Building Organizational Cyber Resilience

Pitfalls and Pearls of Cyber Exercises

Anu Laitila

Master’s thesis
October 2022
Master's Degree Programme in Information Technology, Cyber Security

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Laitila, Anu

Building organizational cyber resilience - pitfalls, and pearls of cyber exercises

Jyväskylä: Jamk University of Applied Sciences, November 2022, 88 pages

Master's Degree Programme in Information Technology, Cyber Security (YAMK). Master thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

Since 2016, the Finnish National Cyber Security Centre (NCSC-FI) has offered several services concerning cyber exercises. Services include, for instance, consulting assistance, instructions and scenarios to organizations planning to organize cyber exercises. Cyber exercise refers to a simulated situation where an organization can practice, for example, recovering from a major cyber incident.

The World Economic Forum has assessed cyber security risks as critical short-term risks that are important for both the business continuity of the organizations and the digitalization of society. For this reason, it is important that cyber exercises are goal-oriented and conducted with high quality.

For the first time, the training services of the NCSC-FI and the challenges within cyber training within Finnish organizations were examined. The goal of the work was to understand how the training activities of Finnish organizations can be improved and what the role of the NCSC-FI has in supporting the activities now and in the future.

According to the research, organizations needed closer cooperation and communication between the public and private sectors. In addition, it was researched that cyber security exercises need to be marketed more effectively than before and a more positive impression relating to exercises need to be created. Small organizations were interested in the services offered by the NCSC-FI. Large organizations were especially interested in opportunities related to cooperation.

The NCSC-FI received several new ideas for the development of its operations from industry professionals. Some of the ideas can be easily implemented as part of the everyday life of the employees of the NCSC-FI, such as establishing a network of cyber exercise organizations. Some of the development ideas require project planning and a longer-term plan, such as an online service that can be used to organize cyber exercises.

Keywords/tags (subjects)

cyber security, cybersecurity, cyber exercise, cyber security exercise, NCSC-FI, Finnish Cyber Security Centre, business continuity, resilience

Miscellaneous (Confidential information)

n/a

Description

Laitila, Anu

Kyberharjoitukset organisaatioiden jatkuvuuden kehittäjänä

Jyväskylä: Jyväskylän ammattikorkeakoulu, marraskuu 2022, 88 sivua

Master's Degree Programme in Information Technology, Cyber Security, opinnäytetyö YAMK.

Verkkojulkaisulupa myönnetty: Kyllä

Julkaisun kieli: Englanti

Tiivistelmä

Suomen kansallinen Kyberturvallisuuskeskus on vuodesta 2016 tarjonnut konsultointiapua, kyberharjoitusohjeita ja skenaarioita organisaatioille, jotka suunnittelevat kyberturvaharjoitusten järjestämistä. Kyberharjoituksella tarkoitetaan simuloitua häiriötilannetta, jossa voidaan harjoitella esimerkiksi kyberhäiriötilanteesta toipumista.

World Economic Forum on arvioinut kyberturvariskit kriittisiksi lyhyen aikavälin riskeiksi, joilla on merkitystä niin organisaatioiden liiketoiminnan jatkuvuuteen kuin yhteiskunnan digitalisoitumiseen. Tämän takia on merkittävää, että kyberturvaharjoitukset ovat tavoitteellisia ja laadukkaasti toteutettuja.
Tässä opinnäytetyössä on ensimmäistä kertaa tutkittu Kyberturvallisuuskeskuksen harjoituspalveluita ja suomalaisten organisaatioiden kyberturvaharjoittelun haasteita. Työn tavoitteena oli ymmärtää, miten suomalaisten organisaatioiden harjoittelutoimintaa voidaan parantaa ja mikä Kyberturvallisuuskeskuksen rooli on toiminnan tukemisessa nyt ja tulevaisuudessa.

Tutkimuksen mukaan harjoittelevat organisaatiot kaipasivat tiiviimpää yhteistyötä ja viestintää julkisen ja yksityisen sektorin välillä. Lisäksi nostettiin esille, että kyberturvaharjoituksia pitää markkinoida aikaisempaa tehokkaammin ja harjoitteluun liittyviä mielikuvia pitää muuttaa positiivisimmiksi. Pienet organisaatiot olivat kiinnostuneita Kyberturvallisuuskeskuksen tarjoamista palveluista. Suuret organisaatiot olivat kiinnostuneita erityisesti yhteistyöhön liittyvistä mahdollisuuksista.

