laurea University of Applied Sciences & Jamk University of Applied Sciences

Joining NATO: Effects on Finland's Cyber Security

Aleksi Helin, Paula Himanen
Information Technology
Security Management
Master’s Thesis
May, 2023

Laurea University of Applied Sciences & Jamk University of Applied Sciences **Abstract**

Degree Programme in Security Management, Degree Programme in Information Technology

Master of Business Administration, Master of Engineering

Aleksi Helin, Paula Himanen

Joining NATO: Effects on Finland's Cyber Security

Year 2023 Number of pages 99

The objective of this thesis was to identify the strengths and weaknesses of Finland’s cyber security as well as the threats and opportunities of NATO membership. These effects were used to analyze how to benefit most from the membership and how to avoid possible detriments. The purpose of the thesis is to increase awareness of Finland’s NATO membership from a cybersecurity point of view. The thesis was conducted as a theoretical study.

The theoretical framework consists of research on the North Atlantic Treaty Organization (NATO), cyber security, selected themes, and existing research on the thesis topic. The emphasis in the theoretical framework is on explaining the terms (themes) used in the thesis.

The thesis topic is divided into twelve themes based on the literature review. Each theme is evaluated individually and compared to each other in the analysis phase. The themes were cyber security management, cyber situation picture, cyber security preparedness, cyber security skills, legislation, cyberspace, cyber warfare, education and capabilities, indirect effects, intelligence, new collaboration partners, and new technologies.

The thesis was conducted using qualitative research methods for data collection and analysis. A literature review and semi-structured expert interviews were used for the data collection. The gathered data were analyzed using the SWOT (*strengths, weaknesses, opportunities, and threats)* analysis framework. SWOT analysis was utilized in comparing the cyber security strengths and weaknesses of Finland to the opportunities and threats of NATO membership. The themes were divided into overall categories based on the SWOT analysis, but most of the themes included both strengths and weaknesses or opportunities and threats. The overall analysis is based on the evaluation of each of these factors.

Finland’s cyber security has more strengths than weaknesses. Only legislation and cyber security management were seen as weaknesses. Membership in NATO provides significantly more opportunities than threats and was seen as a positive development for Finland. Cyberspace and indirect effects were seen as possible threats. Four strategies were identified for battling the threats arising from the membership and five strategies for receiving the benefits from the membership. One of the greatest opportunities was the increase of information sharing and thus the improvement of the situation picture. The identified threats (indirect effects and cyberspace) include multiple uncertainties, but it was found out that Finland has strengths that can be used in mitigating these threats.

The effects of NATO membership have been studied previously, but the focus has not been on cyber security. This thesis provides research information on the effects that the membership has on Finnish cyber security. Due to the vastness of the topic, further research is recommended on the discovered strategies to create action plans to implement them to practice.

Keywords: NATO, cyber security, SWOT analysis

Contents

1 Introduction

Finland applied for NATO membership on May 17th, 2022, to increase the nation's security (Ministry for Foreign Affairs of Finland, 2023). Most of the member countries ratified the membership within half a year after the application and by the end of the year 28 out of 30 member countries had ratified the application. Finland's membership was seen as increasingly likely to happen.

On April 4th,2023, Finland joined NATO. The interviews and the literature review for this thesis were done before the membership and therefore the effects that the membership has had after the membership are not discussed in this thesis.

NATO's collective defence and security guarantees, including Article 5, are considered the most significant effect of the membership (Ministry for Foreign Affairs of Finland, 2023). The effects of the membership have been speculated and there has been numerous research on the topic. Cyber security has been part of some of these studies, but it is less researched compared to other topics such as traditional warfare. A comprehensive study on cyber security effects that the membership may create has not been previously conducted. This thesis aims to respond to this gap and provide an overview of the opportunities and threats that the membership may provide to Finland's cyber security. A few of the previous studies that discussed NATO's cyber security effects are presented in Chapter 2.5 Existing research.

Cyber security is part of Finland's comprehensive security (The Security Committee, 2017a, p. 7). The importance of cyber security to society is addressed in Finland's cyber security strategy. It emphasizes the dependency on information networks and systems in daily activities as well as critical functions. (Ministry of Finance, 2023a). Due to the importance of the topic to the nation, the effects on cyber security must be studied as an entity of its own.

Firstly, the thesis aims to increase awareness of Finland's NATO membership from a cybersecurity point of view. Secondly, it aims to help to prepare for possible threats and to enable the best use of benefits by proactive planning. The research objectives are to identify the strengths and weaknesses of Finland's cyber security as well as threats and opportunities of NATO membership. These effects are used to analyze how to benefit most from the membership and how to avoid possible detriments.

The following research questions are used to answer the research problem:

1. What are the strengths and weaknesses of Finland's cyber security?

2. What are the threats and opportunities of NATO membership to Finland's cyber security?
3. How to avoid the threats produced by NATO membership?
4. How to benefit the most from NATO membership?

The thesis topic is divided into 12 themes which are each evaluated individually. The themes are divided into two categories: the strengths and weaknesses of Finland and the opportunities and threats of NATO. The strengths and weaknesses themes are cyber security management, cyber situation picture, cyber security preparedness, cyber security skills, and legislation. Opportunities and threats themes include cyberspace, cyber warfare, education &capabilities, indirect threats, intelligence, new collaboration partners, and new technologies. After the individual evaluation, the themes are compared with each other.

The thesis is conducted as a theoretical study. The knowledge base of the study is based on a literature review and expert interviews. The literature review consists of recent studies, publications, and articles on the topic. The expert interviews include ten subject matter experts from the public sector.

The thesis consists of theoretical background, which discusses NATO, cyber security in general, and the cyber security topics that were selected for the interviews. Discussion and evaluation of existing research is a part of the same chapter as theoretical background. Chapter 2, theoretical background, is based mainly on the literature review of the thesis topic. Chapter 3, methodology, introduces the research methodology that was used for the thesis and chapter 4 explains how research methodology was used in practice when researching the thesis topic. Chapter 4 explains how the data was collected and analyzed in detail. Chapter 5 discusses the analysis of the data which was collected as well as the results that originate from the analysis. The results can be used to answer research questions 1 and 2. These results are discussed even further in the following chapter, conclusions, which then compares the analyzed results with each other to form strategies on how to avoid the threats produced by NATO membership and how to benefit most from NATO membership. In the last chapter, the thesis is evaluated and reflected upon. It forms a vision of what could have been done differently, what were the limitations of the thesis and what are the following research problems that could be introduced from the results of this thesis. It also discusses the reliability, validity, and integrity of the thesis and the research methods.

2 Theoretical background

The theoretical background of this thesis is gathered from a literature review of relevant topics. Firstly, NATO and its functions are introduced. NATO's Washington Treaty and its articles are relevant to cyber security, and they could have significant effects on Finland's cyber security when it joins the NATO alliance. NATO's cyber organization is also introduced briefly.

Cyber security organizations in European Union are introduced, even though they are not the focus of this thesis. The thesis focuses on NATO and Finnish organizations regarding cyber security. However, the EU has some relevant aspects due to the international nature of cyber security.

Cyber security is a vast topic, which can be divided into various areas. In this thesis, cyber security is studied through twelve topics. These topics are introduced in this chapter in general and they are analyzed even further with the data that is gained from the expert interviews. Lastly, existing research on the topic is discussed and reviewed.

2.1 North Atlantic Treaty Organization (NATO)

NATO was founded on 4 April 1949 in Washington D.C. The 12 founding members signed The North Atlantic Treaty, or The Washington Treaty, which is still the cornerstone of the Alliance to this day. The founding members of NATO are Belgium, Canada, Denmark, France, Iceland, Italy, Luxembourg, the Netherlands, Norway, Portugal, the United Kingdom, and the United States (NATO, 2022a).

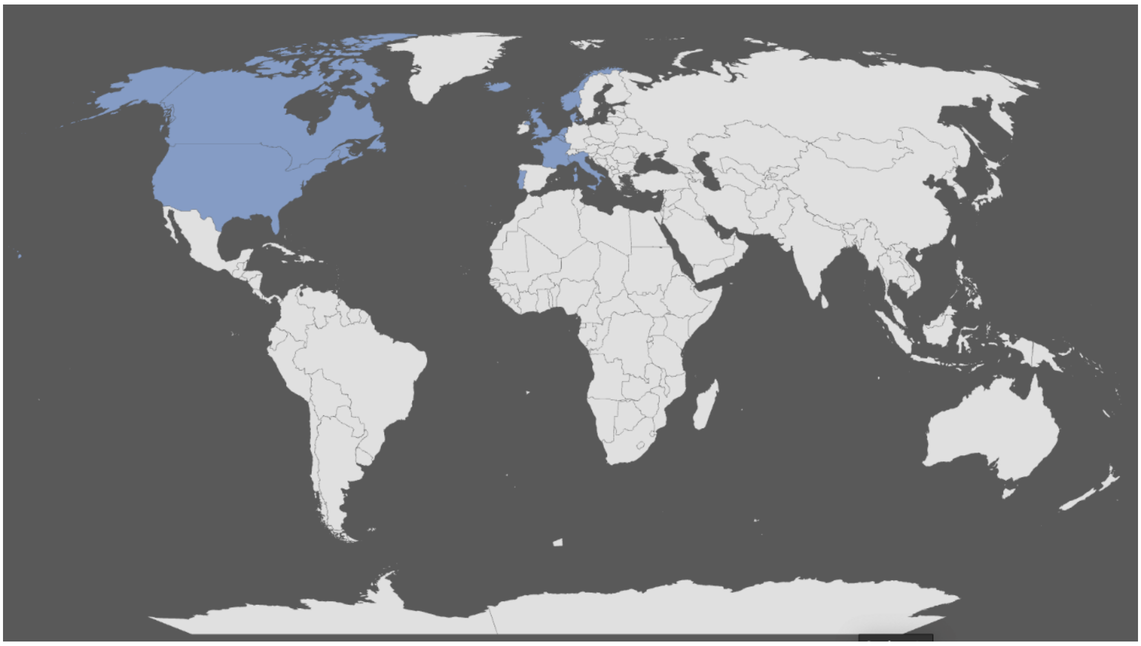


Figure 1 Map of NATO founding members (in blue)

NATO was founded to create an Alliance which could combat the risk of the Soviet Union (NATO, 2022b). Article 5 of the Washington Treaty's 14 articles is fundamental for the

Alliance to function properly. It states that an armed attack against one or more member states shall be considered an attack against all of them. Every member state shall also take action to assist the ally that is attacked (NATO, 1949). Allies can decide individually what kind of assistance they shall provide if Article 5 is invoked (NATO, 2022b). Regardless of the situation, allies must always make a unanimous decision regarding the invocation (Finnish Government, 2022a, p. 24).

When signing the treaty in 1949, the nations were expecting to invoke Article 5 because of invasion or some other more traditional attack. In the modern world, cyber-attacks are a part of warfare, and cyber-attacks against a NATO member could trigger Article 5 (Finnish Government, 2022a, p. 24). The level of armed attack may be reached by a single or cumulative set of malicious cyber activities or hostile operations (NATO, 2022h, p. 7). In NATO's Brussels summit meeting (2021), the Alliance reaffirmed that the decision on the invocation of Article 5 in case of cyber-attack is done case-by-case. It is recognized that the impact of cumulative cyber activities may be the same as from an armed attack. (NATO, 2022j)

Since all NATO decisions are made by consensus of allies, Article 4 is important to discuss in relation to Article 5. Article 4 can be invoked regarding any issue a member state deems to be important to their territorial integrity, political independence, or security. Consultation and decision-making in the Alliance is done in day-to-day business, and do not need the invoking of Article 4. The Article 4 has only been invoked seven times in NATO's history, which are presented in Figure 2.

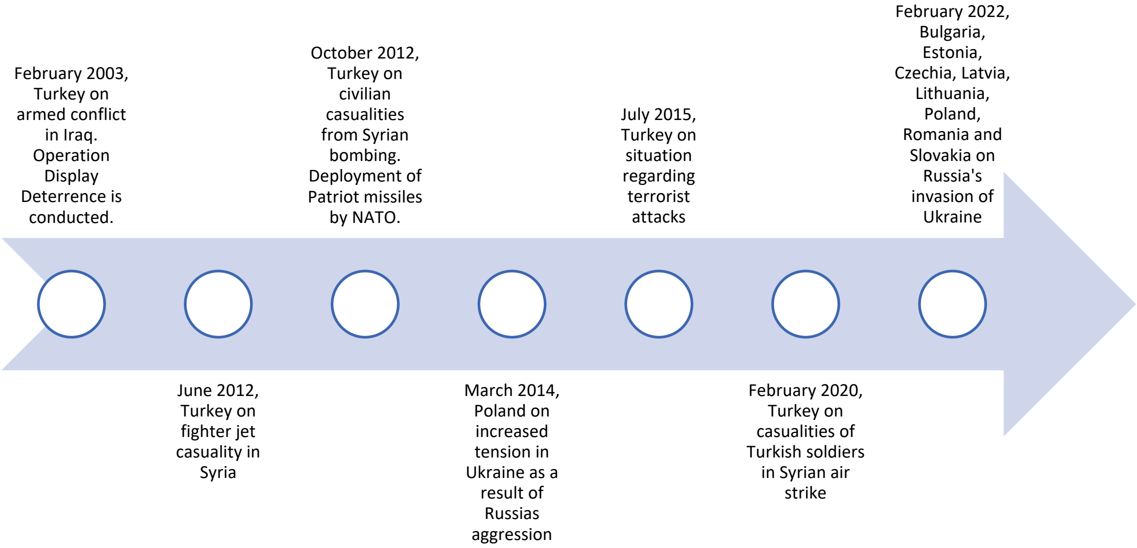

February 2003, Turkey on armed conflict in Iraq. Operation Display Deterrence is conducted.
June 2012, Turkey on fighter jet casuality in Syria
October 2012, Turkey on civilian casualities from Syrian bombing. Deployment of Patriot missiles by NATO.
March 2014, Poland on increased tension in Ukraine as a result of Russias aggression
July 2015, Turkey on situation regarding terrorist attacks
February 2020, Turkey on casualities of Turkish soldiers in Syrian air strike
February 2022, Bulgaria, Estonia, Czechia, Latvia, Lithuania, Poland, Romania and Slovakia on Russia's invasion of Ukraine

Figure 2 Invocations of Article 4

Article 3 of the Washington Treaty obligates alliance members to prepare, resist and recover from armed attacks. This means developing their resilience in both civilian and military domains. Even though the original focus was on armed attacks, resilience today consists of multiple vulnerabilities that need to be taken into focus. NATO has agreed on seven baseline requirements, which member states should take into consideration when developing their resilience capabilities (NATO, 2022n). They are presented in Figure 3.

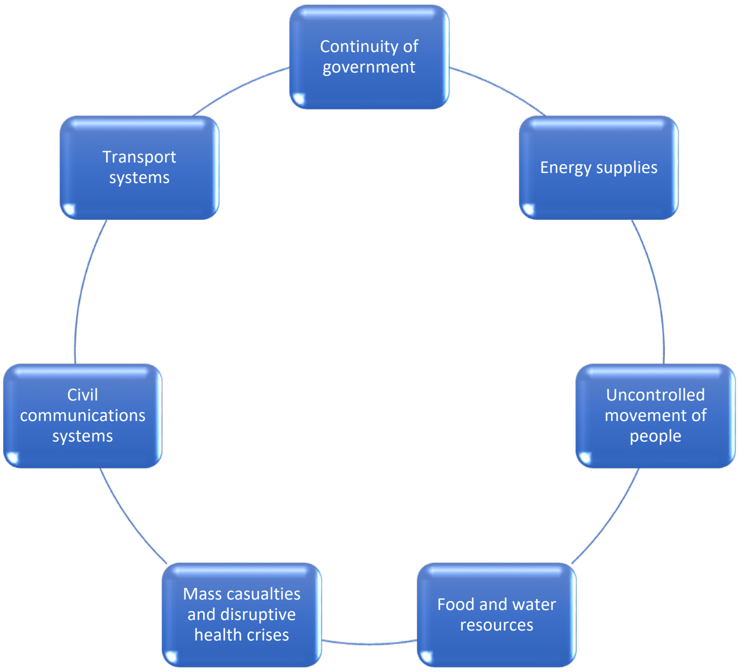

Continuity of government
Energy supplies
Uncontrolled movement of people
Food and water resources
Mass casualties and disruptive health crises
Civil communications systems
Transport systems

Figure 3 Resilience baselines

Civilian and military cooperation in resilience is vital. An illustration of this in cyber is transatlantic internet traffic, which includes military communications. Approximately 90 percent of the traffic is made possible by undersea fiber-optic cable networks, which are civilian infrastructure (NATO, 2022n). Since the separation of civil and military in a resilience context seems impossible, it is in NATO's interest to also improve the defense capabilities of civil organizations as well, which also includes their cyber defense. To highlight this, allies have signed The Cyber Defense Pledge at Warsaw Summit 2016 (NATO, 2016).

2.1.1 NATO cyber organization

The organization of NATO consists of civilian and military structures as well as organizations and agencies (NATO, 2022c). This thesis focuses on bodies that are relevant from a cyber perspective. These bodies are presented in Figure 4.

The highest (political) decision-making body in NATO is North Atlantic Council (NAC). It is currently led by Jens Stoltenberg, and it includes representatives from each member country.

Directly under the command of NAC are the NATO Military Committee, Cyber Defence Committee, and office of the chief information officer. NATO Military Committee is the highest level in NATO's military structure and the second highest decision-making body in NATO. (NATO, 2022d) Cyber Defense Committee is responsible for political governance and defence policy in cyber (NATO, 2022e). The role of Chief information officer (CIO) and chief information security officer (CISO) are in the office of the chief information officer. Currently, both posts are filled by Manfred Boudreaux-Dehmer. CISO is responsible for all cybersecurity issues in NATO. His tasks include for example leading incident management, improvement of NATO's cybersecurity posture, and increasing cybersecurity awareness across NATO. (NATO, 2021a)

Under NATO Military Committee are two equal strategic commands: Allied Command Operations (ACO) and Allied Command Transformation (ACT). The command headquarters of ACO is Supreme Headquarters Allied Powers Europe (SHAPE). Under the command of SHAPE is Cyberspace Operations Centre (CyOC), which provides situational picture and coordinates NATO's operational activity in cyberspace. (NATO, 2022f)

ACT has responsibility for planning and conducting the annual Cyber Coalition Exercise, which is one of the world's largest cyber defence exercises. Finland has been participating in these exercises previously as Partner Nation. (NATO, 2022g)

In addition to the civilian and military structure, NATO has multiple organizations and agencies that take part in NATO's cyber security. One of the important agencies is NATO Communications and Information Agency (NCI). NCI has multiple functions in NATO and its responsibilities vary from Air and Missile Defence Command and control to NCI academy. Cyber security services are on the core tasks in the agency, and it is operated in NATO Cyber Security Centre. Cyber security is also included in the agency's other services such as NATO's Consultation and Command Networks. The centre provides cyber security related services to NCI Agency stakeholders. It also works as a place for cyber information sharing, training, and expertise for allies and partner nations. NATO's Rapid Reaction Team (RRT) in cyber is located at the centre. The centre used to be called NATO Computer Incident Response Capability Technical Centre (NCIRC). (NATO, 2023a)

Another important cyber body in NATO is the NATO Cooperative Cyber Defence of Excellence (CCDCOE). CCDCOE arranges multiple cyber security exercises and trainings such as Locked Shields and Crossed Swords. In addition to trainings and exercises the body is focused on research. (CCDCOE, 2023a)

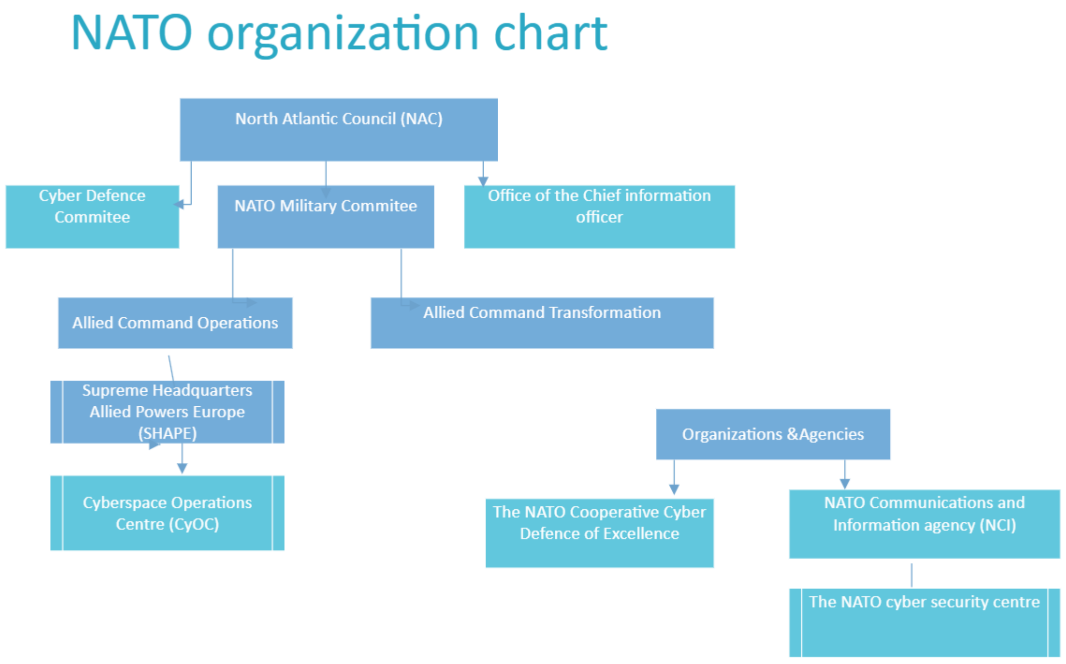

NATO organization chart
North Atlantic Council (NAC)
Cyber Defence Commitee
NATO Military Commitee
Office of the Chief information officer
Allied Command Operations
Allied Command Transformation
Supreme Headquarters Allied Powers Europe (SHAPE)
Cyberspace Operations Centre (CyOC)
Organizations &Agencies
The NATO Cooperative Cyber Defence of Excellence
NATO Communications and Information agency (NCI)
The NATO cyber security centre

Figure 4 NATO organization chart

2.1.2 NATO's core tasks

NATO 2022 strategic concept aligns with NATO's main objective as ensuring the collective defence of the Allies. The collective defence includes a response against all threats, from all directions. The main objective is divided into three core tasks which are deterrence and defence, crisis prevention and management, and cooperative security. The core tasks are implemented by political and military means. (NATO, 2022h, pp. 6-7) Base for the deterrence and defence comes from the Alliance's 360-degree approach which covers land, air, maritime, cyber, and space domains (NATO, 2022i).

Effective deterrence and defence require secure and unconfined access to cyberspace. The Alliance strives to enhance the cyber defence and the ability to operate effectively in cyberspace. The objective is to tackle all kinds of threats by preventing, detecting, countering, and responding actions. (NATO, 2022h, pp. 6-7)

Crisis prevention and management in NATO include preventive and responsive measures. They are directed at crises that may affect the Alliance's security. Preventive measures are preferred over responsive ones. Cyber is not specifically mentioned in the crisis prevention and management part of NATO's strategic concept (NATO, 2022h, p. 9).

The third core task of NATO, cooperative security, pursues to ensure the security of the Alliance and its member countries. The security of the countries aspiring to become members as well as the security of the partner countries is considered. EU is one of the crucial partners of NATO and they have a longstanding partnership. NATO and the EU have many common interests, one of them being cyber threats. The common security challenges are tackled within the alliance as well as in cooperation with partners and third parties. (NATO, 2022h, pp. 10-11)

2.2 Cyber security in European Union

European Union published its first Cybersecurity Strategy in 2013. The strategy divides cyber security into three pillars, which are network and information security, law enforcement, and defence. It also defines EU-level entities related to cyber security. National governments are seen as the main entities in organizing the prevention and response to national cyber incidents (CCDCOE, 2023b). The strategy was updated in 2020 and it contains proposals to develop regulations, investment, and policies regarding cyber security in European Union (European Commission, 2022).

The main EU entities in network and information security are European Commission, the European Networks and Information Security Agency (ENISA), CERT-EU, and the European Public-Private Partnership for Resilience (EP3R). EUROPOL, CEPOL, Eurojust, and European Cybercrime Centre are the main entities in cyber security law enforcement in the EU. Defence pillar consists of military defence entities, such as the European External Action Service (EEAS), the European Union Military Staff (EUMS), and the European Defence Agency (EDA) (CCDCOE, 2023b).

Cyber security in European Union is a broad subject with a multitude of entities. This thesis does not aim to study the effects of Finland's NATO membership to the European Union. However, Finland is linked to European Union in cyber security, and references to European Union and its entities are unavoidable.

2.3 Cyber security in Finland

The important cyber security actors in Finland can be divided into six categories. The same categories were used in the Finnish Government's report (Finnish Government, 2023, p. 22). Firstly, every organization has its cyber or information security department, which contributes to the cyber security of Finland. Due to the limitations of this thesis, private organizations are not focused on. Effects on their cyber security originating from NATO membership are not in the scope of this thesis. Valtori is the Government ICT Centre. Its role in cyber security is to act on cyber security incidents that happen in shared services of the Government or their network (p. 22).

Finnish Transport and Communications Agency Traficom is responsible for acting on cyber security incidents that affect Finland. These actions may include detecting, preventing, and investigating serious cyber security incidents involving fi-domains (Laki sähköisen viestinnän palveluista 917/2014). Criminal investigation officials, such as the Police of Finland, have the authority and responsibility to deal with cybercrimes (Finnish Government, 2023, p. 22). These differ from cyber security incidents, even though a cybercrime might cause a cyber security incident. However, their role is to investigate the crime and not to solve the cyber security incident.

Intelligence officials, such as the Finnish Security and Intelligence Service, aim to discover cyber threats to national security or national defence. Their role is to investigate the potential effects of the discovered threat and to present information about it to security officials, the Finnish Defence Forces, and the Finnish Government. Finnish Defence Forces are responsible for defending Finland against military attack or a threat resembling it (p. 22). A serious cyber-attack against Finland that endangers its sovereignty could be an example of a cyber incident that is the Finnish Defense Forces' responsibility to repel.

2.4 Themes

The topic is divided into 12 themes. Five of the themes cover the strengths and weaknesses of Finland in cyber security and the rest seven themes cover the opportunities and threats of NATO. This chapter includes the theory base and descriptions of each theme. In addition, to the twelve themes, cyber security term is presented in this chapter.

The theory base includes the clarification of the term that is used in this thesis. The theory base does not include the evaluation of the strengths and weaknesses of Finland nor the opportunities and threats of the membership. The evaluation of the themes is presented in chapter 5. Results and analysis and chapter 6. Conclusions.

The themes are selected based on a literature review on the topic. The theory base behind the themes is presented in chapter 4.1. Data collection.

2.4.1 Cyber security

Cyber security is a subject that is incorporated into every aspect of this thesis. Even though it is not an interview subject on its own, the definition is an important part of understanding the thesis context.

Cyber security and information security should not be confused with each other. The Security Committee has specified cyber security to be a state in which cyberspace can be trusted and its function is secured (The Security Committee, 2018, p. 31). Information security means arrangements that aim to ensure information confidentiality, availability, and integrity (p. 10).

NATO defines cyber security as the “application of security measures for the protection of communication, information and other electronic systems, as well as the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation” (NATO, 2019). Information security is seen to be protection against unauthorized disclosure, transfer, modification, or destruction (NATO, 2005).

United States Department of Defense (DOD) has its own definitions, which do not include information security or cyber security. Cyberspace security is however defined as “Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation” (Department of Defense, 2021). This definition as well as NATO’s definition of cyber security can be seen as a combination of elements from other definitions of cyber and information security. NATO’s cyber security and DOD’s definitions of cyberspace security are fairly similar, while The Security Committee’s definition seems to take a different perspective on the matter. In this thesis definition of The Security Committee is used.

The number of cyber-attacks has been increasing in recent years. The targets can range from individuals to municipalities and governments. Finland’s cyber defense should be designed to combat large-scale cyber-attacks from a nation-state actor. The Finnish government has analyzed that these kinds of attacks could target national decision-making, operations of safety and security officials, and critical infrastructure (Finnish Government, 2022a, p. 32).

Companies in Finland face a threat of cyber-attacks ranging from more primitive attacks such as denial of service (DoS) and data break-in to more serious and advanced hostile cyber activity (Finnish Government, 2022a, p. 32). Especially companies working with critical infrastructure, which are excellent targets for nation-state actors, must be vigilant in protecting their environment. Even though a cyber-attack would not be directed toward Finland, it can still have substantial effects because of the global integration of information systems (p. 32).

2.4.2 Cyber security management

Leadership is listed as one of the seven vital functions to society in Security strategy for society. Leadership is vital at all operational levels. Leadership enables the baseline to safeguard the rest of the vital functions listed in the strategy. Functioning leadership is required at all times and all levels. Effective leadership requires clear responsibilities, a situation picture, crisis communication, information sharing, continuity management, and cooperation. (The Security Committee, 2017a, p. 15) In this thesis, leadership related to cyber security is referred to as cyber security management. The focus is on national cyber security management and excludes cyber security management of i.e., the private sector.

Better coordination of cyber security management is part of one of the three objectives defined in Finland's latest cyber security strategy. As a response to the objective, the strategy outlines that a role of Cyber Security Director will be established to coordinate the national development of cyber security. The role of the Director is to coordinate the development, planning, and preparedness of national cybersecurity. The Cyber Security Director is also responsible for acting as an adviser for the central government in cyber security issues. The implementation of the new role doesn't change the current cyber security roles and responsibilities of ministries and authorities. (The Security Committee, 2019, p. 6) Deputy Cyber Security Director acts as a substitute and work partner for the Cyber Security Director. (Ministry of Transport and Communications, 2022)

To fulfill the objectives of the national cyber security strategy, National Cyber Security Development program has been created. The timeline for the Development program is 2021-2030. Cooperation between the public and private sectors in cyber security is emphasized as a significant factor in improving cyber security management. (Ministry of Transport and Communications, 2021, p. 8)

The publications on cyber security management in Finland are mainly focused on strategic level. Tactical and operational levels are not highlighted. The council of state has the overall responsibility for the strategic management of cyber security. The tasks include political guidance on cyber security, strategic alignments as well as deciding on the resources and preconditions of operation. Ministries are responsible for complying with the instructions given by the council of state and management of cyber security incidents. (Laari, et al., 2019, p. 15)

The strategic management of cyber security is defined in the report Strategic management of cyber security in Finland as "identifying and setting goals based on the protection of the digital operating environment. Furthermore, it implies coordinating actions and preparedness as well as managing extensive disruptions." (Lehto, et al., 2018, p. 4) Three significant factors in cyber security management are strategic sensitivity, flexible resources, and coherent leadership. These factors apply to all leadership, not only cyber security management. Cyber security management consists of the management of severe disturbances in normal conditions and state of emergency. Cyber security management also includes preparation and management of cyber security incidents. (Lehto, et al., 2018, p. 12)

Finnish defence forces are responsible for military cyber defence which is part of national cyber security. They bear the responsibility of protecting the cyber domain from external attacks and have leadership role in these situations. Cooperation between civilian and military parties is needed to have functioning cyber security management on national level. (Finnish Government, 2021a, p. 34)

2.4.3 Cyber situation picture

Endsley divides situational awareness into three levels, which are connected (Endsley, 1995). The same methodology can be applied to cyber security. Situational awareness and situation picture need to be comprehended differently. Situation picture means collecting and organizing data to present a picture of the current situation.

This mass of data could be described as situation data. In Endsley's model, situation data is on the bottom level, perception. A useful situation picture contains background information as well as predictions about the evolution of the situation, which are constructed by analyzing the situation data.

Situational awareness consists of Endsley's model's levels 2 and 3, which are comprehension and projection. Situation awareness is the knowledge that is needed to make decisions regarding the current situation (The Security Committee, 2017b, p. 64). This can be achieved through situational assessment of the current situation (Endsley, 1995, p. 36). A properly documented situation picture is essential in achieving situation awareness. Without it, it is not possible to understand what is happening and what is going to happen. Situational awareness is considered to be the most important tool in decision-making and managing cyber operations (Laari, et al., 2019, p. 52).

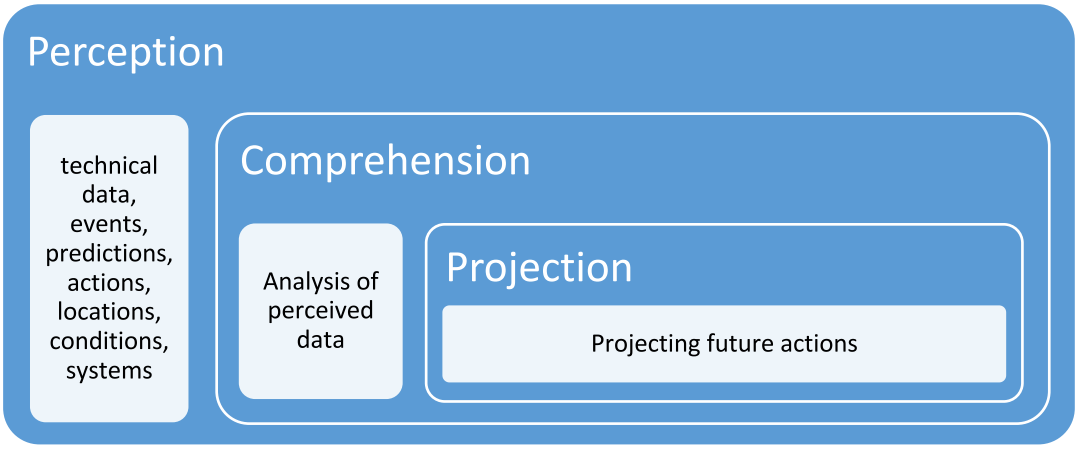

Perception
technical data, events, predictions, actions, locations, conditions, systems
Comprehension
Analysis of perceived data
Projection
Projecting future actions

Figure 5 Levels of situational awareness (Endsley, 1995)

Before planning and implementing actions in cyberspace, one must form a cyber situation picture. This can be done by perceiving what is happening in cyberspace and then comprehending what is happening, through analysis of the perceived information. It is possible to also project future events from collected data. However, as can be seen in Figure 5, information needs to be perceived and comprehended before projection can be done.

Technical data and details are only a part of situational awareness in cyberspace (Laari, et al., 2019, p. 17). By perceiving situational data from the physical world and data from other sources, such as risk analysis of the current situation, one can form an even superior situational picture. Forming a situation picture needs monitoring and detection methods to collect relevant data and cooperation between organizations (Finnish Government, 2021a, pp. 25-28). Co-operation between military and civil organizations regarding situational awareness is also recognized in the Finnish Government's report to be mandatory to implement effective defensive measures against cyber-attacks to Finland. A need to improve this cooperation is recognized and improvements regarding it are being assessed (Finnish Government, 2022a, p. 33).

The National Cyber Security Director of Finland is situated in the Ministry of Transport and Communications. The manager is responsible for the current situation picture of Finland's cyber security. In the event of a serious cyber incident, the Ministry of Transport and Communications together with the Director will coordinate the situation in co-operation with other relevant ministries (Finnish Government, 2022b). Cyber security situational picture is a similar concept as situation picture. It is an accumulated description of the security and availability status and of the current situation of cyberspace. National Cyber Security Centre Finland (NCSC-FI) collects and coordinates the national cyber situational picture (The Security Committee, 2018, p. 22).

2.4.4 Cyber security preparedness

The objective of preparedness is to enable operations to function as normal as possible. It aims to prepare for possible incidents in the future. Preparedness planning, continuity management, education, and training are important parts of preparedness. (The Security Committee, 2017a, p. 9)

Cyber security preparedness means actions to prepare for cyber incidents/attacks such as malware and denial-of-service (DoS). Good information security is the baseline for cyber security preparedness and it's crucial for the continuity of an organization or nation. Regular preparedness as well as cyber security preparedness actions need to be done in advance before an ongoing state of emergency or incident. (National Cyber Security Center, 2022)

Finland has long traditions in cyber security preparedness, and it is enforced by legislation, cooperation between authorities, and preparedness training. According to the Ministry of Transport and Communications Finland's cyber security situation is normal and cyber defence processes are active and functioning. (Finnish Government, 2022b)

Preparedness became an especially significant topic of discussion during the Covid-19 pandemic and after Russia attacked Ukraine in 2022. Cyber security preparedness was raised especially due to the war in Ukraine. Shortly after Russia's attack National Cyber Security Center of Finland stated that the state of cyber security in Finland is currently stable. (National Cyber Security Center, 2022) Speculation on possible cyber-attacks on Finland and the need for preparedness was raised in public media. (Iltalehti, 2022)

Better coordination of cyber security management, planning, and preparedness is listed as one of the three main objectives in Finland's cyber security strategy. Cyber security management is covered in chapter 2.4.2. National Cyber Security Development program supports the fulfillment of the objective. Effective cyber security preparedness requires cooperation between the private and public sectors. Education and training in preparedness are needed in both sectors. Supply chain security is a significant part of cyber security preparedness and must be considered when pursuing to reach the objective of the strategy. (The Security Committee, 2019, pp. 6-7)

An example of cooperation between the private and public sectors is the upkeeping the operability of networks. Functioning networks are vital to the whole society and telecommunications operators bear a significant role in cyber security preparedness in the network area. Many of the operators are experienced in preparedness which supports the national resilience. (National Cyber Security Center, 2022) & (Iltalehti, 2022)

2.4.5 Cyber security skills

The development of cyber security skills is one of the three main objectives of Finland's latest cyber security strategy. Cyber security skills are required in everyday life as well as in work life in the public and private sectors. National cyber security is built on cooperation between officials, the private sector, agencies, and citizens. Individuals' actions can have an effect on their cybersecurity as well as on the cybersecurity of the whole nation. (The Security Committee, 2019, p. 8)

Public and private organizations need skilled cyber security professionals to manage cyber security risks. In addition to professionals, regular workers need to be trained in basic cyber security skills. Cyber security professionals are needed not only in organizations operating in cyber security but nearly in all fields of business. (The Security Committee, 2019, pp. 8-9)

Currently, there is a lack of cyber security workforce globally. According to a recent cybersecurity workforce study, there is a need for 3.4 million cybersecurity workers. The amount of cybersecurity workers has grown recently, but it hasn't been enough to respond to the growing demand. The skills shortage is predicted to continue in the future. (ISC2, 2022, pp. 8, 73, 74)

Finland is also experiencing a shortage of skilled cyber security professionals. The global shortage makes the rival of employees more difficult. 73% of respondents in cyber security survey identified a significant shortage of skilled cyber security professionals within their organization. According to the survey there is a need for 4000 professionals in cyber security organizations already. (University of Jyväskylä, 2022a, pp. 115-116) In 2020, Finnish Information Security Cluster (FISC) estimated that in 2025 there would be a need for 15 000 cyber security professionals. (Finnish Government, 2020a, p. 3)

The need for more cyber security professionals was addressed also by the media in late 2022. The media article highlighted that there aren't enough graduates for cyber professions nor does the education encounter the needs of work life. (YLE, 2022a)

To fulfill the strategic objectives in cyber security strategy, and to respond to the identified shortage of cyber security professionals, Finland needs to increase cyber security education qualitatively and quantitatively. Cyber security education and training need to be addressed comprehensively within the education system (beginning from primary school and continuing to universities). In addition, other stakeholders such as companies and adult education centers arrange cyber security training. (University of Jyväskylä, 2022a, pp. 5-10)

At the end of 2022, University of Jyväskylä and JAMK University of Applied Sciences received 3,4 million in funding to develop cyber security education. The objective of the funding is to improve security in Finland and to respond to the identified need for skilled cyber security professionals. (University of Jyväskylä, 2022b)

The importance of cyber security skills is emphasized in Microsoft's Digital Defence report, which states that over 98% of cyber-attacks are preventable by basic security hygiene. Multifactor authentication, zero trust principles, modern anti-malware, updates, and data protection are some of the mentions of basic security hygiene. (Microsoft, 2022, p. 108)

Regular citizens are provided with various materials to improve their personal cybersecurity. The Security Committee and VAHTI network are a few examples of parties providing these materials. The Security Committee has published a guidebook to operate securely in Digital world. The guidebook advises on basic principles such as firewalls, passwords, and virus protection. The objective is to provide basic knowledge on how to avoid the most common problems such as phishing scams online. (The Security Committee, 2017c)

Finnish VAHTI network develops digital security and provides material for companies and individuals on information security. These materials include guidelines for organizations as well as announcements on current information security trends. (Digital and Population Data Services Agency, 2023) Citizens' cyber skills are also developed by training provided by third parties such as The National Defence Training Association of Finland, (MPK)

(Maanpuolustuskoulutus, 2023). Training and guidelines are a few of the tools used to reach the goal in cyber security strategy (development of cyber security skills).

2.4.6 Legislation

In context of this study legislation regarding cyber defense and cyber security is meaningful. NATO presents a new aspect, with its own articles as a part of The North Atlantic Treaty. As a NATO member, Finland is obligated to follow the articles of the treaty but also gains the benefit of other allies following them. Most substantial benefit could emerge from Article 5.

The question regarding whether hostile actions in cyber space could be associated as an armed attack against a nation-state has been discussed extensively and many interpretations about it can be found. The Charter of United Nations prohibits the use of military force and the threat of using it (Yhdistyneiden Kansakuntien peruskirja 1/1956). The Charter is an instrument of international law and Finland as a United Nations member state is also bound by it (United Nations, 2023). As a part of a conventional kinetic attack, any kind of cyber-attack can be regarded as use of military force (Sirjonen, 2019). If cyber-attack is the only form of aggression, it is debatable whether it fulfills the attribution of military use of force in the context of international law and The UN Charter.

Sirjonen debates in his article (2019), that a cyber-attack is an act of military aggression when it is conducted to further military or political goal of a nation, and it has a direct or indirect effect on the physical world. This conclusion is also echoed by Michael Schmitt, a NATO cyber warfare expert (Schmitt, 2002). However, his definition differs from Sirjonen's and requires more than isolated incidents and that the cyber-attacks are meant to cause damage or death. Isolated cyber-attack would not be considered a military use of force regarding Schmitt and following this logic, article 5 of The North Atlantic Treaty would be problematic to use. Finland published its perception of international law in cyberspace in 2020 (Finnish Government, 2020b). Finland considers cyber-attack that is comparable to an armed attack in its effects and magnitude as an armed attack and it is possible to retaliate to it by means of self-defense. This implies that Finland would consider invoking Article 5 in the event of serious cyber-attack against it.

NATO Cooperative Cyber Defence Centre of Excellence has published the Tallinn Manual, which consists of recommendations on how to combat cyber-warfare. While not legally binding document, it is considered to be NATO’s acknowledgment that rules of engagement for cyber warfare are a necessity (Caso, 2014). Tallinn Manual dictates in its Rule 30(2-3) that “*attacks means acts of violence against the adversary, whether in offence or in defence*”. With this logic, it rules out psychological cyber operations as well as cyber espionage as attacks. Furthermore, an act of violence is not limited to violent actions. In Rule 30(3) is stated that the consequences of an act must be violent (Caso, 2014). For example, shutting down an electric system of a building does not directly cause casualties or damage. However, it is possible that this action could cause harm indirectly and be considered a violent action, for example by interfering with monitoring of patient's health or operations of a critical factory component.

Finland's legislation framework considering cyber security and cyber defense is too extensive to be covered completely in this thesis. Finland does not have a singular cyber-law, rather it has cyber embedded in different decrees. Police Act (Poliisilaki 872/2011) contains regulation regarding civil cyber intelligence and Act on Military Intelligence (Laki sotilastiedustelusta 590/2019) regarding military cyber intelligence. Intelligence laws have been updated to comply with one another and have been regarded as a somewhat successful update to cyber legislation in Finland (Finnish Government, 2021b, p. 36).

Act on Electronic Communications Services (later ECSA) (Laki sähköisen viestinnän palveluista 917/2014) obligates organizations that are critical for national emergency supply to report cyber security breaches or deviations. Deficiency of this law is that all organizations are not obligated to report their deviations in cyber security. Reporting aspect is strongly associated with cyber situational awareness in Finland. The law also added improvements to the security of national networks, by prohibiting the use of devices that could endanger national safety or national defense. ECSA also aims to improve information security of the public sector's networks and information resources. It prohibits the use of devices that could endanger national security or national defense in the critical parts of the communication network (Finnish Government, 2022a, p. 33). In an event of disruption, ECSA enables to implement actions to protect information security. These actions include concluding the contents of a message, denying, or restricting messaging, and deleting content that could endanger information security (Lehto, et al., 2018, pp. 16-17).

Legislation regarding information management as well as information security has been recently renewed. Act on Information Management in Public Administration (Laki julkisen hallinnon tiedonhallinnasta 906/2019) and Government Decree on Security Classification of Documents in Central Government (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019) define the information security requirements and information management practices for the authorities. These laws are further elaborated by guidelines and instructions made by Information Management Board. (Ministry of Finance, 2023b)

However, cyber legislation as an entirety can be seen as fragmentary, even though some legislations is working as intended. Cyber is an entirety that influences many aspects of Finnish society. The magnitude of cyber effects makes the work of lawmakers challenging. Example of the extent of organizations in the scope of one law can be perceived in ECSA's list of entities that oversee the obeying of the reporting obligation. Organizations are divided into different sectors and sectors are overseen by a certain official, which are presented in Figure 6 (Valvira, 2023).

Legislation regarding cyber is seen as a development point by the Finnish Government (Finnish Government, 2022a, p. 33). It is closely related to cyber situation picture and the roles and responsibilities of the officials. A report on the authorities' capacity to act in cyber matters aims to clarify the roles and responsibilities in cyber situation picture context. (Finnish Government, 2023)

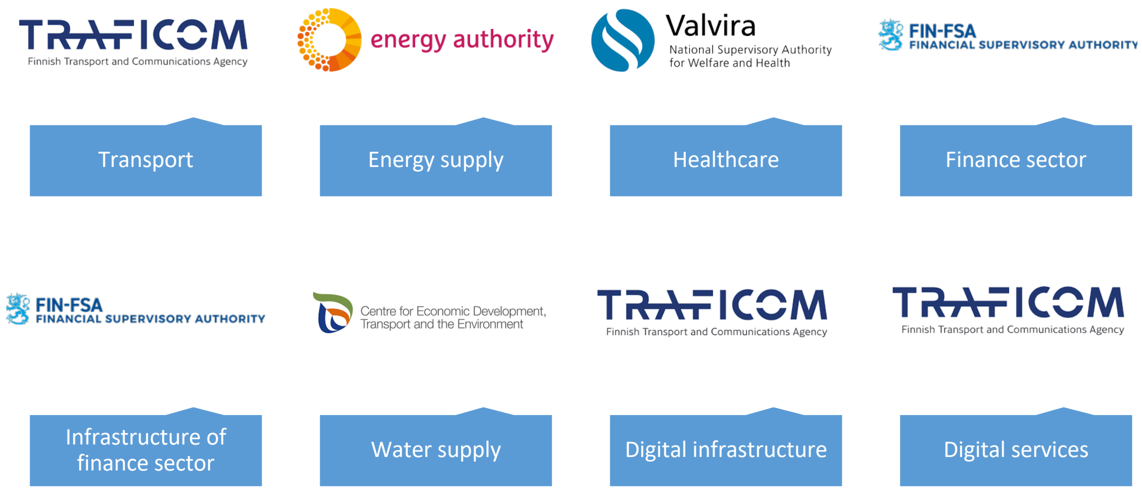

TRAFICOM Finnish Transport and Communications Agency
energy authority
Valvira National Supervisory Authority for Welfare and Health
FIN-FSA FINANCIAL SUPERVISORY AUTHORITY
Transport
Energy supply
Healthcare
Finance sector
FIN-FSA FINANCIAL SUPERVISORY AUTHORITY
Centre for Economic Development, Transport and the Environment
TRAFICOM Finnish Transport and Communications Agency
TRAFICOM Finnish Transport and Communications Agency
Infrastructure of finance sector
Water supply
Digital infrastructure
Digital services

Figure 6 ECSA actors

2.4.7 Cyberspace

Cyberspace has multiple definitions as well as synonyms. The term and definition used vary between actors. The term has been described especially by military actors. A few of the synonyms for cyberspace are cyber environment and cyber domain. Cyber domain is mainly used in a military context. The term cyberspace is used for this thesis.

Cyberspace is a vast and complex term, which can be difficult to comprehend. Simplified description divides it into two units; the physical world and the digital world (cyberspace). The digital world is artificial and created by people. These two worlds are closely linked to each other and incidents occurring in the digital world may have effects in the physical world and vice versa. Cyberspace is part of our everyday lives and most of today’s functions are reliable on information flows (Laari, et al., 2019, pp. 8,10,11,14) & (JCS, 2018, pp. 22-23).