Kyberturvallisuuskeskus sai alan ammattilaisilta useita uusia ideoita toimintansa kehittämiseksi. Osa ideoista on helposti toteutettavissa osana Kyberturvallisuuskeskuksen työntekijöiden arkea, kuten eri harjoitteluun liittyvien organisaatioiden verkoston perustaminen. Osa kehitysideoista vaatii projektisointia ja pidemmän aikavälin suunnitelman, kuten verkkopalvelu, jonka avulla voi järjestää kyberharjoituksia.

Avainsanat (asiasanat)

kyberturvallisuus, kyberturvallisuuskeskus, NCSC-FI, liiketoiminnan jatkuvuus, kyberharjoittelu, kyberharjoitus, kyberturvallisuusharjoitus

Muut tiedot (salassapidettävät liitteet)

n/a

Contents

Figures

Tables

Abbreviations

BIA	Business Impact Analysis
BS	Business Continuity
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, and Availability
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
DVV	The Digital and Population Data Services Agency
EK	Confederation of Finnish Industries
ENISA	European Union Agency for Cybersecurity
FATO	The finance sector exercise
FFCA	Finnish Competition and Consumer Authority
GDPR	General Data Protection Regulation
HER	Electronic Health Records
HSEEP	Homeland Security Exercise and Evaluation Program
HVO	Emergency Supply Organization

ISMS	Information Security Management System
ISO	The International Organization for Standardization
ITU	The International Telecommunication Union
KYHA	Finnish State Administration National Cyber Security Exercise
NCSC-FI	National Cybersecurity Centre in Finland
NCSC-UK	National Cybersecurity Centre in the UK
NDA	The contract and non-disclosure agreement
NESA	The National Emergency Supply Agency
NIST	The National Institute of Standards and Technology
PII	Personal Identifiable Information
PSI DSS	Payment Card Industry Data Security Standards
RA	Risk Assessment
RGCE	Realistic Global Cyber Environments
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SFS	Finnish Standards Association
UVM	University of Vermont Medical Center

1 Introduction

Imagine the situation where you are the hospital's Chief Information Security Officer (CISO), and you receive a phone call from the Service Desk. The Service Desk person informs you they are receiving a high amount of phone calls and messages from the hospital. The hospital personnel have informed the Service Desk that they have many issues. For instance, they cannot access patients' electronic health records (EHRs).

Unfortunately, this story was not just an imagination. A similar incident occurred at the University of Vermont (UVM) Medical Center in the US in October 2020. UVM Medical Center personnel had issues such as they were not able to use EHRs and payroll systems and they didn't know which patients were scheduled for treatments. Some of the many impacts were that many surgeries had to be postponed, and cancer patients were asked to go to another medical center for radiation treatments.

This incident was caused by malicious software, one of the biggest cyber threats to organizations, which IT personnel managed to discover after they started to investigate the issues. IT personnel also uncovered an instruction that they should contact the suspected threat actor who demanded ransom for the stolen data. This attack cost an estimated 50 million dollars, and it took IT personnel approximately three weeks to restore thousands of affected systems, according to the UVM Health Network Chief Medical Information Officer Doug Gentile. Some hospital systems were out of use for nearly a month, and recovery from the incident took several months. (Weiner, 2021)

This case is also an example where personal data's confidentiality, integrity, and availability (CIA) have been compromised, which are the three key elements for information security. Confidentiality means for organizations their must keep their data private, and they must prevent unauthorized access, integrity contains accuracy and reliability of the data so it can be trusted, and the availability means that the data must be available when needed. For the hospital case example, the applications and networks were not functioning, so data could not be accessed, and the data was lost. (Samonas & Coss, 2014)

In 2020, over 600 health care sector organization's business were troubled by cyber-attacks. In total the attacks had impact on nearly 20 million people's EHER's in the USA alone. The estimated cost of these attacks was nearly $21 billion. Worldwide, the healthcare sector is on top of the most attacked sectors. (Bischoff, 2021) An organization's cost of data breaches are an average of US $3.6 million per incident in any industry. On average, an organization takes approximately 280 days to detect and respond to a cyberattack. (IBM, 2022)