Internet is a crucial part of cyberspace, but it also includes for example industry automation, objects in internet of things (IoT) and control systems. Cyberspace activities are not limited to daily activities such as email and social media but also include parts of critical infrastructure and other relevant functions for society. Cyberspace is accessible nearly to everyone and everywhere. In all situations, cyberspace is dependent on physical factors such as power supplies and datacenters. (Laari, et al., 2019, pp. 10-11)

According to the Security Committee, cyberspace consists of one or multiple digital information systems. Physical structures that relate to information and data management are included in cyberspace. Examples of cyberspace are nuclear control systems and logistics systems. (The Security Committee, 2018, p. 21)

Cyberspace has no physical borders, is global by nature and has multiple vulnerabilities. Therefore, cooperation nationally as well as internationally is imperative. Cyberspace is significant not only to national defence but also for the whole society as they are dependent on information and communication systems. (Laari, et al., 2019, pp. 5,8,10)

The complexity of cyberspace may be described by layers. The layers vary slightly between actors. Many of the military actors divide cyberspace into three layers which are the physical network layer, logical network layer/virtual and cyber-persona layer/cognitive. (JCS, 2018, p. 22) Non-military organizations such as ENISA also use layers to define cyberspace. ENISA’s layers describe cybersecurity protection through Maslow’s Pyramid of needs approach. The different levels on the pyramid describe how different challenges in cyberspace should be handled. (ENISA, 2017, pp. 4-5)

The physical network layer consists of physical infrastructure, systems, and IT devices such as computers. The logical network layer consists of elements that are not physical such as services and programming code. The layer is also referred to as the virtual layer. Most of the cyber-attacks occur in this layer. The cyber persona layer or cognitive layer consists of people and personas who operate in cyberspace. The layer connects people to cyberspace. Most of the cyberattacks start from the cyber persona layer (i.e., via phishing email). (JCS, 2018, pp. 22-24) & (Laari, et al., 2019, pp. 13-14) & (Ministry of Defence, 2022, p. 12)

There is no one actor responsible for cyberspace. Companies, ministries, agencies, and non-governmental organizations (NGO’s) are all responsible for their own networks. Few of the crucial actors in cyberspace in Finland are Finnish government, National Cyber Security Centre, National Bureau of Investigation, digital and population data services agency and Erillisverkot. Finnish Defence Forces are responsible for cyber defence. Threats within cyberspace are not limited to companies nor to cyber or security professionals. Operating securely in cyberspace is everyone’s business. Basic cyber skills are required from all the users operating in cyberspace. (Laari, et al., 2019, p. 10)

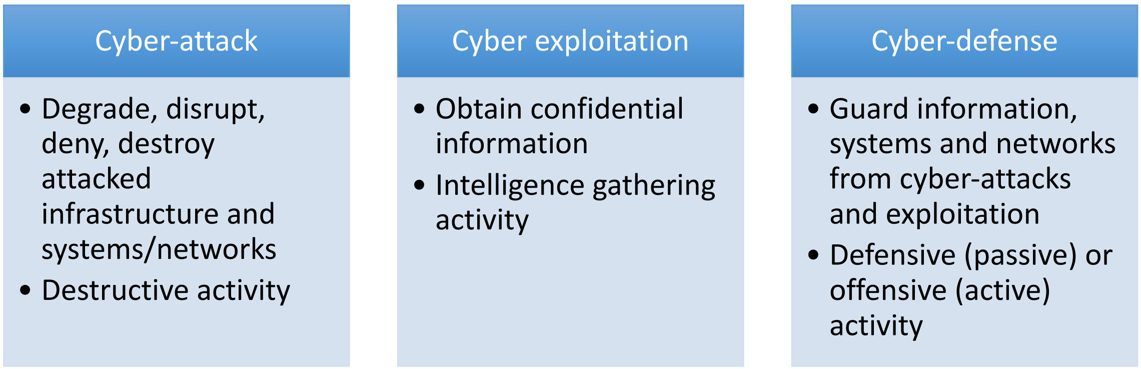
Cyberspace is protected by raising the threshold for cyberattacks. The same principle applies to land, maritime, and air defence. Rapid detection of threats and maintenance of current situation picture is important in protection of the cyberspace. (Finnish Government, 2021a, p. 34)

2.4.8 Cyber warfare

Developed nations such as Finland are dependent on information technology for critical infrastructure, civilian and military purposes. Adversaries such as cyber criminals or nation state actors can leverage this and plan attacks that would be inexpensive and with little risk to them (Gervais, 2011). Low-risk and economical attacks which can also have potentially devastating effects on the physical world has made the cyber domain more frequently used in conjunction with traditional warfare. Russia has used cyber-attacks as a part of their attack in Ukraine. It is suggested that Russia will probably expand its cyber and information operations west from Ukraine as well (Finnish Government, 2022a, p. 32).

Since the term "cyberwarfare" can be interpreted in many ways and has no defined meaning, it shall be divided into three categories in this thesis. They are cyber-attack, cyber exploitation, and cyber-defense. Cyber-attacks can be defined as "*deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks*" (National Research Council, 2009, pp. 10-11). Even though there are various ways to describe cyber-attack, most of them point out that these attacks have destructive nature. An example of a cyber-attack is erasure of data by a computer virus. In comparison, cyber exploitation is commonly seen as non-destructive. A computer virus that searches infected hard disks for all files containing particular information, such as credit card numbers, would be viewed as a tool of cyber exploitation (Lin, 2010).

Cyber-defense aims to guard systems against cyber-attacks and exploitation. Cyber-defense itself can be divided to passive and active defense measures. Passive measures include measures such as hardening systems, facilitating recovery from a successful attack, and educating users (National Research Council, 2009, p. 13). In cyber warfare however, passive measures are often not enough. Thus, active measures need to be applied as well. Active measures of cyber-defense are very similar to cyber-attacks. However, their intention is different. Active measures of cyber-defense could be described more as self-defense than attack. Eliminating or degrading adversary's means of attack can halt the attack in progress or stop it before it was even launched (p. 13). This kind of defensive activity is often accomplished by means like those of cyber-attack. Another type of active defense is the knowledge of deterrent in place in case of cyber-attack. This might deter the adversary from attacking completely if consequences or costs of the attack would raise to be too high (p. 14).



Cyber-attack

- Degrade, disrupt, deny, destroy attacked infrastructure and systems/networks
- Destructive activity

Cyber exploitation

- Obtain confidential information
- Intelligence gathering activity

Cyber-defense

- Guard information, systems and networks from cyber-attacks and exploitation
- Defensive (passive) or offensive (active) activity

Figure 7 Cyber-attack, exploitation, and defense

2.4.9 Education and capabilities

Bodies related to NATO’s cyber capabilities are presented in chapter 2.1.1 NATO cyber organization. These bodies provide the base for NATO’s cyber defence. Each of these bodies have a unique role within the alliance. Tasks of few of these bodies are elaborated in this chapter.

CCDCOE has the main responsibility in cyber defence operations education and training discipline in NATO. It is responsible for the training and education of cyber defence within the whole Alliance. The trainings are provided in strategic, operational, legal, and technical level. Some of the trainings are also available to sponsoring nations and contributing participants. In addition to trainings, CCDCOE takes part in most of the major NATO exercises such as Trident Juncture and Cyber Coalition. (CCDCOE, 2023c)

Another important educational body in NATO is NCI Academy. It has long-term experience on providing training and education across the Alliance. The academy provides training in technical, operational, and managerial levels. Its vision is “To reinforce technological edge through excellence in cyberspace learning.” (NATO, 2023b)

Cyber defence was first mentioned on the Alliance’s political agenda in 2002 NATO Summit in Prague. The first policy on cyber defence was approved years later in 2008, after cyber-attacks against Estonia. Since then, the role of cyber in NATO’s Summit meetings has only increased. Cyber threats are emphasized as growing threat and various actions are set up to improve the cyber defence of the Alliance. (NATO, 2022e) The timeline in Figure 8 presents some of the main cyber points made within the recent Summit meetings. Through the decisions made in the meetings NATO aims to improve its cyber capabilities and enhance the cyber posture of the Alliance.

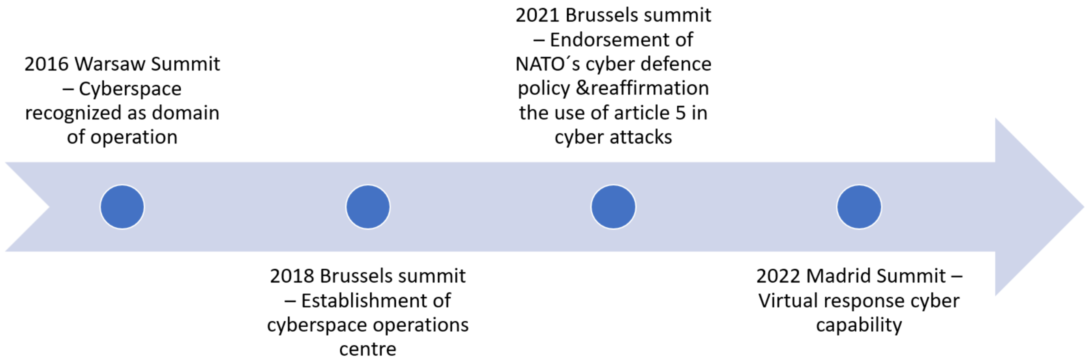

2016 Warsaw Summit – Cyberspace recognized as domain of operation
2018 Brussels summit – Establishment of cyberspace operations centre
2021 Brussels summit – Endorsement of NATO´s cyber defence policy &reaffirmation the use of article 5 in cyber attacks
2022 Madrid Summit – Virtual response cyber capability

Figure 8 Recent Summit Meetings

Cyberspace was recognized as domain of operations at Warsaw Summit in 2016. Since then, cyber defence has been part of NATO's core task (collective defence). Each member of the Alliance is committed to developing their national networks and infrastructures. NATO's capabilities will also be under continuous improvement. The development of cyber capabilities also means further investments on cyber security bodies within the Alliance. Despite the developments in cyber capabilities of NATO, each member country is responsible for protection of their networks and systems. NATO is only responsible for its own assets. (CCDCOE, 2023d)

In Brussels Summit 2018, the decision of establishment of cyberspace operation center was made. The role of the center within the Alliance is described in chapter 2.1.1 NATO cyber organization. (NATO, 2018)

The endorsement of NATO's cyber defence policy was done in 2021 Brussels Summit. The policy was created to respond to the increasing threats within the cyberspace. The objective of the policy is also to support the fulfilment of NATO's three core tasks. The use of Article 5 in cyber-attacks was discussed in the same Summit. (NATO, 2022j)

Madrid Summit Declaration emphasizes how the Alliance is confronting cyber threats. As a response to the emerging threats, the allies decided to create a virtual response cyber capability. The objective of the capability is to respond to significant cyber activities. The capability is based on voluntary action and national assets. (NATO, 2022k)

2.4.10 Indirect effects

Indirect effects in cyber can be interpreted negatively as attack that aim to affect the target in a non-traditional way, for example. It is possible that indirect effects would be positive as well. Trying to force a way through a firewall could be seen as a direct attack in cyber. Indirect would be something that aims to pass the firewall completely, like social engineering. One technical example is indirect command execution (The MITRE Corporation, 2022a). Windows command-line interpreter cmd is used to perform operations to interact with the system (The MITRE Corporation, 2022b). Indirect command execution is a technique that aims to perform operations without invoking the often very highly monitored and protected cmd.

In warfare the term symmetrical and asymmetrical are often used to describe opponents that are not equal in their strength (Palonkangas & Paronen, 2022, pp. 1-3). Cyber and hybrid warfare can be both asymmetrical and indirect and they can have effects on politics, economy, science, culture and sports (p. 83). Actions in cyberspace can have effects globally and indirectly. Attack that is targeted to Finland can have effects in countries that were not targeted at all. In same context, attack that is targeted to NATO country can possibly have direct or indirect effects to Finland. Joining NATO can be seen to propose indirect cyber threats to Finland. Furthermore, accepting Finland as a NATO member can propose indirect threats to NATO as well. This theme aims to uncover these threats and possible opportunities. as a part of conducted the SWOT analysis.

2.4.11 Intelligence

The objectives of intelligence have remained the same since the first book on intelligence was created 500 years before the Common Era. Intelligence services collect and analyze data and report on the results to political or military leadership. Technology has been seen as one of the variables that defines intelligence. Technology developments have shaped intelligence and created new possibilities but also threats. New technologies have for example facilitated collection of extensive amounts of data. On the other hand, new technology also facilitates the intelligence of the adversary. The rapid development of technology and society's increasing dependency on networks have resulted in formation and increasing use of cyber intelligence. (Paul, 2005, pp. 23-25)

Intelligence function in Finland is divided into civilian intelligence operations conducted by Finnish Security and Intelligence Service (SUPO) and military intelligence operations conducted by Finnish Defence Forces. The objective is to gather information that can't be obtained by other means. The intelligence operations are targeted to gather information on actors and phenomenon that threaten Finland's national security. In addition, information is gathered to respond to information need of top-level national government and authorities. (Finnish Government, 2021b, p. 11). Intelligence is prioritized based on nationally defined priorities (Supo, 2023a).

Cyber intelligence is a form of intelligence and has the same objective as other forms of intelligence such as human intelligence. It consists of network intelligence and all other fields used in traditional intelligence to form situational awareness in cyber. These traditional fields are referred to as ISR (intelligence, surveillance, reconnaissance). Intelligence refers to general information collection and analysis on certain topic, surveillance refers to monitoring of network or actor and reconnaissance refers to targeted information collection of specific target. (Laari, et al., 2019, pp. 56-57)

Cyber intelligence is sometimes referred to as synonym for cyber ISR. Cyber intelligence and cyber ISR are conducted in and through friendly, neutral and adversary cyberspace (JCS, 2018, p. 13) (Ministry of Defence, 2016, p. 56)

According to ENISA (2019-2020, p. 2) cyber espionage is defined as “the use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization”. Cyber espionage can be divided into two vectors: state espionage and industrial espionage. The focus in this thesis is mainly on state espionage, where state actors are involved (ENISA, 2017, p. 7). The difference between cyber intelligence and cyber espionage is that cyber espionage is conducted by using illegal methods.

2.4.12 New collaboration partners

Threats in cyber space are global and international cooperation is essential to cyber security and cyber defence. Bilateral and multilateral cooperation in cyber is active and one of the strategic alignments in developing cyber defence is to improve international cooperation. The objective is to focus the resources on already existing relationships that support the development of cyber performance the best (Ministry of Defence, 2019, p. 9). Since cyberspace and cyber threats are global by nature, international cooperation is pivotal to Finland’s cyber security and cyber defense. Cooperation is not always technical, but also political cooperation regarding cyber security and defense needs to be noticed (Finnish Government, 2021a, p. 26).

Education and training are significant aspects in cooperation. Finland has already taken part in NATO’s cyber exercises before the membership. For example, in 2022, team from Finland attended Locked Shields exercise and won the competition. (CCDCOE, 2022a) International exercises are listed as one of the focus areas in defense cooperation in the latest Government’s Defence Report. International cooperation parties will also be asked to join international exercises in Finland. (Finnish Government, 2021a, pp. 44-45)

Most notable multilateral cooperation associations are European Union, NATO and Nordefco. Other notable associations include Joint Expediationary Force (JEF), which is a framework for defence cooperation in Northern Europe and the Baltic Sea led by United Kingdom (Ministry of Defence, 2023). Nordefco also aims to strengthen collaboration in the Nordic during military crises and conflicts (Finnish Government, 2021a, pp. 41-42).

Most notable bilateral partner nations are listed in Government's Defence Report. These are Sweden, Norway, and the United States. United States has significant capabilities in military technology and especially in new technologies. Some technologies are only available to Finland through international cooperation. Among other focus areas, situational picture sharing with Sweden and Norway are one example of benefits from collaboration bilaterally. Other notable collaboration partners are the United Kingdom, Germany, France, and Estonia (2021a, pp. 42-44). Collaboration with these mentioned nations is already strong, as well as with European Union and NATO.

Joining NATO as a member nation may present Finland new opportunities to gain more collaboration partners among NATO member nations or deepen the existing partnerships even further. NATO has a variety of network and group within the alliance. These could provide Finland with opportunities to develop understanding and expertise in areas that are important to Finland's security. Examples of the group are those of counter-terrorism, counter-proliferation and emerging security challenges, such as cyber defense (NATO, 2022m). NATO membership can also present opportunities to businesses in Finland. The NATO Communications and Information Agency initiated noteworthy cooperation with King ICT Croatia and IBM Belgium, by signing a contract for provision of cyber security deployment and configuration service across NATO. Both Croatia and Belgium are NATO member states (NATO, 2023e).

2.4.13 New technologies

The alliance is committed in investing into new technologies and solutions as part of fulfilling the Alliance's core tasks. Application of new technologies and their proper use impacts the success on the battlefield as well as cyberspace. Cooperation within the Alliance as well as with the private sector is vital to stay on brink of the new technologies. (NATO, 2022h, pp. 3,5,7).

NATO allocates its research on new technologies to technologies that it categorizes as emerging and disruptive (EDTs) (NATO, 2022l). In this study, new technologies will focus on NATO's EDTs and the opportunities and threats they present. NATO has launched world's first multi-sovereign venture capital fund, NATO Innovation Fund, in 2022 NATO Summit in Madrid. Its investments will support innovation within the Alliance and are closely linked to the Defence Innovation Accelerator for the North Atlantic (DIANA), launched just year before the fund in 2021 Summit in Brussels (NATO, 2022l). The Fund has three strategic objectives. It seeks to solve the Alliance's defense and security challenges with technological solutions while improving innovation in the Alliance and supporting its start-up development. DIANA also focuses on solving defense and security problems with technology. It will do so by operating security challenge programmes, which are based on the most critical problems that the Alliance faces.

artificial intelligence (AI)

data

autonomous systems

quantum-enabled technologies

biotechnology

hypersonic technologies

space

novel materials and manufacturing

energy and propulsion

Figure 9 NATO’s innovation areas

By using new technologies, such as artificial intelligence and quantum-enabled technologies, NATO can embrace vast number of opportunities. However, its opponents are also ready to use the same new technologies, if they are technically capable. This will present NATO threats that can be combatted with the use of new technological solutions.

Innovation Hub is a collaboration platform sponsored by NATO ACT where experts from NATO, academia and private sector can work together on NATO’s future capability challenges. Innovation Hub has produced various projects and products related to cyber since 2012 (Innovation Hub, 2023). Artificial Intelligence has been studied at Innovation Hub, and it has provided NATO and the Alliance with reports on it in 2019. Benefits of using AI as support tool for human intelligence was studied in 2021, however both reports were made only for NATO members and are not available to public (Innovation Hub, 2023). Artificial Intelligence Front End Learning Information Execution (AI FELIX) is an artificial intelligence and machine learning experiment, which helps NATO Headquarters staff to manage the enormous amount of data that is delivered daily (NATO, 2023c). AI FELIX’s is built to automate metadata extraction, which helps it to distribute information faster. AI can process a document in seconds and analyses its contents by tracking keywords or patterns that appear. This same process could take human at least minutes if not hours. AI FELIX is a public example of new technologies that could be useful for Finland as a NATO member.

2.5 Existing research

The discussion about Finland's NATO-membership has been active since Finland joined the European Union in 1995. Numerous studies have been conducted trying to predict the effects of joining NATO. In 2016 Finland's Ministry for Foreign Affairs commissioned research (Bergqvist, et al., 2016) which divided the effects into six categories which include legacy, Europe, convergence, cohesion, Russia, and decision making. The relation to cyber security can be found in chapters describing the benefits of joint cyber defense (Bergqvist, et al., 2016, pp. 19-21,46-47). The threat of Russia and more specifically its tactics that combine cyber-attacks and traditional warfare is also described (Bergqvist, et al., 2016, pp. 16-17). However, this aspect is not described as a threat because of Finland joining NATO, but as a threat that exists with or without it.

Recent study about Finland's NATO-membership (Forsberg, et al., 2022) was conducted to activate current political discussion by providing key facts and analysis. In his study, Forsberg's (Forsberg, et al., 2022, pp. 16-20) analysis about the benefits of NATO-membership indicated that the main benefit is military deterrent provided by NATO alliance. Even though the context of deterrent provided in the study is focused on traditional warfare, cyber aspect is also relevant. In relationship to deterrent, Forsberg also mentions the safety of being a NATO-member. The safety aspect is in a direct relationship to The North Atlantic Treaty Article 5 (NATO, 1949). Article 5 also applies to cyber warfare operations, as concluded before.

Finnish Government assessed the effects in its recent report (Finnish Government, 2022a). The most significant effect is that Finland would be protected by NATO allies in case of an attack, as stated in Washington Treaty's Article 5. The deterrence of Finland's defense would be considerably greater since it would be backed by every NATO ally in case of attack (Finnish Government, 2022a, p. 25). However, Article 5 also mandates Finland to assist other allies in case any of them were under attack. In this case, Finland could individually decide which kind of help it would provide to its allies. Russia has stated that Finland joining NATO would require actions to balance the military-political situation. This could mean affection towards Finland (Finnish Government, 2022a, p. 27) which could potentially be in form of cyber-attacks. Affection and pressure towards Finland are predicted to happen during the membership process (p. 28). This report also states that authorities' responsibilities and mandates regarding cyber defense need to be clarified and cooperation and exchange of information need to be assessed (p. 16). Co-operation regarding cyber defense with NATO has been ongoing for several years. However, since Finland has not been a full NATO member, the benefits from it have been limited (p. 35). NATO has been a partner of Finland in various other areas of co-operation, including preparedness and resilience. Co-operation in this area has made possible to bolster Finland's strong competence and has helped to improve predictability and stability of the nation (p. 42). Preparedness is undeniably linked to critical infrastructure. Its performance in a crisis is mandatory, thus it needs to be protected against cyber-threats and possible to recover from those attacks that made it through the defense (p. 43).

The possible effects (in cyber) of Finland joining NATO have been also predicted in cyber threatscape report by Accenture in 2019. The report highlights that NATO's enlargement to countries such as Finland, Sweden or Ukraine may attract cyberthreat activity to these countries. The report presents an example of such incidents happening in Montenegro and North Macedonia related to their process of joining NATO. Both countries were allegedly targeted by a group called SNAKEMACKEREL. (Accenture, 2019a) The group is associated to group descriptions such as APT 28, Fancy bear and IRON TWILIGHT (MITRE, 2019). The attacks were targeted to the government officials (Accenture, 2019b).

Direct effects of joining NATO have also been discussed in another brief report by Finnish Government (Finnish Government, 2022c). The number of personnel working with NATO-related matters needs to be raised (Finnish Government, 2022c, p. 3; Bergqvist, et al., 2016; Bergqvist, et al., 2016). This most likely includes cyber security professionals, since cyber is essential part of NATO. The report concludes that Finland should apply for NATO-membership, which was done at 17.5.2022 (Ministry for Foreign Affairs of Finland, 2022). No direct negative effects regarding cyber were discussed in the report.

The relation between Finland and NATO in cyber security has been discussed already in the early 2000-centuary. Cooperation in general has been regarded as beneficial to Finland's cyber security posture, whether it's bilateral or multilateral. Cooperation in cyber is especially crucial as the cyber threats are global. According to the study, Finland has benefitted from partnership with NATO, but has not reached the full potential of the benefits in cyber as it is not a member country. The limitations include for example receiving information on current threat actors and technologies. (Kärkkäinen, 2013, pp. 102-103).

3 Methodology

This research is conducted using qualitative research methods for data collection and data analysis. Since the nature of the research questions is very explorative, quantitative methods are illogical for attaining the goals of the research (Vuori, 2021). Inductive approach is applied since the research question has not been answered in previous studies and data collection and analysis methods support inductive reasoning. Thus, no theory or hypothesis is presented at the beginning of the study (Dudovskiy, 2023). Furthermore, the research group for interviews is selected expediently for their knowledge on the subject oppositely to random selection (Hirsjärvi, et al., 2007, p. 160).

Data is collected with expert interviews and from previous studies as a part of literature review of this study to form a hypothesis about the effects of joining NATO. Gathered data is analyzed using SWOT (*strengths, weaknesses, opportunities, and threats)* analysis framework. SWOT analysis in this study is presented similarly as in business (Kennedy, et al., 2020), however, the target in this case is Finland and its strengths and weaknesses regarding cyber security. These are compared with opportunities and threats that are presented by Finland's NATO membership. Analysis of these effects aims to answer the research questions of this study.

Research questions are presented in chapter 3.1. Answering these questions introduces a vision of the state of Finland's cyber security after joining NATO. This problem forms the perspective of this study and dictates which kind of data collection and analysis methods are the most suitable for this study (University of Jyväskylä, 2009).

Study is delimited to studying the effects that joining NATO has to Finland's cyber security. Cyber security as a concept is also divided into themes, which limits the scope of the study even further.

3.1 Research aim, objectives, and questions

Aim, objectives and questions form the golden thread of the thesis as they are aligned together and help to focus on the relevant topics (Phair & Shaeffer, 2022). The aim of the thesis is to increase awareness of Finland's NATO membership from cybersecurity point of view. In addition, it aims to help to prepare to possible threats and to enable best use of benefits by proactive planning. These aims could also be identified as the research problem.

The research objectives are to identify the strengths and weaknesses of Finland's cyber security as well as threats and opportunities of NATO membership. These effects are analyzed through SWOT analysis to comprehend how to get most out of NATO membership and how to avoid possible detriments. Research objectives are defined according to S.M.A.R.T. principles. They are specific, measurable, achievable, relevant, time-bound (Yemm, 2013).