The cyber-attack against the health care sector is just one example of cyber-attacks against critical infrastructure providers, such as ports, the energy sector, logistics, and airports. The attacks against critical infrastructure have typically significant impacts on society at large, such as the availability of governmental services, availability of electricity, food supply, or important logistics facilities. Critical infrastructure is used when discussing the organization, which has either physical or digital assets, systems, and networks, which are considered so vital to the society that the destruction would have a disturbing impact on national economic security, public health or safety, or any combination thereof. (Cybersecurity and Infrastructure Security Agency, 2020)

Globally, it's been recognized that cyber security risks are amongst the essential short-term risks that governments and the public sector must manage as seen in the Figure 1. The cyber security risks are only going to increase in complexity and volume. For instance, it's been evaluated that since the COVID-19 pandemic started, the cyber security failures as a risk have grown 12,4 %. Currently, cyber security failures are the top 7th most worsened risk. In East Asia, the Pacific, and Europe, cyber security failure ranks in the top five risks, and in Australia, Great Britain, Ireland, and New Zealand, the risk is on top of the list. (World Economic Forum, 2022)

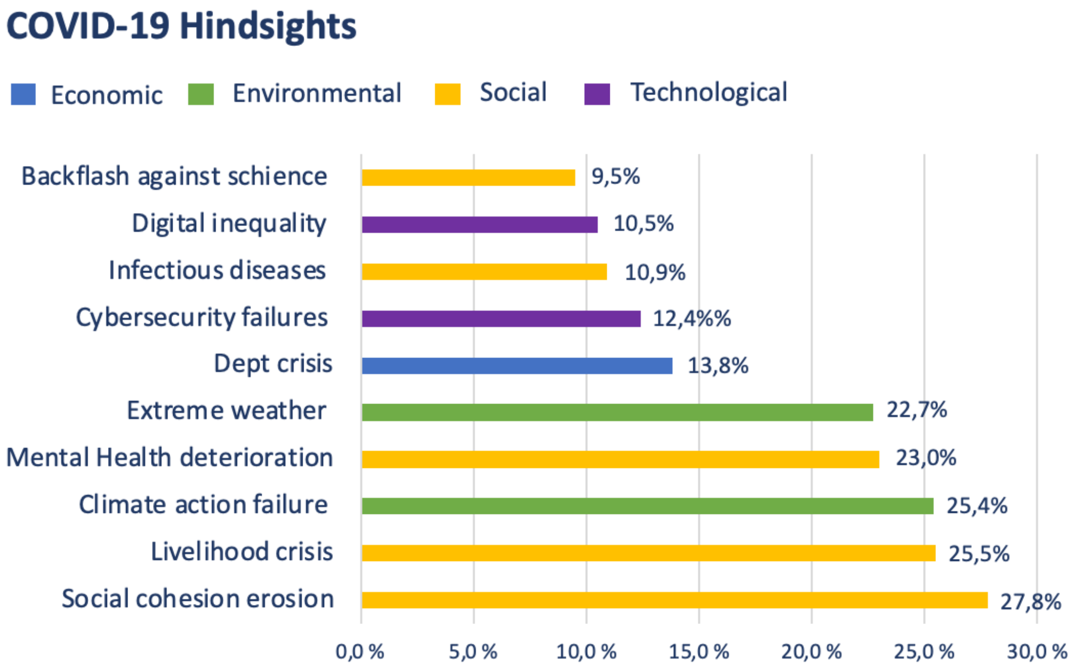
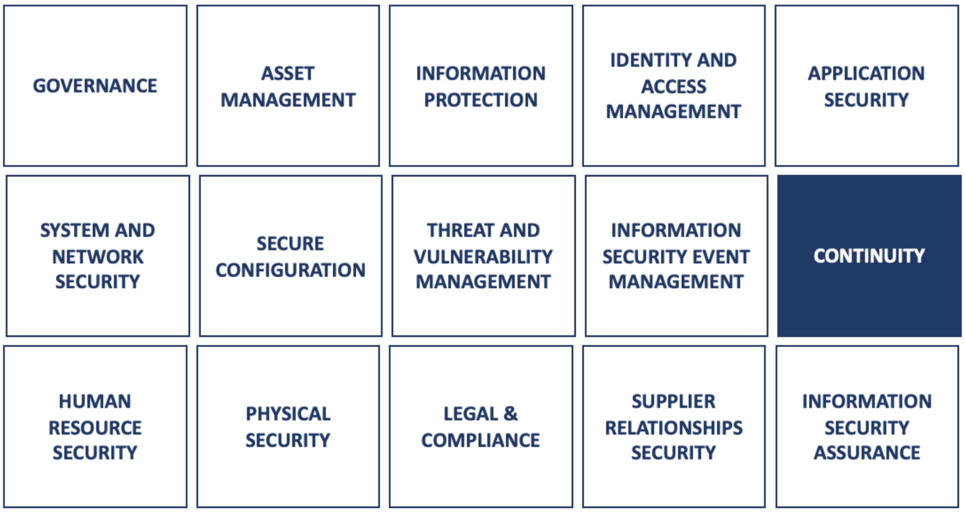