Research questions that this study will answer are "What are the strengths and weaknesses of Finland's cyber security?", "What are the threats and opportunities of NATO membership to Finland's cyber security?", "How to avoid the threats produced by NATO membership?" and "How to benefit the most from NATO membership?".

3.2 Data collection methods

Expert interviews are the main data collection method in this study. Since the subject is current and not fully studied before, interviews present the best method to gather information. Forming premeditated questions in the form of survey was considered too leading. Forming structured questions for survey was also challenging, since the anticipation was that the research problem will provide many types of answer that would need different approach that survey could provide. Clarifying and deepening given answers was also anticipated to be crucial for the success of the study and to get the full benefit from the experts that were interviewed.

Interviews as a data collection method can be divided to three types (Hirsjärvi, et al., 2007, p. 202). Structured interview is done heavily relying on a form that has been made before the interview. Questions and statements will be presented in the same order and form in each interview session (p. 203). This method was ruled out as it was considered too similar to survey in the context of this study. Unstructured interview requires special interview skills are requires plenty of time to complete (pp. 204-205), which excludes it from the list of methods that can be used for this thesis. Semi-structured interview fit best for data collection since the themes for the interview were quite broad and without any structurization the interviews would have been exceedingly long.

Semi-structured interview offered a way to interview the experts on the themes that they were most proficient at without compromising the integrity of structured interview since it is possible to ask the interviewees different questions on the same topic while conducting a semi-structured interview (Hirsjärvi & Hurme, 2004, pp. 47-48). Furthermore, it made possible for the interviewees to decline commenting on the themes that they felt to be not suitable for them. Interviews produce initial answers for the research questions “What are the strengths and weaknesses of Finland’s cyber security?” and “What are the threats and opportunities of NATO membership to Finland’s cyber security?”. However, this data still needs to be analyzed to confirm the initial results of the interview.

3.3 Analysis methods

Analysis of collected data is done with qualitative research methods. Coding (Juhila, 2023) is done to raw data from interviews to organize it correctly for analysis. Data from interviews comes as partly coded, since the interviews are conducted according to set themes. Coding is essential even though data is partly coded. In this case, deductive coding is used (Crosley, 2020) since the coding stems from the interview themes and as such, is pre-established before interacting with the data itself. In the process of interview, it is possible to gather data in the wrong theme since semi-structured interview allows discussion to flow fairly freely. Without the use of coding, it could be possible to interpret the data wrongly which could affect the results of analysis. It is also possible to discover new themes in the interview data with the help of coding.

Themes for the interviews are also divided to two different categories which are strengths and weakness's themes and opportunities and threats themes. These categories are pre-determined since SWOT analysis is used as a method to analyze the interview data. SWOT analysis presents the framework to analyze Finland's strengths that support opportunities from NATO membership among other combinations which are presented more thoroughly in chapter 5.1. By analyzing the data with SWOT, it is possible to gain answers to research questions "How to avoid the threats produced by NATO membership?" and "How to benefit the most from NATO membership?". SWOT can be seen as a thematic analysis method since it categorizes the themes so that they can be analyzed further with the SWOT categories (University of Jyväskylä, 2010).

4 Research implementation

Data collection methods consist of literature review and interviews. Results of data produced by literature review is mainly presented in chapter 2. Data produced by the interviews is presented in chapter 5 and is analyzed further in chapter 6.

Data analysis is done according to SWOT analysis framework. Firstly strengths, weaknesses, opportunities, and threats are concluded from the gathered data from the interviews. Then these categories are examined in relation to each other to find combinations which will then form strategies to implement the desired effects. Combinations and strategies are discussed further in chapter 6. This chapter presents how to research was implemented in practice.

4.1 Data collection

Literature review and interviews are used as the main source of information in this research. Literature review includes the themes used in the research and background information on NATO and its cyber security. The literature review is done using electronic and printed sources. The most recent sources are aimed to use for the literature review, as the topic is very current and the field of cyber security is constantly changing,

The interviews are conducted by using semi-structured expert interviews. The total amount of interviewees for the research is ten. The interviewees are selected expediently based on their expertise. The target group for the interviews are subject matter experts in public sector. The interviewees are experts in different fields of cyber security and/or NATO. All the interviewees volunteered to participate in the research.

The interviews are conducted by two master thesis workers. One of the thesis workers conducted the interview and the other one made notes during the interview. The interviews were also recorded, if permitted by the interviewee. The interviews were conducted in Finnish. The interviews were conducted either face-to-face or via Teams meeting. The duration of the interviews is between one and two hours.

Due to the sensitivity of the topic, the interviewees were given a choice to participate anonymously. The interviewees are referred to in three ways: 1. own name and organization 2. Organization and no name 3. No name nor organization. Interviewees are referred to as follows: I1, I2, I3, I4 and so forth.

The interview questionnaire is divided into two parts according to the SWOT analysis. First part includes themes related to strengths and weaknesses of Finland's cyber security. The second part consists of threats and opportunities created by NATO membership. The themes in the first part are: cyber security situation picture, cyber security skills, cyber security management, legislation, cyber security preparedness. The second part consists of the following themes: cyber security warfare, cyberspace, indirect effects, new technologies, intelligence, new collaboration parties and education & training.

The interviewees are given a choice on which themes they most wanted to be interviewed based on their expertise. Not every theme is discussed with all the interviewees. The interview questions may be elaborated based on the answers of the interviewees. Each interviewee answers to at least one theme in both parts of the interview questionnaire.

The interview questionnaire includes same questions for each theme in part one and two. The questions between part one and two are different. The questions are formatted based on the research question. The questions are rather general, so they don't lead the interviewees to any direction. The interview questionnaire is presented in Appendix 1.

Themes for the research were selected based on a literature review on the topic. Multiple sources were used to create comprehensive picture and to decide the themes used in the research. The themes selected for this thesis don't provide comprehensive list of cyber security related themes that may be affected by the NATO membership. They may also have overlapping and linkage to other themes. The possible relationship between different themes is described in chapter 5.1. SWOT analysis. The most significant sources for the theme selection are presented in Figure 10.

The themes for the part one in questionnaire were selected based on the most recent cyber security publications in Finland. These include for example the Finnish Cyber Security Strategy, Security Strategy for Society and Information Security Audit Tool for Authorities (Katakri 2020). The subjects presented in these publications were compared and considered by the thesis workers. The themes were selected based on consideration which themes are especially important and would most be affected by the NATO membership. Due to the limitations of the resources in the research some themes such as more technical side is excluded.

The Finnish Cyber Security Strategy defines three main objectives to improve and maintain the cyber environment in Finland. Cyber Security Management, cyber security preparedness and cyber security competence are crucial parts of these objectives. Situation picture and legislation are also mentioned within the strategy as means of reaching the objectives. The topics in the strategy are also relevant to some the themes in questionnaire such as cooperation and education & training (The Security Committee, 2019).

Security Strategy for Society includes principles and guidelines for national preparedness. It also presents a cooperation model for comprehensive security. Vital functions to society are presented in the Strategy. Some of the themes for strength and weaknesses (such as leadership, preparedness) and for opportunities and threats (i.e., new collaboration partners, cyber warfare) are lead from these functions. The strategy covers security comprehensively and is not limited to cyber security, but cyber security is firmly part of it (The Security Committee, 2017a, pp. 3,14).

Katakri is a tool used by authorities to access the level of information security. it provides examples how information security controls should be set up when protecting classified information. Katakri is based on Finnish legislation and therefore includes crucial parts on information and cyber security that need to be addressed (Ministry for Foreign Affairs of Finland, 2020, p. 5).

NATO's recent (cyber) publications are used as a base for defining the themes in part two of the questionnaire (opportunities and threats). NATO's strategic concept and the most recent Summit Meetings were benefitted in the definition work.

The Strategic Concept defines the core tasks of NATO and includes commitments made by the Alliance. Cyber Security is a part of the Alliances core tasks, and the strategy includes multiple references on cyber security. These parts were used in defining the themes for strengths and weaknesses. (NATO, 2022h, p. 1)

Most of the recent NATO's Summit Meetings include direct or indirect mentions on cyber security. The agendas of the summit meetings are reviewed to get clarified picture on cyber actions that the Alliance has planned. (NATO, 2023d)

Due to NATO's role as political and military organization, the research and themes cover both of these aspects. The line between political and military side can be difficult to define.

Political decisions may lead to military actions and military actions may lead to political decisions and so forth.

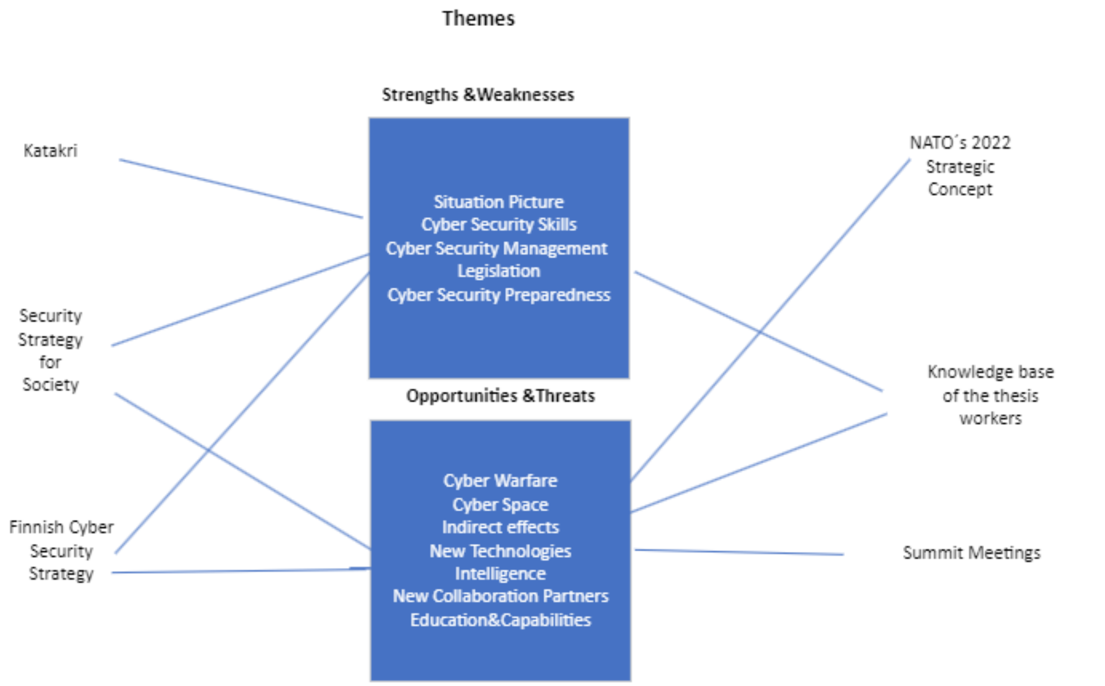


Figure 10 Theme sources

4.2 Data analysis with SWOT

SWOT analysis is used to categorize the themes and to analyze the data. The objective of the SWOT-analysis in this research is to be able to answer the research questions. Finland's strengths and weaknesses in cyber security are identified within five themes. Opportunities and threats are identified within seven themes. The identification aims to answer the first two research questions: "What are the strengths and weaknesses of Finland's cyber security?" and "What are the threats and opportunities of NATO membership to Finland's cyber security? In addition to identification, different combination of strengths, weaknesses, opportunities, and threats are recognized. These combinations aim to answer to answer the last two research questions: "How to avoid the threats produced by NATO membership?" and "How to benefit the most from NATO membership?".

In this research, four SWOT combinations are used to analyze the data. These combinations are: Opportunity-Strength (OS), Opportunity-Weakness (OW), Threat-Strength (TS) and Threat-Weakness (TW) (Community Tool Box, 2023). These combinations are presented in Figure 11. Through these combinations it is possible to turn negative effects into positives, for example an opportunity that the NATO membership provides may tackle a weakness that

Finland has. OS and TS combination are especially in the focus of interest as they are directly linked to the research questions.

OS is a combination where Finland has strength in one or several of the themes (within strengths and weaknesses themes). This strength can be further used by taking advantage of it to benefit from an opportunity provided by the NATO membership.

OW combines positive (opportunity) and negative (weakness) effects together to overcome the negative. An opportunity that the membership provides may be the solution for a weakness that Finland has in cyber security.

TS combination aims to a situation where Finland’s strength in cyber security can be used to avoid threats coming from NATO membership. Through this combination, some of the possible negative effects may be tackled by already existing strengths.

TW is a combination that includes two negatives: threats and weaknesses. This combination requires strategies where both negatives could be eliminated by the same actions. Chapters 5.2 and 5.3 present whether OS, OW, TS and TW combinations are found and what are they.

	Strengths	**Weaknesses**
Opportunities	**Opportunity-Strength (OS)** - How Finland´s strengths can be used to get the most out the opportunities provided by NATO membership?	**Opportunity-Weaknesses (OW)** - How Finland can overcome it´s weaknesses thorough the opportunities provided by NATO?
Threats	**Threat-Strength (TS)** - How Finland´s strengths can be used to avoid threats produced by NATO membership?	**Threat-Weakness (TW)** - How can Finland´s weaknesses be minimized and threats avoided?

Figure 11 SWOT combinations

5 Analysis & results

The first part of this chapter presents Finland’s strengths and weaknesses in cyber security. The strengths and weaknesses are evaluated in five themes which are: cyber security management, cyber se security preparedness, cyber security skills, legislation, and situation picture.

The analysis is based on the expert interviews and the conducted literature review. Most of the themes included both strengths and weaknesses. Within each theme, it is evaluated overall whether the theme is a strength or a weakness.

The second part of this chapter presents the opportunities and threats that arise from the membership to Finland's cyber security. The opportunities and threats are evaluated in seven themes which are: cyberspace, cyber warfare, education & training, indirect threats, intelligence, new collaboration partners, and new technologies.

The analysis is based on the expert interviews and the conducted literature review. Most of the themes included both opportunities and threats. Within each theme, it is evaluated overall whether the theme is an opportunity or a threat. The final part of the chapter summarizes the results of the first and second part.

5.1 Cyber security management

Cyber security management in Finland divided the opinions of the interviewees. Entities that were seen as strength by some were seen as a weakness by others. Clear strengths and weaknesses were also identified within the theme. A summary of the strengths and weaknesses is presented in Table 1.

Clear leadership roles and responsibilities are identified as a strength by multiple interviewees (I2, 2023), (I6, 2022), (I9, 2022). Especially strategic cyber security management and responsibilities within are mentioned as a strength (I4, 2023). Contrarily, leadership roles and responsibilities on tactical and- operational levels are criticized. According to I2 (2023), there is a lack in middle-management and the existing procedures are too official. I4 (2023) agreed, that there is no structure for cyber security management on the middle level. Thus, strategic cyber security becomes more difficult as there is no sufficient tactical cyber security management (I4, 2023). I6 (2022) argued that leadership is the poorest on the practical (operational) level. They also thought that adjustment is a weakness because all administrative areas have different ways of managing cyber security (I6, 2022). The opinions of the interviewees correlate with the theory base of cyber security management, which indicated that operational and tactical cyber security management are not as widely covered topics as strategic cyber security management.

The leadership roles and responsibilities are also seen as weaknesses. The roles are seen as unclear, especially from the point of view of the public, regular citizens as well as on ministry level (I2, 2023), (I5, 2023). I2 (2023) pointed out that obscurity is a weakness on ministry level but otherwise, it can be seen more as a protection method. They stated that not all information is relevant and necessary to the public and especially to the adversary, who would receive the same information. (I2, 2023) The weakness within unclear responsibilities may therefore be more based on information sharing than the actual roles. I6 (2022)raised that the unclear roles and responsibilities can also be seen as a strength as it is then more difficult for the adversary to predict the actions of cyber security management.

The diffusion of cyber security management roles to various parties (such as Foreign Ministry, Ministry of Interior, Finnish Defence Forces, and prime minister's office) is seen as a weakness by an interviewee. They also raised a question on who is responsible for the cohesion of decisions related to NATO (I1, 2023). I7 (2023) argued that no one is leading cyber security and especially cyber defence. In order to have functioning cyber security management, civilian and military sides should integrate their processes and work together. (I7, 2023)

I5 (2023) thought that it would be good if there was only one leader for cyber security management. The National cyber security center could take the role and other organizations would support it by sharing information and giving consultation. I5 (2023) suggested that the responsibilities stated in the security strategy for society should be applied more in cyber security management.

The legislation should clearly state the roles and responsibilities (I5, 2023). In addition, to incomplete legislation, too strict legislation may also create problems. I6 (2022) stated that one of Russia's techniques is to operate on the edge of the responsibility areas which creates challenges for leadership as well as to legislation.

Information sharing and cooperation between officials were seen as a strength for cyber security management (I2, 2023), (I3, 2023). Information is shared with relevant parties, and they can use it in their own cyber security management (I2, 2023). Trust is on a good level which facilitates the information sharing (I3, 2023). Current legislation is sometimes an obstacle to functioning information sharing. It creates restrictions that limit the information sharing with all relevant parties. (I2, 2023), (I3, 2023). The obligation for pretrial investigation was mentioned as an example which might create restrictions (I3, 2023). Intelligence legislation was also mentioned as a possible creator of restrictions (I6, 2022).

The management of clear information security incidents that affects for example companies is seen as a strength in Finland. Information is shared and instructions are given. The National Cyber Security Centre has an important role in these cases. (I4, 2023) Management of incidents related to preparedness was also seen to be on a good level (I6, 2022).

The management of more complex cyber security incidents, where possibly a state actor is involved, is seen more as a weakness or at least a grey area. This would mean for example incidents that have significant effects on multiple organizations. I4 (2023) pointed out that Article 5 requires a lot of leadership. Finland should know when to activate it and when to take part in cases where other member countries activate the Article. They thought that currently there is no one to give recommendations related to this theme. (I4, 2023). I3 (2023) agreed that Finland should define the use of the Article. NATO podcast created by CINE-A also highlights that Finland should proactively define what cyber defence in Finland means and how Article 5 is used (CINE-A, 2022). These weaknesses could be managed by cooperation and by proactively planning the cyber defence actions of Finland (I4, 2023).

Overall, the management of cyber security was seen as more reactive than proactive. Reactiveness can be seen as strength as it is then more difficult for the adversary to predict it, but mainly it was seen as a weakness. Strength within the theme is that cyber security management in Finland often goes quickly from planning to leading and implementation. The weakness is that the implementation takes time, as there hasn’t been enough planning and proactive measures. According to I6 (2022), Sweden has different and seemingly working model where they use more time for planning and act proactively. To manage these weaknesses, the management model in Finland should become more proactive.

From military side, Finnish leadership structure and cyber security skills are seen as a strength in cyber security management. Finland’s national defence skills were highlighted. The final listed weakness was so called “Finnish perfectionism”. Finland aims to be a role model, but the NATO structure is too heavy for perfectionism. (I9, 2022) According to I9 (2022), the culture should be changed to more allowing and various scenarios should be practiced, to learn that sometimes mistakes happen.

Many of the interviewees were uncertain whether the theme would overall be strength or a weakness. Opinions to both sides were raised. Some thought that the theme is currently a weakness but in the long-term there is opportunities to become a strength. One of the significant suggestions to manage the weaknesses is cooperation and information sharing. Through these means of control, the theme could change into strength. However, based on the overall evaluation of the interviews, the theme is at the moment a weakness.

Strengths	Weaknesses
• Cyber security management does not rely on one person • Information sharing & cooperation • Clear leadership roles • “Simple case management” • Strategic cyber security management • Fast implementation • Cyber defence management	• Legislation restrictions • Tactical and operational cyber security management • Uncertainty about leadership roles& lack of information • “Difficult case management” • Responsibilities are too divided • Reactive instead of proactive • Finnish perfectionism

Table 1 Cyber security management strengths and weaknesses

5.2 Cyber situation picture

Situation picture gathering is highly mature in Finland (I1, 2023), (I3, 2023), (I8, 2022) and is considered a strength (I3, 2023), (I5, 2023) , (I8, 2022). Its continuity is ensured with budgeting of resources at national level. (I1, 2023). Since the operation has been active for numerous years, there has been a growing number of participating members (I5, 2023). Cooperation between officials and between officials and companies is considered to be active and effective (I2, 2023), (I3, 2023). Since the operation of cyber security situation picture gathering is mature in Finland, there is a large network of organizations working together (I4, 2023). National Cyber Security Centre is essential facilitator of the cooperation by providing essential cyber situation data to organizations and also with working groups which it facilitates (I2, 2023), (I7, 2023).

Reporting of situation data is active, and Finland has national tools which are used effectively (I1, 2023), (I4, 2023), (I8, 2022), (I9, 2022). One tool of situation data reporting and situation picture gathering is HAVARO. It is provided by the Ministry of Transport and Communications. HAVARO is designed to build national cyber security situation picture and is made especially for national officials and organizations working with critical infrastructure (Traficom, 2022a). HAVARO is considered to be beneficial tool for cyber situation picture gathering, even though the information gathered with it is not available to all (I6, 2022).

Situation picture frameworks are sometimes assembled ad hoc (I1, 2023), (I2, 2023), (I6, 2022). This means that situation data gathering, analysis and projection are done within an ad hoc organization that is formed when the situation presents itself. NATO is predicted to present situations that are rapidly changing and developing and need to be taken into monitoring quickly (I1, 2023). This is also seen as strength, since the framework is constantly changing and thus it is not possible for adversaries to figure out the exact framework for upcoming situations (I2, 2023). Ad hoc situation picture process is seen as a strength (I2, 2023), (I6, 2022).

Lack of shared situation picture system is seen as weakness (I1, 2023), (I3, 2023), (I4, 2023), (I6, 2022), (I7, 2023). Every party must create their own situation picture and share it with each other. This creates responsibilities to the parties to share their data, since other parties cannot access it directly through a shared system (I1, 2023), (I3, 2023). This also forms challenges in information sharing, since systems that are in use differ and may not be able to process the information that is wished to share with them (I6, 2022), (I7, 2023). Furthermore, without a shared situation picture system, there can be significant delays receiving documents from NATO, because of need to transfer data from one system to another (I3, 2023).

Specific roles of officials are seen as strength by many interviewees (I1, 2023), (I2, 2023), (I5, 2023), (I6, 2022). Roles and jurisdiction of officials come from Finnish legislation. Each official is an expert in their own role and can form very detailed situation picture from its perspective. Joint cyber situation picture can be enriched with each organizations own expertise and perspective (I2, 2023) (I6, 2022).

Roles can be sometimes overlapping in cyberspace, one situation can have attributes that concern law enforcement, military defence and intelligence at the same time. These can cause conflicts in situation data gathering and sharing (I4, 2023). Specific roles of officials can lead to a situation that deprives much needed co-operation in situation picture process if the parties choose not to share their information with each other and rather make their own situation picture with only their own situation data (I7, 2023). This leads to a situation, that in fact many different operational situation pictures of the same situation are formed and sometimes they are merged only when they reach the Finnish Government, which provides strategic management on the situation (I6, 2022). This is not optimal for building situation awareness and creates a weakness within situation picture theme. The weakness is the lack of combining different situation pictures and analyzing them cooperatively. Tactical management of the situation is sometimes skipped, and situation picture is presented directly from operational level to strategic level. Thus, even though specific roles are considered a strength, they need to work cooperatively by sharing their own situation picture and analyzing the situation picture together or they will not be a strength completely.

Government Situation Centre acts as a hub which gathers information from open sources and from government officials. National Cyber Security Centre as well as other organizations provide information about cyber security to the Situation Centre (I8, 2022). Its mission is to provide security situation picture for Finnish Government (I1, 2023). Even though gathering of the situation data is considered a strength, many interviewees see the lack of analysis of gathered information as a weakness (I4, 2023), (I5, 2023), (I6, 2022). More co-operation between officials and information sharing are needed to obtain even better situation picture and situation awareness.

Cyber situation data can be very technical and without proper analysis, it does not form a useful situation picture. Technical data needs to be combined with other data about the situation. When combined, they form even more specific situation picture. This means that one situation will have many different types of situation data and it is also possible that is has many types of situation pictures, i.e., strategic situation picture and technical situation picture (I2, 2023). Lack of collective situational cyber threat awareness within the EU is also noticed in the European Union's cyber security strategy. The challenge is the same: how to get the parties to systematically work together and share information with each other (European Commission, 2020). Need-to-share should be considered instead of need-to-know more frequently (I3, 2023), (I6, 2022), (I9, 2022).

Cyber situation picture is seen as a strength by majority of the interviewees (I1, 2023) (I3, 2023) (I4, 2023) (I7, 2023) (I8, 2022) (I9, 2022). However, there is hesitance within the answers (I1, 2023), (I7, 2023), (I9, 2022). Some see the situation data gathering and situation picture forming as a strength, but the situation awareness and situation analysis as a weakness (I4, 2023). The theme is also seen as a strength, because of untapped potential (I9, 2022). Some interviewees could not decide if the theme is a strength or a weakness, since it contains elements of both (I2, 2023). Other interviewees decided that the theme is weakness, since it is too focused on situation data gathering and lacks analysis of the gathered data (I5, 2023), (I6, 2022).

Ultimately, the theme is considered as a strength. Even though it has some weaknesses, the interviewees (I2, 2023), (I3, 2023), (I7, 2023) (I8, 2022) presented possibilities to develop these weaknesses, such as the report on authorities capacity to act in cyber security matters (Finnish Government, 2023). An organization similar to Government Situation Centre with experts from different organization is proposed (I6, 2022), (I7, 2023), (I9, 2022). Its focus would be to analyze the gathered situation data in tactical level, which requires experts from different organizations since the roles of officials are so specific. Opportunities can also be found from NATO membership and the new partners that it provides, which are discussed further in Chapter 6. One of the opportunities is the new information that is gained from new collaboration partners, which is not available to other than member nations (I5, 2023).

Strengths	**Weaknesses**
• Maturity of situation picture gathering activities • Active situation data reporting and beneficials tools and channels • Specific roles of officials • Ad-hoc situation processes	• Lack of situation picture analysis and situation awareness • Lack of shared situation picture system

Table 2 Cyber situation picture strengths and weaknesses

5.3 Cyber security preparedness

The maturity level of preparedness in Finland is on good level (I3, 2023), (I7, 2023), (I8, 2022), but the maturity of cyber security preparedness is lower (I3, 2023), (I8, 2022), (I9, 2022). The traditional preparedness model in Finland is very good and can be seen valuable from EU and NATO perspective. National Emergency Supply Agency is unique actor in Finland as well as globally. The know-how from traditional preparedness can be benefitted in improving the preparedness of cyber security. (I3, 2023) Historically Finland has maintained its preparedness level, while other countries in EU decreased preparedness actions because of thought on lasting peace (I8, 2022).

In cyberspace, disruptions are normal and malicious activities occur constantly. The difference is on the maturity level (customization) of the malicious activity or cyber-attack. Cyber hasn't been part of preparedness for long period of time, but phenomena's such as ransomwares have forced to consider preparedness in cyber security. At the moment, the utilization of cloud in cyber preparedness is considered. The cloud transformation in Ukraine is an example of fast and successful cloud transformation. To improve the preparedness level in cyber, there is a need for holistic discussion where costs and risks are balanced. (I8, 2022)

Cooperation is seen as strength within the theme, as well as a mean to manage the weaknesses. The functioning cooperation should be developed further to get the most out of it and manage the weaknesses. The cooperation should be conducted in both civilian and military domains. To improve the preparedness level in cyber, exercises and scenarios should be conducted in collaboration between officials such as state and- municipality actors and Finnish Defence Forces. Information should be shared more openly with the officials and there should be functioning and secure ways for it. (I9, 2022)

The level of (cyber) preparedness varies between organizations and officials (I7, 2023), (I8, 2022). Preparedness level is on good level in many organizations, especially on civilian side.

They have good response teams and Finland has practiced good preparedness for long period of time. (I7, 2023) The weaknesses are comprised from lack of basic cyber security procedures, such as vulnerability management, backups, and patch management (I7, 2023), (I8, 2022). Due to ransomwares, the organizations have started to pay more attention to these procedures.

Larger organizations can put more resources on cyber security and preparedness, and they often have higher maturity in cyber preparedness. Small and medium sized organizations have less resources and the preparedness level within is often low. In public sector, the security culture between officials varies a lot as does the level of cyber security preparedness. (I8, 2022) The high level of preparedness skills of individuals was seen as strength that supports the national cyber security preparedness (I7, 2023).

Another weakness in cyber preparedness is the internationalization of organizations and the expanding supply chains. Therefore, cyber security preparedness actions may need to be expanded to also organizations outside Finland. International cooperation and the possible NATO membership is seen as a method for managing the weakness. Through the membership, there is an opportunity to receive more information from members of the alliance and their partners from private sector. (I7, 2023)

The actions caused by insufficient risk management is seen as a weakness in this theme. The organizations don’t have complete picture of their technology situation, which results in low level of preparedness. Risks coming from new technologies are not considered or vice versa the problems in old technologies are not identified or act upon. Conducting changes is not based on change management (process) which creates problems also for preparedness. This may lead to too rapid changes where information security is not considered. (I8, 2022)

To respond to the increasing threats preparedness should be considered proactively, by mitigating the risks, instead of only reacting. To mitigate the risks and to improve the level of preparedness, better cyber threat intelligence is needed. The high level of classification creates problems in sharing the threat intelligence. (I7, 2023) Another problem is that the information sharing is reactive, which disadvantages the preparedness for cyber incidents (Finnish Government, 2023, p. 33).

I3 (2023) pointed out that NATO membership will increase the cyber threat level in Finland. NATO has mainly considered threats coming from countries such as Russia, China, Iran and North-Korea, but also other countries like India and Latin America should be considered. Both state and non-state actors should be considered. Cyber terrorism is one possible threat from non-state actors. Due to the membership Finland may also become a part of an attack that is targeted at NATO. Article 3 covers the preparedness and obligates the members to consider the seven baseline requirements for resilience. Through the baseline requirements the threats may be mitigated but it is questionable whether it is enough. (I3, 2023)

The opinions on whether the theme is a strength or weakness varied between the interviewees and there is no clear distinction on either side. The preparedness level in Finland is considered to be good (I3, 2023), (I7, 2023), (I8, 2022), but the maturity of cyber security preparedness is low (I3, 2023), (I8, 2022), (I9, 2022) . One of the interviewees considered the theme as strength (I3, 2023) and another one hoped it to be (I8, 2022). Third interviewee saw it as a weakness at the moment, but they thought that through the membership it might become a strength (I9, 2022). Ultimately the theme is considered as strength based on the strong baseline of preparedness.

Strengths	**Weaknesses**
• Long traditions in preparedness • Preparedness level in organizations • Preparedness level in civil society • Preparedness skills of individuals • Cooperation	• Low maturity in cyber security preparedness • Preparedness in small and medium sized organizations • Basic cyber security measures such as vulnerability management • Supply chain management • Insufficient risk management

Table 3 Preparedness strengths and weaknesses

5.4 Cyber security skills

The identified strengths and weaknesses of cyber security skills in Finland are presented in Table 4. Good education system and high level of civilization were highlighted in the interviews as few of the most significant strengths. (I1, 2023), (I8, 2022), (I10, 2022) Part of the good education system is that there are multiple actors providing cyber security training (I8, 2022), (I10, 2022). JAMK, XAMK, Laurea, Aalto University and Tampere University are few of the examples on actors providing cyber security training in bachelor's and master's degree level. Cyber security training is also partly embedded in general education program in primary school and high school, but it is not comprehensively covered. (University of Jyväskylä, 2022a, pp. 20, 36, 58-60, 77)

In addition to cyber security education provided by the schooling system, third parties arrange education and training on cyber security. One of the examples is training provided by the Finnish Defence forces as part of the military service. (I1, 2023) Already prior to the NATO membership Finland has been actively attending and participating international courses and trainings on cyber security. Professionals have had the opportunities to study abroad. These possibilities have increased the level of proficiency of the cyber security professionals in Finland (I5, 2023).

Despite the good education system and multiple actors, it was criticized that the provided training is on too general level. Due to this lack of specific training for example for industries, there is a need for different cyber security education program (I10, 2022). Another criticism for the education system was that it doesn't keep up with the changes in the field of cyber security (I1, 2023). This may also explain the gap in the provided education and the needs of work life.

A significant strength for Finland is that is has identified the importance of education and training. Cyber security education and training has been part of Finland's all cyber security strategies (2013, 2017, 2019). In 2019, the development of cyber security competence was lifted as one of the strategic guidelines in the strategy (I1, 2023), (The Security Committee, 2019).

One of the most significant weaknesses based on the interviews is the lack of professionals. The level of proficiency of the existing professionals was seen as good or even excellent, but the amount of these professionals is not nearly enough. (I1, 2023), (I5, 2023), (I8, 2022), (I10, 2022). The lack of professionals has been identified as a problem in Finland as well as globally. Studies regarding the lack of professionals are presented in chapter 2.2.2 Cyber security skills.

Better use of reserve is mentioned as a way to manage the weakness resulting from the lack of professionals. Part of these reservists use their competence at work and the other part at free time. The competence of the reservists provide a possibility to benefit from already existing skills also for national cyber security. (I)

Cyber security skills of the citizens were seen as slight weakness within the theme (I1, 2023), (I5, 2023). Cyber security training is on some level embedded to the education system in Finland, but it was argued that at the current state it is not enough. In addition to the education, citizens are provided with lot of materials regarding cyber security. (I8). Despite the opportunities to attend cyber security education and read the materials, cyber security may seem as too distant and difficult theme for regular citizens. The basic nature of Finns was mentioned as possible weak spot. Finnish people are seen as honest and trusting which may result in being fooled by i.e., phishing email (I10, 2022).

The lack of suitable cyber security training and rapidly evolving technologies are part of the weakness in cyber security skills. Not enough training and education is provided for the citizens which results in poor cyber competence. Due to the lack of training, there isn't always competence to act securely on the internet. Rapidly evolving technologies aggravate this problem. Technologies are growingly more difficult to use, and thus secure use of the technologies becomes harder. Cyber security built in technologies could be a way to manage the weaknesses within cyber security skills. Built in cyber security would decrease the responsibility of the user.

The rapidly evolving and changing technologies provide a challenge not only for citizens but also for organizations. There might not be certainty of the security level of the new technology but contrarily the old technologies often become less secure by the age. The lack of professionals makes the problem worse as there may not be enough competence to look after the old or new technologies. Cyber security should be considered from the beginning of the planning of the new technologies (I8, 2022).

The education system was seen as one of the means to manage the weaknesses. Good and comprehensive cyber security education would respond to lack of professionals as well as help to improve the cyber security skills of citizens (I8, 2022), (I10, 2022). The development of cyber security education received extra funding at the end of 2022 (Finnish Government, 2022d). The development of cyber security training is also presented in chapter 2.2.2 Cyber security skills. The development should take into consideration the education needs for organizations, citizens as well as for the nation.

Despite the mentioned weaknesses, cyber security skills in Finland were seen overall as a strength. The high-level skills of the professionals and the level of cyber security training were seen as the most significant and beneficial factors. The lack of resources was seen as the main weakness.

Strengths	**Weaknesses**
• Good education system • Multiple actors in cyber security education • High level professionals • High level of civilization • Training provided by third parties (i.e., military) • Cyber security strategy • Attending international courses and exercises	• Lack of professionals • Education doesn’t keep up with the changes and is too general • Human nature • Cyber skills of citizens • Finnish nature (honest & trusting)

Table 4 Cyber security skills strengths and weaknesses

5.5 Legislation

Finland has long tradition in information security legislation (I1, 2023), (I8, 2022). Cyber is included in various acts in Finland, some of which are briefly presented in chapter 2.4.5. The amount of legislation in Finland is considered to be comprehensive and it is seen as a strength by the interviewees (I1, 2023), (I7, 2023), (I8, 2022), (I10, 2022). Finland has updated Police Act and Act on Military Intelligence recently, which is seen as a positive trend and is hoped to continue in other legislation regarding cyber (I1, 2023), (I7, 2023). Act on Electronic Communications Services was seen as useful and highly relevant legislation (I8, 2022).

Finnish mentality of following law rigorously is seen as a strength (I1, 2023). Even though the legislation might be very difficult to follow, it is seen as impossible to not follow it (I2, 2023). The role of authorities would be to raise their concern on the state of legislation and to point out the weak spots in it (I2, 2023).

In addition to legislation, Finland has useful guidelines and tools regarding cyber security (I1, 2023), (I10, 2022). Katakri is considered to be relatively useful tool and officials have reached an understanding on how to interpret it (I1, 2023), (I10, 2022). Since its nature as an information security assessment tool, it allows a possibility for officials to implement it in different ways, which helps to reach understanding between officials. This differs from interpretation of legislation, since it has the principle that every party should interpret it in same way. Ultimately, the right interpretation is made by judges in different court instances. Katakri is based on Finnish legislation and is seen as a tool which clarifies some legislative requirements (I1, 2023), (I10, 2022). Katakri was recently updated with an appendix, which contains requirements regarding NATO information security (I10, 2022).

Interpretation of legislation is under debate of officials in some cases (I1, 2023), (I7, 2023). This leads to situations where it is not possible to transfer, share or handle classified data together, since the parties cannot reach an understanding what requirements should be followed. It is noted that not all requirements are mandatory to follow under Finnish legislation, some are purposely left as recommendations or good practices that organizations and officials can choose to follow if they see it suitable (I1, 2023). Application and interpretation of same legislation vary between authorities, which was seen as a weakness (I1, 2023), (I7, 2023).

Finnish legislation is in some cases regarded as too detailed (I2, 2023). Furthermore, the number of different laws regarding cyber is seen as a burden (I3, 2023). Even though the intention might be appropriate, this kind of legislation leads to situations where it can’t properly accomplish its purpose. Legislation is struggling to keep up with constantly evolving technology. It is seen to be very challenging in combination with highly detailed legislation regarding technology (I2, 2023). Interviewees had mixed opinions on whether there should be more cyber legislation or if there is too much of it. In some cases, such as preserving national safety, and cyber defense, the legislation was observed to be missing (I3, 2023), (I7, 2023), (I9, 2022). The consensus, however, was that the current state is not working, and reformation is needed (I2, 2023), (I3, 2023), (I7, 2023), (I9, 2022).

Some interviewees consider cyber legislation in Finland as a strength due to its comprehensiveness (I1, 2023), (I10, 2022). Even though the legislation is considered as a strength, it is observed that legislation only obligates authorities to protect their data, which leaves private sector with possibly vulnerable masses of data (I10, 2022). However, majority of the interviewees see this topic as a weakness (I2, 2023), (I7, 2023), (I9, 2022). Even though the topic is seen as a weakness, some positive predictions about the state of cyber legislation are also formed (I7, 2023). Report published by the Finnish Government (2023), is seen to possibly clarify the interpretation of cyber legislation and to help authorities to act in cyber security matters (I2, 2023), (I3, 2023), (I7, 2023), (I8, 2022).

Strengths	**Weaknesses**
• Legislation is comprehensive • Shared guidelines and tools regarding cyber security • Legislation is followed rigorously	• Interpretation of law is different between officials • Legislation is too detailed and cannot keep up with technology

Table 5 Legislation strengths and weaknesses

5.6 Cyberspace

The threats that the Alliance is facing are global. Malicious activities in cyberspace and disinformation campaigns are highlighted in the strategic environment of the Alliance. The Russian federation and the People’s Republic of China’s (PRC) have been identified by the Alliance as actors that pose threat to the peace and security of the Alliance. Cyber operations and disinformation are mentioned as means to reach these targets. The operations may be conducted directly or through proxies. (NATO, 2022h, pp. 3-5)

The most significant opportunities in cyberspace derive from collective defence (I1, 2023) (I5, 2023), (I6, 2022), (I7, 2023) and information sharing (I6, 2022) (I7, 2023), (I8, 2022). The membership enables the protection of cyberspace in cooperation instead of by Finland alone. The means of collective defence include for example information sharing, supportive actions and creating an impact in adversary’s cyberspace. (I6) Through the membership the attribution of attacks may become easier (I1, 2023). Attribution means identification of the perpetrator and if necessary, holding them accountable for the act (The Security Committee, 2017b, p. 27).

The collective defence and membership means new collaboration partners and extending cooperation with existing partners in NATO. The cooperation is done in collaboration with civilian and military sector. To benefit the most from this opportunity, Finland should be an active actor and decide significant points of focus and important partnerships. Finland has high proficiency of its own, for example in technology, and can also provide new capabilities to NATO. (I7, 2023).

According to I6, the most significant opportunity is that Finland obtains better situation picture on what is happening in cyberspace. This relates to information sharing and profounding cooperation. The opportunities exist in technical, political, and strategical level. The information sharing creates opportunities especially for security authorities, who can collect and share information as well as exchange it to threat intelligence of other member states. (I6, 2022).

I7 (2023) and I8 (2022) agreed that the membership provides an opportunity for expanding information sharing. I7 (2023) highlighted the intelligence information and NATO's intelligence analysis that Finland will receive. NATO's Cyber Operations Centre is used for sharing cyber security information related to military side. (I7, 2023). The membership provides opportunities for receiving information from many new public and private sources. The expanding information sharing enhances the creation of situation picture on critical infrastructure. The compatibility of the systems may create challenges for benefitting from this opportunity. (I8, 2022)

In addition to expanding information sharing the membership can provide further opportunities for businesses in Finland. Industries and universities get the opportunity to join the research hubs and receive funding from there. Finland has successful companies, and the membership can enhance their further development and thus strengthen the capabilities of Finland. (I4, 2023)

The negative impact or threats from collective defence and the use of Article 5 derive from growing hostile activities and expanding attack surface. Through the membership, Finland becomes an adversary country to parties that oppose NATO. (I1, 2023), (I3, 2023), (I7, 2023), (I8, 2022). Therefore, it is likely that state and non-state actors will direct more hostile activities in cyberspace towards Finland (I3, 2023), (I8, 2022).

State actors include for example Russia, who may justify its hostile actions and their legitimacy through the threat that it encounters from NATO member states (Finland) (I1, 2023). To manage the threat Finland should have 5–10-year plan for cyber security. In practice the execution of the plan may be difficult. The plan should consider what Finland doesn't want to happen in cyberspace. (I3, 2023). The expanding attack surface includes not only other member countries but also their supply chains (I7, 2023).

Non-state actors include for example activists and cyber criminals who oppose NATO. Finland may become a target of their actions through the membership. (I8, 2022). Non-state actors may work on their own or they can have state actor behind them making the orders (I6, 2022). Hacking-as-a-service (buying cyber capabilities and malicious attacks online) is easy nowadays and creates significant threat (I3, 2023). Drawing the line between state and non-state actor is often not straightforward and making an attribution is difficult (I8, 2022).

I8 (2022) argues, that Finland is already a target of cyberattacks and the membership doesn't create fundamental change. Finland may become a target when NATO drifts into a conflict in geographically distant location, but this has already happened prior the membership for example in Afghanistan and Africa. As a member the growing hostile activities are targeted to whole Alliance and not merely Finland. The information sharing, wider threat intelligence and collective defence can be seen as an opportunity in this theme. (I8, 2022). After Finland decided to apply for membership in spring 2022 YLE published news regarding the number of cyber-attacks toward Finland. It stated that the application for membership hadn't significantly increased the number of cyber-attacks. (YLE, 2022b).

Article 5 is the baseline for the Alliance's collective defence and provides security guarantees for Finland. The reverse side of the Article is that Finland is obligated to respond to the activation of the Article in other member countries and may therefore become part of cyber warfare. The willingness to activate the Article and the possible counter actions may also be tested by the adversaries. (I6, 2022) Forsberg, et al. (2022) state that the Russo-Ukrainian war and the increasing cyber-attacks have increased the need for firm security guarantees that can be utilized in hybrid-and cyber warfare. However, it is argued that such attacks may not cross the threshold of activating the Article 5. (Forsberg, et al., 2022, p. 40)

The strategic culture for battling against the malicious activities in cyberspace varies between the member states, but many of the members have means and practices from which Finland can benefit a lot as a member. (I6, 2022)

Rapid development and unpredictability of cyberspace were raised as possible threats. The effects of attack in cyberspace may be directed to Finland even when the aim is somewhere else. (I4, 2023) . The significance of cyberspace has been recognized globally and NATO has addressed the fact in Strategy Concept 2022. Society's in present day are highly connected and dependent on electronic systems. Thus, malign actors aim to create in an impact also in cyberspace. Critical infrastructure, government services, intelligence, intellectual property, and military activities are likely targets of the cyber operations. (NATO, 2022h, p. 5) The importance of cyberspace exists with or without NATO and it is unclear what the effects thorough the membership are. Even within NATO it is still unclear what cyberspace is. To respond to the growing threat in cyberspace Finland should invest in research and development of cyber security. (I4, 2023)

Finnish cyber security professionals leaving for NATO positions was identified as minor threat. The lack of cyber security professionals in Finland is identified as weakness in chapter 5.2.3 and therefore the professionals leaving to other duties may aggravate the problem. This was not seen as a significant threat, but it may create some problems if for example a key person leaves. The positions in EU create more significant risk than the ones in NATO. (I6, 2022)

Part of Finland's cyber security capabilities may need to be engaged in giving help for other member countries for example in case of using Article 5. Finland hasn't been part of Eu's Cyber Rapid Response Teams but NATO will most likely obligate in doing so. With or without NATO, Finland needs more cyber security professionals. How cyber defence is built is seen as more important factor than focusing on professionals possibly needed in NATO tasks. (I6, 2022).

Half of the interviewees considered the theme as a threat (I3, 2023), (I4, 2023), (I6, 2022) and another half (I1, 2023), (I7, 2023), (I8, 2022) saw it as an opportunity. Some of the interviewees more uncertain about their opinion while others were certain of theirs. Cyberspace changes whether Finland is part of NATO or not. The effects in cyberspace when joining NATO are difficult to predict. Most likely the number of cyber activities increases but on the other hand Finland will have more capabilities to counter them. Overall, the theme is a threat.

Opportunities	**Threats**
• Collective defence • Business opportunities • Information sharing • Lessons learned	• Growing hostile activities - State actors - Non-state actors • Unpredictability • Cyber warfare • Professionals leaving for NATO

Table 6 Cyberspace opportunities and threats

5.7 Cyber warfare

Joining NATO is seen as a possible catalyst for evolution of cyber warfare in Finland (I4, 2023), (I6, 2022), (I7, 2023). Especially offensive cyber capabilities as a form of self-defense is still new concept to Finland (I4, 2023). This type of thinking is familiar to NATO, and

Finland can learn much from it (I6, 2022). Since NATO has recognized cyberspace as a domain of operations, it is also logical that every member nation needs to be able to defend their cyberspace, which can mean self-defensive cyber-attacks. This requirement is consistent with NATO's Article 3, which is related to resilience. Furthermore, since cyber is recognized as a domain of operations, allies can contribute their capabilities in cyber, as well as in land, sea, or air domains (Loverdos, 2022). Cyber-attack supporting the defense of an allied nation can have similar effects as providing a tank or a plane for its defense.

NATO's Cyber Operations Centre will provide allies with situational awareness for cyberspace operations, but its operation is designed for defence. NATO personnel will not execute cyber-attacks themselves, instead the allies have created an instrument which is described as sovereign cyberspace effects from allies who are capable and willing to provide them (Loverdos, 2022). This instrument is formally recognized as "Sovereign Cyber Effects Provided Voluntarily by Allies" (SCEPVA) (CCDCOE, 2022b), and it is used for offensive cyber activities i.e., cyber-attacks. Use of this mechanism needs the approval of North Atlantic Council, which means the invocation of NATO's Article 4 and most likely Article 5. NATO has not disclosed publicly what cyber threats are considered major enough to mandate the use of SCEPVA capabilities (CCDCOE, 2022b). Nevertheless, joining the group of likeminded allies in SCEPVA activities is seen as a major opportunity for Finland which could evolve its defensive and offensive cyber warfare capabilities (I4, 2023), (I7, 2023). Currently, SCEPVA includes nations such as the United States, the United Kingdom, the Netherlands, Estonia, and Denmark (Loverdos, 2022).

SCEPVA is also linked to another opportunity that is recognized by the interviewed experts. NATO membership presents Finland an opportunity to get new information for cyber-attack and operations (I4, 2023), (I7, 2023). This information cannot be obtained from anywhere else than NATO, as a NATO member (I9, 2022). The quantity of information gained is also increased dramatically (I9, 2022). However, this requires national management of information gained from NATO, which is discussed in chapter 5.2.1.

Importance and intensity of cyber warfare will grow against Finland, which is seen as an threat (I6, 2022), (I7, 2023). However, Finland is already under continuous aggression in cyberspace and no new adversaries as a result of NATO membership are identified (I7, 2023). It is possible that Finland will face advanced attacks that is has not faced before NATO membership (I9, 2022). Not a single NATO nation has declared to be under attack in a military sense as an result of cyber-attack, even though there have been attacks against them (I6, 2022). North Macedonia suffered a hybrid attack which included bomb threats and cyber-attacks in 2023. NATO responded by sending help in form of information, team of experts and technical support (NATO, 2023g). Albania suffered a cyber-attack in 2022 which was attributed to Iran. This also prompted response from NATO (NATO, 2022o). These attacks did not invoke Article 4 or 5, and it remains to be seen when they will be invoked as a result of cyber-attack. Nevertheless, Finland needs to be prepared for increased pressure in cyberspace.

Theoretically, Finland loses a part of its autonomy as part of NATO. Politics regarding security incidents will change and NATO will require Finland to form declarations about current situations (I4, 2023), (I6, 2022). Even though Finland is known to be impartial in many situations, NATO will force it to choose sides and Finland needs to show concrete actions in support of its declarations (I6, 2022). Concrete actions are an indicator of capabilities in cyberspace, which adversaries like Russia and China respect more than declarations (I6, 2022).