Figure 1. Risks that worsened the most since the start of the COVID-19 crisis (World Economic Forum, 2022)

To mitigate the growing cyber security risks, the public and private sectors have started to manage information security systematically. Building an Information Security Management System (ISMS) means focusing on understanding what the assets to be protected are, what the risks are related to these assets, and which security controls must be implemented to mitigate the risks. For instance, ISO 27001 presents a set of globally known best practices for security controls related to people, processes, and technology and typically builds one or more operational capabilities, such as information protection and continuity as presented in Figure 2. (ISO 22398:2013)



GOVERNANCE	ASSET MANAGEMENT	INFORMATION PROTECTION	IDENTITY AND ACCESS MANAGEMENT	APPLICATION SECURITY
SYSTEM AND NETWORK SECURITY	SECURE CONFIGURATION	THREAT AND VULNERABILITY MANAGEMENT	INFORMATION SECURITY EVENT MANAGEMENT	CONTINUITY
HUMAN RESOURCE SECURITY	PHYSICAL SECURITY	LEGAL & COMPLIANCE	SUPPLIER RELATIONSHIPS SECURITY	INFORMATION SECURITY ASSURANCE

Figure 2. Continuity is one of the operational capabilities in Information Security Management (ISO 27002:2022)

Continuity can be defined as the ability to maintain the all-important function during and after the disruption has occurred. Business Continuity consists of Business Impact Analysis (BIA), Risk Assessment (RA), identifying the essential functions, defining disaster recovery point objective (RPO) and time objective (RTO), making disaster recovery plans, testing, training, and regular cyber exercises as presented in Figure 3. The main aim of Business Continuity (BS) is to maintain the organization's resiliency and keep essential functions operating during the disruption with the minimum downtime of the services. (ISO 22301: 2019)

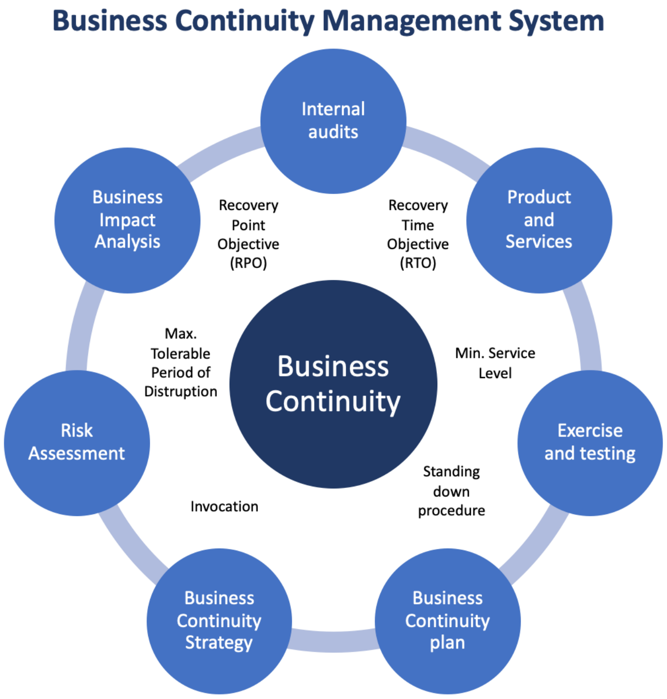


Figure 3. Exercise and Testing are vital components of Continuity Management according to ISO 22301:2019.