NATO forces Finland to think strategically and to make its position known globally for example in matters regarding cyber warfare (I4, 2023), (I6, 2022). Since Finland has been in an impartial role for such a long time, this change of dynamics in its global role and politics can be seen as a threat (I4, 2023). One recognized risk is that Finland cannot ascend to the role of serious NATO member and remains impartial in cyberwarfare (I4, 2023). This would mean that the opportunities of gaining new information and evolving cyber warfare capabilities through groups such as SCEPVA are mitigated. Ascending to a serious cyber warfare nation requires demonstrating cyber warfare capability and determinacy in developing it (I4, 2023).

All of the experts interviewed see this topic as an opportunity (I4, 2023), (I6, 2022), (I7, 2023), (I9, 2022). Finland’s cyberwarfare capabilities will evolve as a part of NATO alliance, and for some parts, they are demanded to do so. It is possible that during the harmonization of NATO requirements there is a moment that will seem as negative effect, but after the harmonization is complete, Finland will gain positive effects and becomes even stronger in cyber warfare (I9, 2022).

Opportunities	**Threats**
• Evolution of cyber warfare in Finland • New information on cyber-attacks and operations	• Increased pressure and intelligence towards Finland and NATO • Finland is not recognized as an important NATO member in cyber warfare

Table 7 Cyber warfare opportunities and threats

5.8 Education and capabilities

Based on the interviews, NATO membership provides significantly more opportunities than threats within this theme. The identified opportunities and threats are presented in Table 8. All the interviewees who answered to the education and capability's theme emphasized the new education and training opportunities. Already prior to the membership Finland has been participating in courses, trainings and exercises provided by NATO.

The close partnership of Finland and NATO began in 1994 when Finland joined the Partnership for Peace (PfP) programme. For Finland, PfP meant bilateral cooperation with NATO. One of the key areas of cooperation within the programme was cyber defence. Finland for example participated in NATO cyber defence exercises and cyber related projects. An arrangement for cooperation on cyber defence was made in 2017. (NATO, 2023f) In addition to PfP programme, Finland and NATO have had information security agreement for approximately ten years, so the membership might not bring so many changes to education and capabilities, according to interviewee (I1, 2023).

Through the close cooperation with NATO, Finland has had the possibility to participate the courses provided by NATO, but through the membership NATO education system becomes more available (I1, 2023), (I5, 2023), (I8, 2022). In addition, to the education opportunities provided by NATO, the membership will also enable Finland to participate more in education and trainings arranged by other member countries (I10, 2022). For officers, NATO provides new career opportunities (I1, 2023).

Not only education and training but also NATO exercises were highlighted as possible opportunity (I10, 2022). The trainings and exercises provided by NATO are elaborated in chapter 2.4.9 Education and capabilities. One of the identified threats was linked to trainings arranged by Finland to NATO members. It was stated that there is a possibility that too much information about the capabilities of Finland is shared in the trainings which may result in information leak. The threat was not seen as high importance. (I5, 2023) The threats related to new collaboration partners are described in chapter 5.3.6 New collaboration partners.

The increasement in cooperation was seen as an opportunity for the development of education and capabilities in Finland (I5, 2023). NATO's centres of excellence (COEs) were mentioned as an opportunity for new trainings and support in training arrangements. Especially the expanding cooperation with CCDCOE was highlighted. (I10, 2022)

An obstacle for benefitting from the opportunities is the lack of resources in Finland. The lack of cyber professionals in Finland was identified as a weakness in theme cyber security skills. Due to this weakness, there may not be possibility to send professionals to some of the trainings and education provided. The lack of professionals also creates a possible threat. As

NATO provides new vacancies for cyber security professionals, there is a possibility that some of the professionals in Finland leave for NATO vacancies or countries. (I5, 2023)

NATO's cyber capabilities were seen to be on good level. The war in Ukraine was mentioned as an example of demonstration of the cyber capabilities of the Alliance. Multiple NATO countries have supported Ukraine in cyber activities during the Russo-Ukrainian war. Russia hasn't been able to create significant cyber effects which also represents the cyber capabilities of the Alliance. Therefore, according to an interviewee, the theme can be seen as a clear opportunity for Finland. (I10, 2022)

New cyber capabilities may be created through different pools/groups within the Alliance (I1, 2023). NATO has deployed advisory teams, to support the Allies on different topics. One of these team is counter-hybrid support team. The team can assist the Allies in a crisis or in developing its capacities. (NATO, 2021b) Overall, NATO is used as platform for sharing information on malicious cyber activities, best practices as well as consultation. (NATO, 2022e)

Finland's own proactivity and interests are in key role, when deciding which cyber activities (groups/pools/teams/bilateral cooperation etc.) would be the most beneficial for developing the national capabilities. Especially due to the lack of cyber security professionals, there is a need for prioritizing the resources.

In addition to receiving information from previously mentioned cooperation groups, the membership will overall increase the amount of information that Finland as a member receives. The information is received for example through situation picture. (I5, 2023)

One of the interviewees pondered that in this theme Finland would be more on receiving side (opportunities but not many threats) (I5, 2023). On the other hand, Finland's cyber capabilities have been recognized also internationally. Finland's capabilities have been mentioned as a possibility to improve the Alliance's cyber defence. The history of Finland and cyber talents have also been highlighted. Especially the talent and skills within technology and private sector have been recognized. (SIGNAL, 2023)

All of the interviewees that responded to the theme agreed that there are clearly more opportunities than threats within education and capabilities. Only few threats were identified, and these were not seen as significant threats for Finland. One of the limitations for benefitting from the opportunities is that the possibilities are mainly limited to the defence sector (I1, 2023).

Opportunities	Threats
• New education and training • NATO exercises • Collaboration and cooperation • Centres of excellence (COEs) • New capabilities through different pools/groups within the Alliance • More information i.e., thorough situation picture • New career opportunities for officers • NATO cyber capabilities	• Professionals leave for NATO vacancies or countries • Too much information sharing which may result to information leak

Table 8 Education and capabilities opportunities and threats

5.9 Indirect effects

No new opportunities from indirect effects of NATO membership were discovered. By thinking positively, opportunity to get knowledge from new indirect effects against Finland could be seen as an opportunity (I9, 2022).

Indirect effects from NATO membership could include political and economic influencing towards Finland and NATO. One interviewee noted that it is possible to influence cyberspace and cybersecurity by means that are outside of cyber (I7, 2023). Response to a cyber-attack could be for example economical or a political sanction. When Albania suffered a cyber-attack, which was attributed to Iran, it cut diplomatic ties with Iran. This marked the most powerful political response to cyber-attack to this date (The Iran Primer, 2022), (Lyngaas, 2022). Effects such as these could affect Finland’s cyber security as well after joining NATO. China and India have been monitoring the growing of NATO. These nations may present a threat to NATO and Finland in form of indirect influencing in future (I7, 2023).

Finland could be used as a part of supply-chain attack to attack NATO (I9, 2022). Even though this tactic against Finland would not be indirect effect, its consequences are. Finland could suffer reputation loss if it is seen as the weakest link which enabled the opportunity to attack NATO through its infrastructure, or network (I9, 2022). Russia has used unconventional operations in the Ukraine War, which have some resemblance to this topic. In the beginning of the war, Russia launched a cyber-attack against the company Viasat. This attack was successful, and it had effects to communications systems in Ukraine (Danylyuk, et al., 2023).

It is possible that the Finnish companies could suffer similar indirect effects of a malicious cyber-attack in the future.

Indirect effects is seen as a difficult topic to comment on and it gathered the least amount of responses. It was seen as a threat by all of the interviewees (I7, 2023), (I9, 2022). It is possible to find opportunities in this topic in the future (I9, 2022), however the analysis for the current situation presented only threats.

Opportunities	**Threats**
	• Political and economic influencing • Supply chain attack enabled by Finland

Table 9 Indirect effects opportunities and threats

5.10 Intelligence

Intelligence information sharing is seen as the greatest opportunity from the membership (I7, 2023), (I9, 2022). Members of the Alliance have various information collection methods which provide opportunities for receiving information that would have not been possible otherwise. Intelligence related to cyber doesn't only come from cyber intelligence and furthermore cyber intelligence can be used to get information from objects that could have not been obtained by other means. (I7, 2023). I9 (2022) highlighted that the membership enables Finland to receive information that it otherwise wouldn't. Due to the differences in legislation, some of the member states can collect information that Finland can't due to the restrictions in legislation. The membership enables the access to this information. (I9, 2022)

Prior to the membership, Finland has conducted multi-and bilateral cooperation with many of the NATO member countries. Especially after becoming observer member in 2022, Finland has been more involved in the intelligence community of the Alliance. Already prior the actual membership, the cooperation and information sharing has been rewarding. It remains to be seen what all the consequences from the membership are. (Supo, 2023b, p. 22). The opportunities from the membership are also described in the latest Finnish military intelligence review. Especially information sharing, and cooperation are highlighted as possible benefits. (The Finnish Defence Forces, 2023, p. 17).

In addition to information sharing, it is important to combine the intelligence information. Through the membership, Finland has an opportunity to have global influence through NATO and the USA. The influence can for example be on the intelligence questions and information collection plans (ICP's). Due to Finland's geopolitical location it is seen as a wanted partner by the Alliance. Therefore, the opinion of Finland is also listened to. (I7, 2023)

Difficulties in political and diplomatic practices may create obstacles for benefitting from these opportunities. Different committees, their roles, and responsibilities as well as their actions may also be obstacles for the opportunity. (I9, 2022)

The increase in intelligence actions conducted towards Finland is seen as the most significant threat in this theme (I7, 2023), (I9, 2022). NATO systems and information are identified as targets of APT actors and as result of membership this can lead to increased intelligence activity towards Finland as well (I9, 2022). NATO technologies and information can make Finland and companies within more interesting target for intelligence. However, decision making of Finland, remains as one of the priority targets of intelligence. (I2, 2023)

According to I7 (2023), the intelligence actions towards Finland will most likely increase and they are conducted through cyber or human- intelligence. Russia is seen as a possible party to conduct such intelligence activities (I7, 2023), (I9, 2022). Finland has had decent relations with Russia until 2014. There is a possibility that the actions towards Finland get rougher and the amount of intelligence increases due to the membership. (I7, 2023). Russia may use proxies to obtain information, which complicates the attribution. The use of third parties becomes more common in intelligence which increases the risk of escalation of the situation. (I9, 2022). I2 (2023) disagreed on the effects that the membership will have on intelligence activities. They considered that the membership doesn't change the intelligence methods conducted towards Finland.

The latest National security overview states that NATO membership makes Finland more interesting target for intelligence. Russia, China and other authoritarian countries are mentioned as possible threat actors. Cyber intelligence is specifically mentioned as a method that China utilizes along with human intelligence. So far, the reactions have been mild however. The membership has also increased the (cyber) intelligence threat towards critical infrastructure. (Supo, 2023c)

To combat the threat of increasing intelligence activities, the cooperation between officials needs to be improved. Finland should invest in centers where officials can work together and share information. In addition, more proactive information and improved cyber threat intelligence is needed to respond to the threats of intelligence. Jurisdictions may create challenges in implementing the improvements. (I7, 2023)

New partnerships are seen as an opportunity from the membership. Cyber threats are global phenomenon and partners are important in battling against the threats. NATO membership and the practices applied within the Alliance as well as the member countries can work as good benchmark for Finland. The benefits that come from the Alliance are greater than the threats in this theme. (I2, 2023)

The new opportunities also create workload for Finland. The information must be managed and analyzed. More human resources and automatization are required. (I7, 2023) The lack of cyber security professionals has been identified as a weakness in Finland and due to the new tasks that the opportunity creates there is a risk for even bigger lack of the professionals. This lack is seen as a possible threat in this theme (I2, 2023). The lack of resources itself may not be a threat but it is an obstacle for receiving all the possible benefits from the membership. Unmanaged data may escalate some threats if information is for example missed due to the lack of resources.

I7 (2023) thought that Finland has good competences for collection and analyzing intelligence information. Bilateral and multilateral cooperation has been conducted already for a long period of time before NATO. Still, they think, that the growing amount of information and the lack in resources may be an obstacle for benefitting most from the opportunities within this theme. (I7, 2023)

All three interviewees (I2, 2023), (I7, 2023), (I9, 2022) regarded the theme as an opportunity. I9 (2022) considered that the theme might be a threat in the beginning, but it will change into opportunity over time. They thought that the opportunities come mutually to Finland and NATO. Finland provides good information, and it can receive valuable information for example on attacks that are being targeted to Finland. (I9, 2022)

Opportunity	**Threat**
• Information sharing • New partnerships • Best practices • Global influence	• Increase in intelligence actions towards Finland • Lack of resources

Table 10 Intelligence opportunities and threats

5.11 New collaboration partners

Most notable opportunity that was seen by the interviewees was enhanced partnerships between Finland and other NATO nations (I4, 2023), (I5, 2023), (I9, 2022). While Finland has already been actively conducting cooperation with NATO nations before joining the alliance, NATO membership will provide Finland access to even more information and operations than before, since some information is strictly restricted for NATO allies only (I5, 2023), (I9, 2022). Cooperation between Finland and its allies will enhance as a result (I4, 2023), (I9, 2022).

Finland needs to choose which nations it will work with more intensively, since it does not have resources to maintain cooperation with each NATO nation individually (I4, 2023).

NATO-membership will provide Finland with partnerships with large corporations as well as other allied nations, which is seen as an opportunity (I2, 2023). One example is Microsoft, which has performed observation to its own systems during the Ukraine war. Microsoft has enormous amount of data at its disposal combined with high level of threat intelligence capability. Microsoft states that before the Russian troops invaded Ukraine on February 24, 2022, Russians had already started the attack in cyberspace. Using their cyberweapon “Foxblade”, Russians targeted Ukraine’s digital infrastructure, with intention to cause destructive effects (Smith, 2022). Microsoft has also detected cyber-attacks from Russia towards Finland in 2022 (Microsoft, 2022, p. 41). It has also stated that threat actor NOBELIUM, which is linked to Russia’s Foreign Intelligence Service (SVR) targeted NATO nations with supply chain attack tactics (p. 37).

Threat indirectly generated by gaining new NATO partners is regarding the limited resources in disposal of Finland (I2, 2023), (I4, 2023). Finland needs to divide its cyber recourses carefully to avoid overextending itself to too many cooperation forums or partnerships (I2, 2023), (I4, 2023). Even though opportunities and new information could be gained from many allies, Finland simply does not have capability and resources to work with each nation. By beginning a cooperation with a nation, without possibility to invest in it can be seen as disrespectful. In this case it could be better not to start bilateral cooperation in the first place. Some partnerships will also require more resources than other, this also signifies the importance of planning and correctly distributing the resources (I4, 2023). This also requires enhanced cooperation between officials in Finland, so that every organization recognizes their own area of responsibility (I2, 2023), (I5, 2023).

By joining NATO, Finland gains new allies and new cooperation forums. This also means that Finland needs to share information with larger group of recipients than before (I2, 2023), (I5, 2023). However, without sharing anything, Finland cannot gain any information either (I5, 2023). Threat that is generated from sharing more information comes from within NATO (I9, 2022), (I10, 2022). Possibility of an insider in NATO nation spying on Finland is realistic and there has been a case of NATO insider in Portugal. Portuguese secret service official was recruited by Russia and sold them classified information about NATO and European Union (Bugge, 2018), (Schindler, 2016). In this case the spying nation was not NATO nation Portugal, but Russia used Portuguese individual with means to access information. Another case that is similar to insider threat is United States spying on European politicians with assistance from Denmark. The U.S. National Security Agency (NSA) gained access to information cables and was able to spy on officials in Sweden, Norway, France, and Germany (Gronholt-Pedersen, 2021). Finland needs to prudently analyze which information it will share with others to gain most benefit and without risking too much if the information shared is lost (I5, 2023).

New partnerships are seen as an opportunity by all interviewees, which answered the categorization between opportunity and threat (I2, 2023), (I4, 2023), (I5, 2023), (I9, 2022). However, Finland needs to carefully plan where to distribute its cyber resources to fully benefit from the opportunity that is presented by gaining new partnerships (I2, 2023). Secondly, the analysis of information sharing is crucial (I5, 2023). Sharing all information with the alliance is not beneficial and is not conducted with other allied nations either (I9, 2022), (I10, 2022). This does not mean that Finland should abstain from sharing as much information as possible with its new partners. Rather it needs to verify that information is suitable and beneficial for sharing and it will gain something valuable in return.

Opportunities	**Threats**
• Enhanced partnerships • Big corporation partners	• NATO insider • Coordinating of limited resources

Table 11 New collaboration partners opportunities and threats

5.12 New technologies

Every interviewee saw new business opportunities as an opportunity that stems from NATO membership (I2, 2023), (I3, 2023), (I8, 2022). It is possible that the financial benefits are so substantial, that it could have effects on nation budget (I2, 2023). Finland has strong knowledge in ICT and defense technologies. Startups in Finland have also been regarded as an asset (I2, 2023). By joining NATO, Finland will become more influential and more desirable business partner in the technology field (I3, 2023), (I8, 2022). DIANA and NATO Innovation Fund were also seen as a great opportunity for businesses to gain investments to develop their products, especially in the field of emerging and disruptive technologies (I3, 2023).

Disruptive technologies such as autonomous systems or quantum-enabled technologies are in focus of NATO's innovation projects, described in chapter 2.4.13. These technologies were recognized by the interviewees as well and were seen as an opportunity for Finland (I2, 2023) (I3, 2023). Finland is currently regarded as a respected nation regarding some disruptive technologies, such as quantum (I3, 2023). Finland is also seen as an ally which will bring new cyber capabilities to NATO (Laje, 2023). Finnish has notable capabilities regarding new technologies already such as the most powerful supercomputer in Europe, called LUMI. LUMI is also the world's third most powerful supercomputer (TOP500, 2022). Since NATO already has a strong innovation framework and numerous projects regarding disruptive technologies, it is possible that Finland will benefit from NATO's knowledge regarding it (I2, 2023).

One opportunity that was seen to be created by joining NATO is possibility of gaining new technical capabilities as a NATO member nation (I3, 2023), (I8, 2022). Example of new capabilities that could be facilitated by NATO is the Niels Bohr Institute in Copenhagen, Denmark (Invest in Denmark, 2023), (I3, 2023). The institute is NATO's leading centre for knowledge about quantum technology and is also part of the DIANA program. New capabilities and knowledge from NATO such as the Niels Bohr Institute could also be possible for Finland as well. NATO will not disclose all its capabilities publicly (I8, 2022). Some of its capabilities come from allies who voluntarily provide them, and an argument could be made that these are not NATO's capabilities. This mechanism is regarded as SCEPVA. By being active in SCEPVA cooperation will provide opportunity to Finland for new technical capabilities.

New technologies can be used for malicious purposes as well. This was regarded as the most notable threat in new technologies (I3, 2023), (I8, 2022). Technologies such as machine learning, internet of things, artificial intelligence, robotics, biotechnology were pointed out to be a threat, if used maliciously against Finland (I3, 2023). These technologies make possible for them to be used collectively by combining two or more of these technologies, which makes the threat even greater.

NATO's adversaries such as Russia and China are both interested in new technologies and expertise regarding them (I2, 2023). Since NATO is predicted to generate new information about NATO technologies and new expertise to Finland, this creates a threat of increased intelligence towards Finland (I2, 2023).

New technologies are seen more as an opportunity than a threat by all of the interviewees (I2, 2023), (I3, 2023), (I8, 2022). Business opportunities for small businesses and startups were highlighted as the main opportunity, which accompanied by opportunities regarding disruptive technologies and new possible capabilities for Finland. Malicious use of new technologies against Finland is seen as a threat (I3, 2023), (I8, 2022). However, this is not caused directly because of NATO membership. Rather, it is caused by general technological evolution and new technologies being more easily obtainable and usable. Increased intelligence on NATO technologies and information is direct cause of NATO membership, but overall, the opportunities outweigh the threats generated.

Opportunities	Threats
• Business opportunities and funding • Disruptive technologies • New technological capabilities	• Malicious use of new technologies against Finland • Increased intelligence on NATO technologies and information

Table 12 New technologies opportunities and threats

5.13 Summary of results

Finland's cyber security has more strengths than weaknesses, according to the interviewees. Finland has been developing its cyber situation picture and cyber security preparedness capabilities for numerous years and it is positive for Finland that it is seen as a strength by the interviewees. Cyber security skills have been a topic of discussion in Finland as well as globally. Even though cyber security professional shortage is a serious issue that was discovered in the interviews as well, cyber security skills are still a strength of Finland.

Legislation was concurred as a weakness by the interviewees. Interviewees spotted issues that need to be addressed in interpretation of legislation and the level of detail of legislation. Legislation in Finland is updated rather slowly compared to the evolution speed of technology. This leads to inconsistencies if legislation is too detailed in terms of technical regulation. Cyber security management was a theme that raised opinions regarding whether it is a strength or a weakness. Ultimately it was seen as weakness. One of the key weaknesses was divided responsibilities regarding Finnish cyber security. This was seen as a topic that needs to be solved in Finland and which is currently a weakness.

NATO provides Finland with more opportunities than threats. Overall, the interviewees saw NATO as a positive development for Finland and themes that were discussed were mainly seen as opportunities. Threats were seen in indirect effects of NATO membership and in cyberspace. Cyberspace is such an unpredictable environment that it could produce threats to Finland, which are not seen yet. This was one of the key reasons that cyberspace ultimately was seen as a threat, even though there are some opportunities that NATO membership could provide for Finland in cyberspace as well.

New technologies and new collaboration partners were themes that were seen as opportunities. Furthermore, new collaboration partners is an opportunity, which was mentioned in other themes as well as an positive aspect of NATO membership. In addition to new technologies and collaboration partners, NATO membership provides Finland with new information which can be used in intelligence and cyber warfare. These themes were seen to gain a positive effect from NATO. When education and capabilities theme was discussed with the interviewees, it also formed a link between technologies, partners, intelligence and warfare as well. It provides Finland with opportunities in other opportunity areas as well. Another synergy link was formed with new technologies, which would provide positive effects to intelligence and cyber warfare.

Strengths 💪 • Cyber security preparedness • Cyber security skills • Cyber situation picture	**Weaknesses** 📉 • Legislation • Cyber security management
Opportunities 🌸 • New technologies • New collaboration partners • Intelligence • Education and capabilities • Cyber warfare	**Threats** 🔥 • Indirect effects • Cyberspace

Table 13 SWOT Analysis

Strengths, weaknesses, opportunities, and threats need to be analyzed in comparison with each other to discover strategies for Finland’s cyber security. They will form combinations, which were introduced in chapter 4.2. It needs to be noted that not all strengths will form combination or a workable strategy with every opportunity nor will they counter every threat that was discovered with SWOT analysis. Discovered combinations are presented in Table 14.

6 SWOT strategies

Strengths, weaknesses, opportunities, and threats need to be analyzed in comparison with each other to discover strategies for Finland’s cyber security. They will form combinations, which were introduced in chapter 4.2. It needs to be noted that not all strengths will form combination or a workable strategy with every opportunity nor will they counter every threat that was discovered with SWOT analysis. Discovered combinations are presented in Table 14.

Strategies aim to improve Finland’s cyber security by utilizing opportunities of NATO membership. Weaknesses can be logically improved with opportunities. Strengths can also be improved and the also provide possibility to benefit from the opportunities. Without existing strengths, some opportunities would be unavailable for Finland.

Threats can be avoided by using the existing strengths of Finland. However, combinations which include weaknesses and threats can also be discovered. In this case, the outcome is negative at the moment. Weakness-Threat strategies are however essential in improving cyber security level of Finland. These strategies discover the weak spots which need the most improving to avoid the threats that NATO membership creates.

6.1 Strength-Opportunity strategies

Strength-Opportunity (SO) strategies take advantage of possible opportunities of NATO membership by utilizing the internal strengths of Finland's cyber security.

SO1 strategy utilizes situation picture strength to gain full advantage of new partners that will be gained from NATO membership. Cyber situation picture was acknowledged as a strength of Finland, which could utilize new collaboration partners which was recognized as an opportunity. NATO will provide Finland with access to new information which can be adapted to Finland's already strong situation picture operations and processes. The United States and the United Kingdom were mentioned as partners that could provide Finland with valuable new information regarding situation picture (I3, 2023). The new information and data that can be gained from new collaboration partners is the key element that will strengthen Finland's situation picture operations. To fully take advantage of this opportunity, Finland needs to avoid misuse of its limited resources. This means that the resources should be allocated so that Finland gains new insight, data, and capability to improve its cyber situation picture.

SO2 strategy will also utilize the situation picture strength to take advantage of new technologies that NATO will have to offer to Finland. Lack of information sharing platform is a weakness within situation picture theme, which can be strengthened with NATO's new technologies. Even though lack of information sharing platform was initially discovered as a weakness within cyber situation picture theme, it is also evidence for maturity of cyber situation picture operations in Finland. Without level of maturity, need for joint information shared platform would not have been discovered in the interviews. This sign of maturity is also aligned with the consensus that cyber situation picture theme is strength of Finland. NATO will bring an opportunity to create a new information sharing platform, since NATO messages and documents need to be distributed to all parties (I4, 2023). This opportunity can also be considered as a requirement, as I4 states in their interview. NATO's new technologies will provide Finland with opportunity to gain new knowledge and capability to handle situation picture data and also technologies which will help with the situation data gathering and sharing.

SO3 strategy, on the other hand, utilizes cyber security skills strength to take advantage of NATO's education and capabilities. The level of expertise of cyber security professionals and diverse cyber security training were seen as the most significant strengths in cyber security skills theme. Finland has good education system, and the education is provided by various parties. However, it was seen that the education doesn't keep up with the latest changes and is sometimes on too general level. New education and training as well as cooperation opportunities were identified in education and capability's theme. All interviewees agreed that the theme included significantly more opportunities than threats.

Through the membership Finland will have the opportunity to develop further the skills of the cyber security professionals. The professionals will have more opportunities to attend various trainings as well as education programs. The cooperation and common exercises will increase and diversify the competences of the professionals. Through the opportunities from the membership, it is possible to expand the cyber security expertise in Finland.

The membership provides an opportunity for the professionals to receive training and education on topical issues which might not be yet addressed in the Finnish education program. In addition, Finland can develop its own education system through the information and knowledge received from NATO.

The lack of cyber security professionals globally as well as in Finland was identified as the most significant weakness in cyber security skills theme. The lack of professionals may create an obstacle for benefitting from the presented opportunities as there might not be enough professionals to attend the trainings. Therefore, Finland needs to prioritize the education and training opportunities it wants to firstly develop. Due to the lack of resources, professionals leaving for NATO positions can also be seen as threat.

SO4 strategy takes advantage of opportunities that NATO will present in intelligence area, while utilizing the strength of Finland's cyber situation picture. Situation picture gathering activities, active situation data reporting and beneficials tools and channels were seen as the strengths in cyber situation picture theme. Untapped potential was also identified within the theme. Intelligence information sharing was seen as the greatest opportunity within intelligence theme. The membership provides an opportunity to receive information that would have not been possible otherwise. The intelligence information is received through cyber intelligence as well as other intelligence methods.

The intelligence information received from the membership can be benefitted in enrichening the national cyber security picture. The lack of resources was identified as possible obstacle in gathering and analyzing the intelligence information. The limited amount of resources must be acknowledged when considering the strategy for improving the situation picture through the intelligence information.

The lack of situation picture analysis and situation awareness were seen as a weakness in Finland. The best practices (of other member countries) for the analysis of intelligence information and situation picture may be used to improve the weaknesses in Finland. The membership may provide tools for making use on the untapped potential in cyber situation picture.

6.2 Strength-Threat strategies

Strength-Threat (ST) strategies will implement Finland's internal cyber security strengths to prevent threats emerging from NATO membership.

ST1 strategy will utilize cyber preparedness as a strength to prevent the threat that comes from indirect effects of NATO membership. Cyber security preparedness was identified as a strength based on long history and baseline in preparedness. The preparedness level was seen good in organizations as well as in civil society. The skills of the individuals were also seen to be on sufficient level. Cooperation strengthened the preparedness level in Finland.

Indirect effect's theme included only threats and no opportunities. Indirect threats are difficult to predict, and the effects can be massive. The effects from indirect threats are not limited to cyber and can include for example political, reputational, and economical losses.

Due to the unpredictability of the indirect threats, it is difficult to forecast what they might be and what kind of effects will result. To be able to battle these threats it is crucial to be prepared. The good level of preparedness in Finland creates a valuable baseline for being ready for the unpredicted. Even though the scenarios arising from indirect threats may not have been predicted as such, the preparedness actions that have been conducted to prepare for similar incidents provide support for the results of the effects. However, it should be considered that even though the good level in preparedness can help in preventing the threats from occurring there might still be unseen threats that can't be tackled with only good cyber security preparedness.

Basic cyber hygiene measures, supply chain management and risk management were seen as a weakness within cyber security preparedness. The level of cyber security preparedness was seen lower as the overall preparedness level. To battle the threats of indirect threat it is crucial that Finland further develops its cyber security preparedness and the identified weaknesses within.

ST2 strategy prevents cyberspace threats by utilizing the strengths that were discovered in cyber situation picture activities of Finland. Since cyberspace is concluded to produce threats to Finland's cyber security, preventive strategies need to be implemented. While indirect effects could be countered with strong preparedness, cyber situation picture introduces measures to prevent cyberspace threats. The nature of cyberspace is constantly changing and rapidly evolving. This presents challenges in defensive measures. Cyber situation picture needs to be prompt and data reporting needs to be active and constant.

Cyber situation picture has numerous strengths which will help Finland to counter threats from cyberspace. Situation data reporting is active and situation picture gathering activities are considered mature. Cyberspace can produce very rapid ad-hoc situations, which need to be coordinated very quickly. Fortunately, ad-hoc situation process is one of the strengths that was discovered during the interviews regarding cyber situation picture. Threats from cyberspace range from very simple activities like attempting to log in to system with default credentials to very detailed attacks involving multiple attack vectors and methods, done by state actors like APT groups. Preparedness of Finland is also a strength that counters threats from cyberspace. However, for this strategy, cyber situation picture offers more suitable strengths. Cooperation of cyber situation picture officials in unpredictable situations is a strategy that will prevent cyberspace threats.

6.3 Weakness-Opportunity strategies

Weakness-Opportunity (WO) strategies take advantage of gained opportunities to minimize the effects of weaknesses. Cyber security management was concluded as a weakness of Finland in the conducted interviews. WO1 strategy utilizes cyber warfare as an advantage which could provide Finland with benefits to minimize the effects of cyber security management as a weakness.

Weak management will hinder all cyber security operations in Finland, whether they are considered as a strength or weakness by themselves. However, opportunities from NATO membership can benefit Finland’s cyber security and especially in this case, cyber security management. Cyber warfare is seen as a strength of NATO by the interviewees and Finland will gain knowledge and capabilities as a NATO member (I4, 2023), (I6, 2022), (I7, 2023), (I9, 2022). Potential cyber warfare threat linked to leadership was discovered during the interviews. If Finland is not recognized as an important NATO member in cyber warfare, it is possible that the opportunities gained from this area are not available to Finland. To handle this potential threat, Finland needs to be united in cyber security sector and needs clear objectives which it wants to achieve. Cyber warfare is an opportunity for Finland to grow and learn in this sector of cyber security. Interviewees declared it as an important opportunity which needs to be taken advantage of. If this opportunity is utilized, it will enhance Finnish cyber security management in all sectors, not just cyber warfare, by promoting new methods of leadership and cooperation, for example. Evolution of cyber security management in Finland is mandatory, and NATO provides opportunity to do so. Activation of Article 5 could be considered as a threat to Finland, if its management roles and processes are unclear, as they were seen to be in the interviews (I2, 2023), (I5, 2023).

6.4 Weakness-Threat strategies

Weakness-Threat (WT) strategies aim to minimize the threats that could emerge from new threats that are presented by the NATO membership, if they are directed towards areas that are a weakness of Finland.

WT1 strategy aims to minimize the cyberspace threats which could exploit the legislation weakness of Finland. Cyberspace is an aspect of cyber security which is evolving rapidly. Legislation related to cyber was seen as weakness of Finland, and one of the reasons is that the development and evolution of legislation is too slow. This creates an obvious discrepancy between legislation, which is slowly evolving, and cyberspace, which is rapidly evolving. Joining NATO will create threats, since Finland's presence in cyberspace grows to include the presence of other NATO nations as well. Attack surface will not only consist of systems and networks of Finland, but the whole NATO alliance should be considered as Finland's cyberspace.

Cyberspace is also very unpredictable and needs to be constantly monitored for hostile actions and new trends. This forms challenges for Finnish legislation. Finland should consider how it will handle activation of Article 5 in case of cyber-attack. The process requires decision making and detailed interpretation of legislation, which is considered a weakness in Finnish cyber security. Result from the interviews indicate that interpretation of law is different between officials. This can lead to situations that are greatly hindered by disputes on how to interpret the law. As stated before, situations in cyberspace can be rapid and require unified and clear decision making in constricted timeframes. Another weakness that can be exploited by threats originating from cyberspace is the level of detail in legislation itself. Some aspects offer no possibility to interpret the law. If a weakness is found in legislation, it is possible that cyberspace actor can exploit it and officials are left in a difficult situation on how to counter the threat. Minimizing the threat requires cooperation and shared guidelines on how to interpret legislation and how to act in cyberspace events.

WT2 strategy aims to minimize the threats of cyberspace, which emerge from cyber security management weakness of Finland. Cyberspace after Finland's NATO membership is anticipated to provide difficult cyber cases for Finland. Finland's presence in cyberspace will grow and thus there will be increased number of attack vectors against it. Globally the number of cyber-attacks has been growing annually. This has also been the trend in Finland (Traficom, 2022b). Responding and handling cyber security incidents is routine in Finland. However, difficult case management is considered to be a weakness. This is problematic when considering the threats from cyberspace after NATO membership. While it may be true that the incident management and leadership in simple cases is clear already, NATO membership may require Finland to face more complex and advanced incidents than before. Hostile activities in cyberspace will increase and there is also the possibility that activation of Article 5 needs to be considered. Without compatible cyber security management, these threats will present Finland with considerable challenge that needs to be taken into consideration in all organizations. Uncertainty about management roles and responsibilities need to be clarified while also making developments to tactical and operational cyber security management.

	Opportunities 🌸 • New technologies • New collaboration partners • Intelligence • Education and capabilities • Cyber warfare	**Threats** 🔥 • Indirect effects • Cyberspace
Strengths 💪 • Cyber security preparedness • Cyber security skills • Cyber situation picture	**SO Strategies** • SO1 - Situation picture data from new partners • SO2 - Situation picture information sharing • SO3 - Improving and expanding skills through education and training • SO4 - Improving situation picture through intelligence	**ST Strategies** • ST1 - Preparing for the unpredicted • ST2 – Cooperation of cyber situation picture officials
Weaknesses 📉 • Legislation • Cyber security management	**WO Strategies** • WO1 – Evolution of cyber security management in Finland	**WT Strategies** • WT1 – Shared processes and cooperation of officials • WT2 – Development of tactical and operational cyber security management

Table 14 SWOT combination strategies

6.5 Analysis of strategies

Cooperation, information sharing and the activity of Finland as member country were subjects that were raised in multiple themes. The importance of cooperation in Finland as well as globally was raised frequently, for example in cyber security management, situation picture and new collaboration partners themes. The cooperation in Finland was considered to be on good level, but there was still room for improvement. The cooperation needs to be conducted between civilian and military sector as well as between private and public sector. The membership was mainly seen as an opportunity for increasing and improving the cooperation with the Alliance as well as the member countries.

Multiple interviewees highlighted in different themes (i.e. cyber security management and education & training) that Finland needs to be active actor to receive the benefits from the membership. Firstly, Finland needs to prioritize where it wants to focus. Due to the limited resources, it is important to decide for example which partners are the most relevant for cooperation and which trainings to attend.

Information sharing and new information identified to be in significant role for Finland’s cyber security. Information is crucial in many of the themes such as cyber security management and cyber situation picture. The membership was seen as an opportunity for receiving more information and thus further developing the national capabilities. This is also the case regarded intelligence, which will gain benefits from the enhanced partnership between Finland and NATO member states.

Legislation was detected as a weakness of Finland. It was the only theme that did not form a combination with the opportunities that were discovered during the interviews and analysis. It did, however, form a combination with a threat of cyberspace and is thus concluded to be negative aspect of Finnish cyber security. It needs to be noted that within this weakness are also strengths and it’s not completely negative.

NATO membership provides Finland with numerous opportunities. The result of the analysis of SWOT combinations was, that there were most combinations and formed strategies in strengths and opportunities category. These strategies take advantage of the strengths that Finland already has to make use of opportunities that NATO membership presents. This result can be deducted to be positive for Finland and it also correlates with the initial results of the interviews before they were analyzed further. Even though strengths and weaknesses of Finland are divided almost equally, opportunities and threats are divided more clearly in favor of opportunities.

Numerous opportunities presented a possibility that the discovered weaknesses could be minimized by utilizing the discovered opportunities. However, the least amount of strategies were discovered for this theme, which implies that the opportunities do not directly minimize the weaknesses that were discovered. Since there are only two weaknesses, legislation and cyber security management, half of them could be minimized with strategies that emerge from the opportunities. This can be seen as a positive result as well.

7 Discussion

The research objectives were to identify the strengths and weaknesses of Finland's cyber security as well as the threats and opportunities of NATO membership and the aim of the thesis was to increase the awareness of Finland's NATO membership cybersecurity point of view as well as to help to prepare to possible threats and to enable best use of benefits by proactive planning. SWOT analysis was used to analyze the information and to form strategies for developing Finland's cyber security. Research objectives were accomplished and answers to the research questions were formed from the analysis of the gathered data.

The results concluded that Finland has more strengths than weaknesses in cyber security. However, weaknesses were also identified within the themes that were identified as strengths. Legislation and cyber security management were seen as weaknesses in Finland while cyber security preparedness, cyber security skills and cyber situation picture were identified as strengths. Based on the results, the membership provides more opportunities than threats. Only indirect effects and cyberspace were seen as a threat within the seven themes. Gathered data from interviews provided answers to research questions 1 and 2 after analyzing the data.

To avoid the threats produced by NATO membership (indirect effects and cyberspace) two kind of strategies were formed: Strength-Threat and Weakness-Threat. Three strategies were identified to battle the threats arising from cyberspace and one strategy for threats arising from indirect effects. In conclusion, these threats were seen to arise from NATO membership, and they could have effects on Finland's cyber security. Cyberspace differs from indirect effects, since it had also some opportunities, even though the threats were finally concluded to be greater. It is possible however, that both threats can be mitigated or even turned to be opportunities by utilizing the strategies that were presented in chapter 6.

To benefit the most from the membership strength-opportunity and weakness-opportunity strategies were formed. For each identified opportunity, at least one utilization strategy was formed. Especially SO strategies were identified which can be concluded as positive results as they provide opportunities for improving and strengthening Finland's cyber security. Despite multiple identified opportunities, strategies for battling the weakness in Finnish legislation were not found. Analysis and forming of strategies provided answers to research questions 3 and 4.

Many of the results in strength-weakness section are in line with the recent Report on the authorities' capacity to act in cyber security matters (Finnish Government, 2023). The results of the report as well as the conclusions from this study pointed out the development needs in proactive preparedness and information sharing. The report presents development actions to improve the current state of Finland's cyber security. The strategies identified in this thesis and the identified development actions should be reviewed together to find possible synergies. The benefit from this thesis is that it includes the evaluation and consideration of the opportunities and threats from the membership.

Further research on the discovered strategies should be conducted. These strategies should be formed to action plans that Finland could apply directly to its cyber security. Cyber security strategy could present these strategies as a part of its development strategy. Since the official's capacity to act in cyber security matters is also recently studied, the strategies discovered in this study should be examined in relation to the results of that study. Concrete action plans derived from the discovered strategies could benefit Finland and realistically help it to gain the most benefit from NATO membership while mitigating the discovered threats. These strategies could be implemented by individual authorities, but some of them require cooperation and implementation on a higher level. Synchronization of cyber security strategy with the discovered themes should be studied further.

7.1 Integrity, validity, and reliability

This thesis is conducted according to ethical guidelines provided by Finnish national board on research integrity. According to the board, the basic principles for research integrity are reliability, honesty, valuation, and responsibility (Finnish Advisory Board on Research Integrity, 2023, p. 11). The results of the study are presented as they are, and the thesis includes the required in-text references as well as a list of references at the end of the thesis. To ensure the transparency and repeatability of the research, the research methods, as well as the research questionnaire, are presented.

The reliability of this study evaluates its repeatability and consistency with previous studies. The interviewees consisted of subject matter experts and the number of interviewees was sufficient (10). The interviewees were gathered from different sectors to receive holistic information on the topic. As the thesis was conducted as qualitative research it is likely that different interviewees could raise different opinions or subjects. However, it is considered that the difference would have not been significant. Due to the topicality of the thesis topic, it is not possible to repeat the study precisely similarly. Finland joined NATO and thus some of the effects have already occurred and might change the answers of the interviewees. The results of the study pointed in the same direction as previous studies conducted on cyber security in Finland. The effects of the membership have not been evaluated comprehensively before but similarities with effects that have occurred in other NATO member countries were identified.

The validity of the study evaluates how the selected method is suitable for measuring the researched topic and answering to the research questions. The researched topic is wide, it has not been fully studied before and there is no one correct solution to the problem. Therefore, qualitative method and interview were seen as suitable methods for the study. To stay within the research topic and limited themes, semi-structured interviews were used. This allows the interviewees to discuss the topic more freely within the selected topic. The selected method provided desirable answers to the research questions.

7.2 Limitations

Cyber security is a crucial part of comprehensive security in Finland. Due to its importance to the nation as well as to the private sector and citizens, many of the entities related to the topic are classified. Thus, one of the most significant limitations of the study is that the thesis is conducted as public research. Classified information has been limited outside the scope of the research. The scope of the thesis is wider instead of focused on one or few specific themes as it is then easier to stay on public level. The generality of the scope of the research also provides an opportunity for gaining an overview of the topic. This kind of research has not been conducted previously.

The topic of the thesis is limited to national cyber security and is not focused on the private sector or individual citizens. The private sector and individuals are only considered in themes if they create positive or negative effects on national cyber security. Due to this limitation, only representatives from the public sector are interviewed for the thesis.

The objective was to discover Finland’s strengths and weaknesses regarding cyber security as well as threats and objectives that NATO membership would produce. However, these effects were researched using interviews that were semi-structured and divided into themes. This meant that themes were already concluded before the interview which limited the interviewees' range of answers. It is possible that not all strengths and weaknesses regarding Finland’s cyber security or opportunities and threats presented by NATO membership were not discovered due to this research method. However, the themes were designed so that they would limit the interviewee and their thoughts as little as possible. They could raise issues outside the selected themes whether they considered them as important for the topic. This was also the rationale for choosing semi-structured interview, which allows more discussion than a structured interview, while still limiting the discussion enough that it can be divided into themes and pre-determined question patterns. During the interviews, no new themes could be derived from the interviewees' answers. This was also the case when the gathered data was coded and divided into themes. No new themes appeared during the coding of gathered interview data, which lead to the conclusion that the pre-determined interview themes worked as intended in this research.

The focus of the study is on the effects that the membership has on Finland’s cyber security within the selected themes. The effects that Finland as a member might have on the cyber security and defence of the Alliance are not the focus of the thesis. However, some of these effects were also identified within the research and they are presented. The list of these effects is not comprehensive, and the results are mainly used to support the theories on why Finland may get certain opportunities or threats from the membership.

Due to the topicality, there isn’t much previous research conducted on the theme even though Finland’s membership has been discussed since Finland joined the EU. The discussion on the effects of the membership has been mainly focused on the traditional side of defence such as nuclear weapons. Research and discussion around cyber and NATO have grown recently and cyber has been addressed as an increasingly important domain. However, there has been a lack of comprehensive study on the opportunities and threats that the membership brings to Finland’s cyber security.

Finland joined NATO on April 4th, 2023. The interviews for this thesis were conducted prior to the membership and therefore the effects that occurred after the membership have not been considered in the interviews. Likewise, the theory base for the thesis was conducted prior to the actual membership.

References

Printed

Caso, J. S., 2014. The rules of engagement for cyber-warfare and the Tallinn Manual: A case study. In: *The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent*. Hong Kong: s.n., pp. 252-257.

Endsley, M. R., 1995. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors Journal, Volume 37, Issue 1*, pp. 32-64.

Hirsjärvi, S. & Hurme, H., 2004. *Tutkimushaastattelu*. Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P., 2007. *Tutki ja kirjoita*. 13th ed. Keuruu: Otavan Kirjapaino Oy.

Kärkkäinen, A., 2013. The origins and the future of cyber security in the Finnish Defence Forces. In Rantapelkonen, J.&Salminen, M. (toim.) The fog of cyber defence. Volume 2, pp. 102-103.

Laari, T. et al., 2019. *#kyberpuolustus-Kyberkäsikirja Puolustusvoimien henkilöstölle*. 3 ed. Helsinki: Maanpuolustuskorkeakoulu, Sotataidon Laitos.

Lin, H. S., 2010. Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy*, Issue 4, pp. 63-64.

Palonkangas, M. & Paronen, A., 2022. *Epätavallisen tavallista*. Joensuu: PunaMusta Oy.

Paul, J.-P., 2005. *Tiedustelu 2000-luvulla*. Helsinki: Kustannusosakeyhtiö Tammi.

Schmitt, M. N., 2002. Wired Warfare: Computer network attack and jus in bello. *International Review of the Red Cross, Volume 84, Issue 846*, 6, pp. 365-399.

Sirjonen, R., 2019. Oikeutettua sotaa verkossa: Milloin kyberhyökkäys täyttää aseellisen voimankäytön vaatimukset?. *Acta Legis Turkuensia 1/2018*, pp. 187-215.

The Security Committee, 2017b. *Vocabulary of Comprehensive Security*. 2nd ed. Helsinki: Sanastokeskus TSK ry.

Electronic

Accenture, 2019a. *Cyber threatscape report*. [Online]
Available at: https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf
[Accessed 26. 2. 2023].

Accenture, 2019b. *SNAKEMACKEREL:Threat campaign likely targeting NATO members, defence and military outlets.* [Online]
Available at: https://www.accenture.com/_acnmedia/pdf-94/accenture-snakemackerel-threat-campaign-likely-targeting-nato-members-defense-and-military-outlets.pdf
[Accessed 26 2 2023].

Bergqvist, M., Heisbourg, F., Nyberg, R. & Tiilikainen, T., 2016. *Arvio Suomen mahdollisen NATO-jäsenyyden vaikutuksista.* [Online]
Available at:
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79159/IP1601374_UM_Nato-arvioFI_13371.pdf
[Accessed 7. 1. 2023].

Bugge, A., 2018. *Portuguese secret service official sentenced for spying for Russia.* [Online]
Available at: https://www.reuters.com/article/us-portugal-spy-idUSKBN1FS2Q1
[Accessed 22. 4. 2023].

CCDCOE, 2022a. *Finland Wins Cyber Defence Exercise Locked Shields 2022.* [Online]
Available at: https://ccdcoe.org/news/2022/finland-wins-cyber-defence-exercise-locked-shields-2022/
[Accessed 26 3 2023].

CCDCOE, 2022b. *Cyberspace Strategic Outlook 2030: Horizon Scanning and Analysis.* [Online]
Available at: https://ccdcoe.org/library/publications/cyberspace-strategic-outlook-2030-horizon-scanning-and-analysis/
[Accessed 10. 4. 2023].

CCDCOE, 2023a. *The NATO Cooperative Cyber Defence Centre of Excellence is multinational and interdisciplinary cyber defence hub.* [Online]
Available at: https://ccdcoe.org/
[Accessed 22 1 2023].

CCDCOE, 2023b. *Europen Union.* [Online]
Available at: https://ccdcoe.org/organisations/eu/
[Accessed 6. 4. 2023].

CCDCOE, 2023c. *Training.* [Online]
Available at: https://ccdcoe.org/training/
[Accessed 16 3 2023].

CCDCOE, 2023d. *NATO Recognises Cyberspace as a "Domain of Operations" at Warsaw Summit.* [Online]

Available at: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/
[Accessed 16 3 2023].

CINE-A, 2022. *NATO tutuksi suomalaisille.* [Online]
Available at: https://cinea.fi/blogi/nato-tutuksi-suomalaisille/
[Accessed 10 4 2023].

Community Tool Box, 2023. *Section 14. SWOT Analysis: Strengths, Weaknesses, Opportunities, and Threats.* [Online]
Available at: https://ctb.ku.edu/en/table-of-contents/assessment/assessing-community-needs-and-resources/swot-analysis/main
[Accessed 25 3 2023].

Crosley, J., 2020. *Qualitative Data Coding 101.* [Online]
Available at: https://gradcoach.com/qualitative-data-coding-101/
[Accessed 16. 3. 2023].

Danylyuk, O. V., Reynolds, N. & Watling, J., 2023. *Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022–February 2023.* [Online]
Available at: https://rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-russias-unconventional-operations-during-russo-ukrainian-war-february-2022
[Accessed 15. 4. 2023].

Department of Defense, 2021. *DOD Dictionary of Military and Associated Terms.* [Online]
Available at: https://irp.fas.org/doddir/dod/dictionary.pdf
[Accessed 28. 3. 2023].

Digital and Population Data Services Agency, 2023. *VAHTI network develops digital security.* [Online]
Available at: https://dvv.fi/en/vahti-network
[Accessed 16 3 2023].

Dudovskiy, J., 2023. *Inductive Approach (Inductive Reasoning).* [Online]
Available at: https://research-methodology.net/research-methodology/research-approach/inductive-approach-2/
[Accessed 26. 2. 2023].

ENISA, 2017. *ENISA overview of cybersecurity and related terminology.* [Online]
Available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-

opinions/enisa-overview-of-cybersecurity-and-related-terminology
[Accessed 12 3 2023].

ENISA, 2019-2020. *Cyber espionage-ENISA Threat landscape*. [Online]
Available at: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-cyberespionage
[Accessed 26 2 2023].

European Commission, 2020. *The EU's Cybersecurity Strategy for the Digital Decade*. [Online]
Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
[Accessed 7. 4. 2023].

European Commission, 2022. *The Cybersecurity Strategy*. [Online]
Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
[Accessed 6. 4. 2023].

Finnish Advisory Board on Research Integrity, 2023. *Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa [The guidelines for the responsible conduct of research and for handling alleged violations of conduct].* [Online]
Available at: https://tenk.fi/sites/default/files/2023-03/HTK-ohje_2023.pdf
[Accessed 30 4 2023].

Finnish Government, 2020a. *Kyberosaamistarpeet -esiselvitys*. [Online]
Available at: https://api.hankeikkuna.fi/asiakirjat/164ec5f9-d5a8-4d1b-9bf6-05e6470daab5/a40f74fd-b8f3-4bb7-a829-242de5732fb0/RAPORTTI_20210204085928.pdf
[Accessed 14 3 2023].

Finnish Government, 2020b. *Finland published its positions on public international law in cyberspace*. [Online]
Available at: https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace
[Accessed 1. 4. 2023].

Finnish Government, 2021a. *Government’s Defence Report*. [Online]
Available at:
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163407/VN_2021_80.pdf
[Accessed 23 3 2023].

Finnish Government, 2021b. *Valtionneuvoston selonteko tiedustelulainsäädännöstä*. [Online]
Available at: http://urn.fi/URN:ISBN:978-952-383-500-9
[Accessed 20 2 2023].

Finnish Government, 2022a. *Ajankohtaisselonteko turvallisuusympäristön muutoksesta.* [Online]
Available at:
https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/VNS_1+2022.pdf
[Accessed 15. 1. 2023].

Finnish Government, 2022b. *Ministerial working group discussed the development of cybersecurity and the preparedness of public administration.* [Online]
Available at: https://valtioneuvosto.fi/en/-//10623/ministerial-working-group-discussed-the-development-of-cybersecurity-and-the-preparedness-of-public-administration
[Accessed 25. 3. 2023].

Finnish Government, 2022c. *Selonteko Suomen liittymisestä Pohjois-Atlantin liittoon.* [Online]
Available at:
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164094/VN_selonteko_FI.pdf
[Accessed 15. 1. 2023].

Finnish Government, 2022d. *Kyberturvallisuusalan koulutusta kehitetään korkeakoulujen yhteistyönä – myös informaatiopsykologista tutkimusta vahvistetaan.* [Online]
Available at: https://valtioneuvosto.fi/-/1410845/kyberturvallisuusalan-koulutusta-kehitetaan-korkeakoulujen-yhteistyona-myos-informaatiopsykologista-tutkimusta-vahvistetaan
[Accessed 1 4 2023].

Finnish Government, 2023. *Report on the authorities' capacity to act in cyber security matters.* [Online]
Available at: http://urn.fi/URN:ISBN:978-952-383-542-9
[Accessed 12. 4. 2023].

Forsberg, T. et al., 2022. *Suomen Nato-kevät 2022.* [Online]
Available at: https://toivoajatuspaja.fi/wp-content/uploads/2022/04/Suomen-Nato-kevat-2022.pdf
[Accessed 7. 1. 2023].

Gervais, M., 2011. *Cyber Attacks and the Laws of War.* [Online]
Available at: https://ssrn.com/abstract=1939615
[Accessed 23. 1. 2023].

Gronholt-Pedersen, J., 2021. *U.S. spied on Merkel and other Europeans through Danish cables - broadcaster DR.* [Online]

Available at: https://www.reuters.com/world/europe/us-security-agency-spied-merkel-other-top-european-officials-through-danish-2021-05-30/
[Accessed 22. 4. 2023].

Iltalehti, 2022. *Näin suomalaiset operaattorit varautuvat Venäjän kyberhyökkäysiin.* [Online]
Available at: 4. https://www.iltalehti.fi/tietoturva/a/d0e6344e-3ecb-4f79-881d-c8f256c3379f
[Accessed 21 3 2023].

Innovation Hub, 2023. *Projects and Products.* [Online]
Available at: https://www.innovationhub-act.org/content/projects-and-products
[Accessed 18. 3. 2023].

Invest in Denmark, 2023. *New Danish NATO Center for Quantum Technology.* [Online]
Available at: https://investindk.com/insights/new-danish-nato-center-for-quantum-technology
[Accessed 15. 4. 2023].

ISC2, 2022. *Cybersecurity workforce study.* [Online]
Available at: https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx
[Accessed 14 3 2023].

JCS, 2018. *Cyberspace operations.* [Online]
Available at: https://info.publicintelligence.net/JCS-CyberspaceOperations.pdf
[Accessed 20 2 2023].

Juhila, K., 2023. *Koodaaminen.* [Online]
Available at: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/koodaaminen/
[Accessed 16. 3. 2023].

Kennedy, R. et al., 2020. *Strategic Management.* [Online]
Available at: https://vtechworks.lib.vt.edu/handle/10919/99282
[Accessed 26. 2. 2023].

Laje, D., 2023. *Finland Brings Cyber Capabilities to NATO.* [Online]
Available at: https://www.afcea.org/signal-media/cyber-edge/finland-brings-cyber-capabilities-nato
[Accessed 15. 4. 2023].

Laki julkisen hallinnon tiedonhallinnasta 906/2019, n.d. [Online]
Available at: https://www.finlex.fi/fi/laki/alkup/2019/20190906
[Accessed 28 3 2023b].

Laki sähköisen viestinnän palveluista 917/2014, n.d. [Online]
Available at: https://www.finlex.fi/fi/laki/ajantasa/2014/20140917
[Accessed 14. 3. 2023].

Laki sotilastiedustelusta 590/2019, n.d. [Online]
Available at: https://www.finlex.fi/fi/laki/ajantasa/2019/20190590
[Accessed 14. 3. 2023].

Lehto, M. et al., 2018. *Kyberturvallisuuden strateginen johtaminen.* [Online]
Available at: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160717/28-2018-Kyberturvallisuuden%20strateginen%20johtaminen.pdf?sequence=1&isAllowed=y
[Accessed 18 3 2023].

Loverdos, A., 2022. *THE OFFENCE-DEFENCE BALANCE: NATO'S GROWING CYBER CHALLENGE.* [Online]
Available at: https://www.nato-pa.int/document/2022-offence-defence-natos-cyber-challenge-report-pinotti-015-dscfc
[Accessed 10. 4. 2023].

Lyngaas, S., 2022. *Albania blames Iran for second cyberattack since July.* [Online]
Available at: https://edition.cnn.com/2022/09/10/politics/albania-cyberattack-iran/index.html
[Accessed 15. 4. 2023].

Maanpuolustuskoulutus, 2023. *Kyber- ja informaatioturvallisuus.* [Online]
Available at: https://mpk.fi/koulutukset/kyber-ja-informaatioturvallisuus/
[Accessed 21. 3. 2023].

Microsoft, 2022. *Microsoft Digital Defence Report 2022.* [Online]
Available at:
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us
[Accessed 14 3 2023].

Ministry for Foreign Affairs of Finland, 2020. *Katakri 2020. Information Security Audit Tool for Authorities.* [Online]
Available at: https://um.fi/documents/35732/0/FINAL+-+Katakri-

2020_201218_en.pdf/705d2bc6-6f1b-90dd-52e1-1ef97dae0623?t=1625140100978
[Accessed 25 3 2023].

Ministry for Foreign Affairs of Finland, 2022. *Suomen Nato-jäsenyyshakemus*. [Online]
Available at: https://um.fi/suomi-hakee-naton-jasenyytta
[Accessed 15. 1. 2023].

Ministry for Foreign Affairs of Finland, 2023. *Finland's membership in NATO*. [Online]
Available at: https://um.fi/finlands-membership-in-nato
[Accessed 26 4 2023].

Ministry of Defence, 2016. *Cyber primer (2nd Edition)*. [Online]
Available at: http://www.fraw.org.uk/data/wbd/mod-cyber-2016.pdf
[Accessed 20 2 2023].

Ministry of Defence, 2019. *Kyberpuolustuksen kehittämisen strategiest linjaukset*. [Online]
Available at:
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161771/Kyberpuolustuksen_kehitt%c3%a4misen_strategiset_linjaukset_PLM2019.pdf?sequence=1&isAllowed=y
[Accessed 26 3 2023].

Ministry of Defence, 2022. *Cyber Primer*. [Online]
Available at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1115061/Cyber_Primer_Edition_3.pdf
[Accessed 12 3 2023].

Ministry of Defence, 2023. *JEF cooperation*. [Online]
Available at:
https://www.defmin.fi/en/areas_of_expertise/international_defence_cooperation/jef_cooperation#e503c276
[Accessed 26. 3. 2023].

Ministry of Finance, 2023a. *Kyberturvallisuusstrategia*. [Online]
Available at: https://vm.fi/kyberturvallisuusstrategia
[Accessed 29 4 2023].

Ministry of Finance, 2023b. *Tiedonhallintalautakunta*. [Online]
Available at: https://vm.fi/tiedonhallintalautakunta
[Accessed 28 3 2023].

Ministry of Transport and Communications, 2021. *Kyberturvallisuuden kehittämisohjelma.* [Online]
Available at:
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163219/LVM_2021_7.pdf?sequence=1&isAllowed=y
[Accessed 18 3 2023].

Ministry of Transport and Communications, 2022. *Stefan Lee apulaiskyberturvallisuusjohtajaksi.* [Online]
Available at: https://www.lvm.fi/-/stefan-lee-apulaiskyberturvallisuusjohtajaksi-1880521
[Accessed 18 3 2023].

MITRE, 2019. *APT28.* [Online]
Available at: https://attack.mitre.org/groups/G0007/
[Accessed 26 2 2023].

National Cyber Security Center, 2022. *Kybreturvallisuuden varautuminen tehdään hyvän sään aikaan -ohje organisaatioille.* [Online]
Available at: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuden-varautuminen-tehdaan-hyvan-saan-aikaan-ohje-organisaatioille
[Accessed 21 3 2023].

National Research Council, 2009. *Technology, Policy, Law and Ethics regarding U.S. Acquisition and Use of Cyberattack Capabilities.* [Online]
Available at: https://nap.nationalacademies.org/read/12651/chapter/1
[Accessed 30. 1. 2023].

NATO, 1949. *The North Atlantic Treaty.* [Online]
Available at: https://www.nato.int/cps/en/natohq/official_texts_17120.htm
[Accessed 7. 1. 2023].

NATO, 2005. *Record 38531.* [Online]
Available at: https://nso.nato.int/natoterm/
[Accessed 28. 3. 2023.].

NATO, 2016. *Cyber Defense Pledge.* [Online]
Available at: https://www.nato.int/cps/en/natohq/official_texts_133177.htm
[Accessed 1. 4. 2023.].

NATO, 2018. *Brussels Summit Declaration.* [Online]
Available at: https://www.nato.int/cps/en/natohq/official_texts_156624.htm
[Accessed 18 3 2023].

NATO, 2019. *Record 39183.* [Online]
Available at: https://nso.nato.int/natoterm/
[Accessed 28. 3. 2023].

NATO, 2021a. *Manfred Bordeaux-Dehmer.* [Online]
Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm
[Accessed 16 1 2023].

NATO, 2021b. *Enlarging NATO's toolbox to counter hybrid threats.* [Online]
Available at: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html
[Accessed 7 4 2023].

NATO, 2022a. *Member countries.* [Online]
Available at: https://www.nato.int/cps/en/natohq/topics_52044.htm
[Accessed 15. 1. 2023].

NATO, 2022b. *Collective defence and Article 5.* [Online]
Available at: https://www.nato.int/cps/en/natohq/topics_110496.htm
[Accessed 15. 1. 2023].

NATO, 2022c. *NATO Organization.* [Online]
Available at: https://www.nato.int/cps/en/natohq/structure.htm
[Accessed 16 1 2023].

NATO, 2022d. *NATO Command Structure 2022.* [Online]
Available at: https://www.youtube.com/watch?v=yylsDFuvIJc
[Accessed 16 1 2023].

NATO, 2022e. *Cyber Defence.* [Online]
Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm
[Accessed 16 1 2023].

NATO, 2022f. *About us.* [Online]
Available at: https://shape.nato.int/about
[Accessed 16 1 2023].

NATO, 2022g. *Excercise Cyber Coalition.* [Online]
Available at: https://shape.nato.int/news-releases/exercise-cyber-coalition-2022-
[Accessed 22 1 2023].

NATO, 2022h. *NATO 2022 Strategic Concept.* [Online]
Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf
[Accessed 30 1 2023].

NATO, 2022i. *Deterrence and defence.* [Online]
Available at: https://www.nato.int/cps/en/natohq/topics_133127.htm
[Accessed 30 1 2023].

NATO, 2022j. *Brussels Summit Communique.* [Online]
Available at: https://www.nato.int/cps/en/natohq/news_185000.htm
[Accessed 18 3 2023].

NATO, 2022k. *Madrid Summit Declaration.* [Online]
Available at: https://www.nato.int/cps/en/natohq/official_texts_196951.htm
[Accessed 18 3 2023].

NATO, 2022l. *Emerging and disruptive technologies.* [Online]
Available at: https://www.nato.int/cps/en/natohq/topics_184303.htm
[Accessed 18. 3. 2023].

NATO, 2022m. *Partnerships: projecting stability through cooperation.* [Online]
Available at: https://www.nato.int/cps/en/natohq/topics_84336.htm
[Accessed 26. 3. 2023].

NATO, 2022n. *Resilience, civil preparedness and Article 3.* [Online]
Available at: https://www.nato.int/cps/en/natohq/topics_132722.htm
[Accessed 1. 4. 2023].

NATO, 2022o. *NATO reaffirms support for Albania following cyber attacks.* [Online]
Available at: https://www.nato.int/cps/en/natohq/news_207552.htm?selectedLocale=en
[Accessed 10. 4. 2023].

NATO, 2023a. *NATO's Cyber Security Centre.* [Online]
Available at: https://www.ncia.nato.int/what-we-do/cyber-security.html
[Accessed 22 1 2023].

NATO, 2023b. *NCI Academy.* [Online]
Available at: https://www.ncia.nato.int/what-we-do/nci-academy.html
[Accessed 16 3 2023].

NATO, 2023c. *Innovation.* [Online]
Available at: https://act.nato.int/innovation
[Accessed 18. 3. 2023].

NATO, 2023d. *Summit meetings.* [Online]
Available at: https://www.nato.int/cps/en/natohq/topics_50115.htm
[Accessed 25 3 2023].

NATO, 2023e. *NATO Agency signs important cyber security agreements.* [Online]
Available at: https://www.ncia.nato.int/about-us/newsroom/nato-agency-signs-important-cyber-security-agreements.html
[Accessed 26. 3. 2023].

NATO, 2023f. *Relations with Finland.* [Online]
Available at: https://www.nato.int/cps/en/natohq/topics_49594.htm
[Accessed 5 4 2023].

NATO, 2023g. *NATO team in North Macedonia to help against hybrid attacks.* [Online]
Available at: https://www.nato.int/cps/en/natohq/news_212621.htm?selectedLocale=en
[Accessed 10. 4. 2024].

Phair, D. & Shaeffer, A., 2022. *Research Aims, Objectives & Questions.* [Online]
Available at: https://gradcoach.com/research-aims-objectives-questions/
[Accessed 19. 2. 2023].

Poliisilaki 872/2011, n.d. [Online]
Available at: https://www.finlex.fi/fi/laki/ajantasa/2011/20110872
[Accessed 14. 3. 2023].

Schindler, J. R., 2016. *NATO's Big New Russian Spy Scandal.* [Online]
Available at: https://observer.com/2016/05/natos-big-new-russian-spy-scandal/
[Accessed 22. 4. 2023].

SIGNAL, 2023. *Finland brings cyber capabilities to NATO.* [Online]
Available at: https://www.afcea.org/signal-media/cyber-edge/finland-brings-cyber-capabilities-nato
[Accessed 7 4 2023].

Smith, B., 2022. *Digital Technology and the war in Ukraine.* [Online]
Available at: https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/
[Accessed 22. 4. 2023].

Supo, 2023a. *Intelligence is the main product of Supo.* [Online]
Available at: https://supo.fi/en/intelligence-serves-national-leadership
[Accessed 20 2 2023].

Supo, 2023b. *SUPO 2022 vuosikirja.* [Online]
Available at:
https://vuosikirja.supo.fi/documents/62399122/66519032/SUPO+Vuosikirja+2022.pdf/2650348b-77fb-ddf8-e80c-cc46a21d7074/SUPO+Vuosikirja+2022.pdf?t=1679642310821
[Accessed 22 4 2023].

Supo, 2023c. *Foreign intelligence and influence operations.* [Online]
Available at: https://supo.fi/en/intelligence-and-influence-operations
[Accessed 22 4 2023].

The Finnish Defence Forces, 2023. *Sotilastiedustelu julkinen katsaus 2023.* [Online]
Available at:
https://puolustusvoimat.fi/documents/1948673/73396483/Sotilastiedustelun+julkinen+katsaus+2023.pdf/d4cd9ebf-366d-242f-858a-24197750da1e/Sotilastiedustelun+julkinen+katsaus+2023.pdf?t=1674025184746
[Accessed 22 4 2023].

The Iran Primer, 2022. *Albania Cuts Ties with Iran Over Cyberattack.* [Online]
Available at: https://iranprimer.usip.org/blog/2022/sep/09/albania-cuts-ties-iran-over-cyberattack
[Accessed 15. 4. 2023].

The MITRE Corporation, 2022a. *Indirect Command Execution.* [Online]
Available at: https://attack.mitre.org/techniques/T1202/
[Accessed 25. 3. 2023].

The MITRE Corporation, 2022b. *cmd.* [Online]
Available at: https://attack.mitre.org/software/S0106/
[Accessed 25. 3. 2023].

The Security Committee, 2017a. *Security strategy for society. Government resolution.* [Online]
Available at: https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf
[Accessed 18 3 2023].

The Security Committee, 2017c. *Kodin kyberopas -Ohjeita digitaaliseen arkeen.* [Online]
Available at: https://turvallisuuskomitea.fi/wp-

content/uploads/2017/04/Kodin_kyberopas_TK_2017_verkkojulkaisu.pdf
[Accessed 16 3 2023].

The Security Committee, 2018. *Vocabulary of cyber security*. [Online]
Available at: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf
[Accessed 4 3 2023].

The Security Committee, 2019. *Suomen kyberturvallisuusstrategia*. [Online]
Available at: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf
[Accessed 12 3 2023].

TOP500, 2022. *ORNL'S EXAFLOP MACHINE FRONTIER KEEPS TOP SPOT, NEW COMPETITOR LEONARDO BREAKS THE TOP10*. [Online]
Available at: https://www.top500.org/lists/top500/2022/11/press-release/
[Accessed 15. 4. 2023].

Traficom, 2022a. *Havaro FAQ*. [Online]
Available at: https://havaro.fi/en/faq
[Accessed 7. 4. 2023].

Traficom, 2022b. *Threat level in cyber environment has risen – activity towards Finland has increased*. [Online]
Available at: https://www.traficom.fi/en/news/threat-level-cyber-environment-has-risen-activity-towards-finland-has-increased
[Accessed 29. 4. 2023].

United Nations, 2023. *United Nations Charter*. [Online]
Available at: https://www.un.org/en/about-us/un-charter
[Accessed 12. 3. 2023].

University of Jyväskylä, 2009. *Tulevan ennustaminen*. [Online]
Available at:
https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/ongelmanasettelu/tulevan-ennustaminen
[Accessed 19. 2. 2023].

University of Jyväskylä, 2010. *Thematic Analysis*. [Online]
Available at: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/en/methodmap/data-analysis/thematic-analysis
[Accessed 18. 3. 2023].

University of Jyväskylä, 2022a. *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimus-hankkeen loppuraportti.* [Online]
Available at:
https://jyx.jyu.fi/bitstream/handle/123456789/82709/Kyberturvallisuuden%20koulutusohjelman%20muutostarpeiden%20tutkimus%20v4.pdf?sequence=1&isAllowed=y
[Accessed 14 3 2023].

University of Jyväskylä, 2022b. *Jyväskylään lähes neljän miljoonan euron rahoitus kyberturvallisuusalan koulutuksen kehittämiseen.* [Online]
Available at: https://www.jyu.fi/fi/ajankohtaista/arkisto/2022/12/jyvaskylaan-lahes-neljan-miljoonan-euron-rahoitus-kyberturvallisuusalan-koulutuksen-kehittamiseen
[Accessed 14 3 2023].

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019, n.d. [Online]
Available at: https://www.finlex.fi/fi/laki/alkup/2019/20191101
[Accessed 28 3 2023a].

Valvira, 2023. *Monitoring the implementation of the Directive on Security of Network and Information Systems (NIS).* [Online]
Available at: https://www.valvira.fi/web/en/healthcare/information-systems-for-social-welfare-and-health-care/monitoring-the-implementation-of-the-directive-on-security-of-network-and-information-systems-nis-
[Accessed 14. 3. 2023].

Vuori, J., 2021. *Johdatus laadulliseen tutkimukseen ja verkkokäsikirjaan.* [Online]
Available at: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/mita-on-laadullinen-tutkimus/johdatus-laadulliseen-tutkimukseen-ja-verkkokasikirjaan/
[Accessed 26. 2. 2023].

Yemm, G., 2013. *Essential Guide to Leading Your Team: How to Set Goals, Measure Performance and Reward Talent.* Harlow, England: Pearson Education Limited.

Yhdistyneiden Kansakuntien peruskirja 1/1956, n.d. [Online]
Available at: https://www.finlex.fi/fi/sopimukset/sopsteksti/1956/19560001/19560001_2
[Accessed 12. 3. 2023].

YLE, 2022a. *TIetoturva-alan opiskelijoita ei valmistu riittävästi eikä koulutus vastaa työelämän tarpeita, kertoo yliopistotutkimus.* [Online]
Available at: https://yle.fi/a/3-12637353
[Accessed 14 3 2023].

YLE, 2022b. *Kyberhyökkäykset eivät ole lisääntyneet Suomessa Nato-hakemuksen jättämisen jälkeen.* [Online]
Available at: https://yle.fi/a/3-12461321
[Accessed 15 4 2023].

Unpublished

I1, 2023. *Expert 1, Public sector* [Interview] (6. 2. 2023).

I2, 2023. *Sari Kajantie, Finnish Security and Intelligence Service* [Interview] (15. 2. 2023).

I3, 2023. *Stefan Lee, The Ministry of Transport and Communications* [Interview] (25. 1. 2023).

I4, 2023. *Expert 1, The Finnish Defence Forces* [Interview] (25. 1. 2023).

I5, 2023. *Richard Wunsch, The Finnish Defence Forces* [Interview] (10. 1. 2023).

I6, 2022. *Tuomo Rusila, Defence Command* [Interview] (19. 12. 2022).

I7, 2023. *Expert 2, The Finnish Defence Forces* [Interview] (2. 1. 2023).

I8, 2022. Juhani Eronen, National Cyber Security Centre [Interview] (3. 12. 2022).

I9, 2022. Expert 1, Defence Command [Interview] (13. 12. 2022).

I10, 2022. *Timo Ryynänen, Private individual* [Interview] (7. 11. 2022).

Figures

Tables

Appendices

Appendix 1: Interview questionnaire

Agenda of the interview and themes

Interview themes have been divided according to the SWOT-analysis framework to strengths and weaknesses of Finland's cyber security and opportunities and threats of NATO membership.

Strengths and weaknesses: Cyber situation picture, Cyber security skills, Cyber security management, Legislation, Cyber security preparedness

- What strengths Finland has concerning this theme?
- How could the strengths be utilized better?
- What is the most notable strength of this theme?
- What weaknesses Finland has concerning this theme?
- How should the weaknesses be mitigated or developed?
- What is the most notable weakness in this theme?
- Is the theme strength or weakness in Finland's cyber security?
- Which themes are Finland's cyber security's most notable strengths and weaknesses?

Opportunities and threats: Cyber warfare, Cyberspace, New technologies, Intelligence, New collaboration partners, Education, and capabilities

- What new opportunities NATO membership generates for Finland regarding this theme?
- Are there obstacles to utilizing the opportunities?
- What is the most notable opportunity in this theme?
- What are the threats regarding this theme?
- What are the consequences of those threats?
- How likely is the threat?
- How could the threat be controlled?
- Are there more opportunities or threats in this theme?
- Which of the themes are the most notable opportunity and threat to Finland's cyber security?