Cyber exercises simulate an incident that could happen to an organization and interrupt its everyday operations. Cyber exercise is like a fire drill, but the imagined issues happen, at least partly in a digital environment. In these cyber exercises, organizations can practice and test their operating processes in case of disruptions and find their weaknesses. Organizations can improve continuity planning from exercise observations and learnings to increase their resilience. The exercises can be prepared for different levels and target audiences. Strategic level exercises are usually for management where they practice decision making; operational level exercises are more tactical and have good coordination. In technical level exercises, the focus is on detection, investigation, and mitigation. (European Union Agency for Network and Information Security, 2015) The different types of exercises are presented in Figure 4.

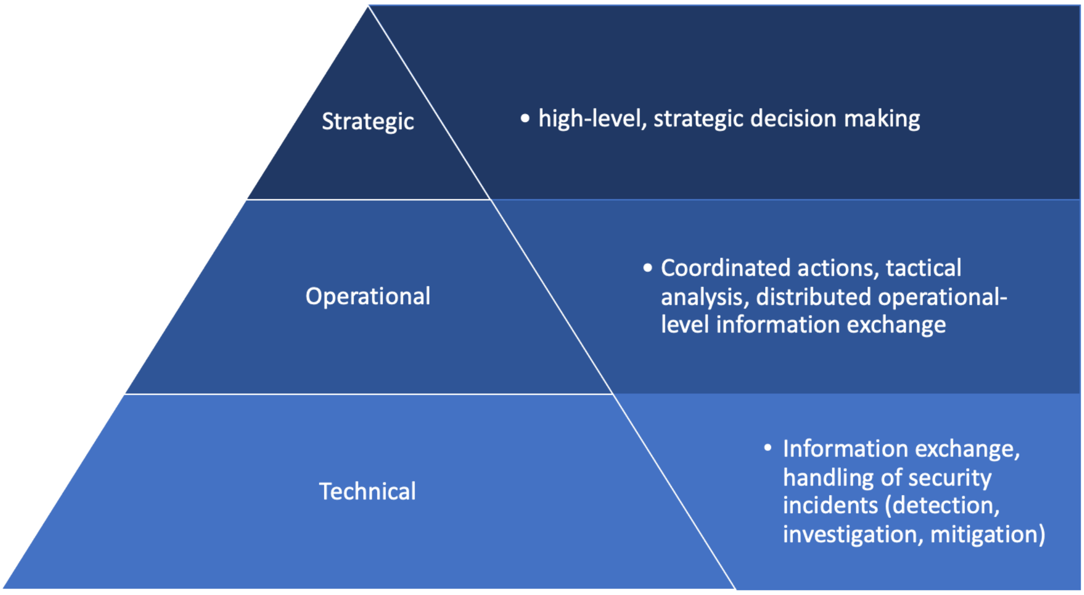

Strategic
• high-level, strategic decision making
Operational
• Coordinated actions, tactical analysis, distributed operational-level information exchange
Technical
• Information exchange, handling of security incidents (detection, investigation, mitigation)

Figure 4. Scope and functions of different types of cyber exercises (European Union Agency for Network and Information Security, 2015)

The European Commission, its Member States, and many governments worldwide have identified the importance of the cyber exercises when increasing the cyber resilience of organizations. For instance, the NCSC-UK has created an exercise simulator that can be used for any organization, The Cybersecurity and Infrastructure Security Agency (CISA) has created a library of exercise scenarios targeted especially at critical infrastructure entities, and the Victorian Government in Australia has created a guide that advises the organizations on how to produce and host exercises.

In Finland, Finnish National Cyber Security Centre (NCSC-FI) has cyber exercise-related services, especially for critical infrastructure organizations, and they are introduced more in detail in the next chapter. Their services are part of the action plan of the cyber security strategy of Finland, which states that the national cyber security education and exercise system will be strengthened as part of public administration. The federal and international training and exercise activities and their development also support the competence development of cyber security professionals in Finland. (Secretariat of the Security Committee, 2019)

In my daily work at Nixu cyber security, I have participated over 50 exercises in the past three years. I have seen that exercises are one of the best ways to prepare organizations for cyber-related issues, strengthen their business processes, share the knowledge among their employees, and learn new concerning different areas of cyber and information security. The cyber exercises are efficient tool for learning, and people learn when they need to ponder the answers to complex questions. Questions that most likely should also be answered when an actual real incident occurs.

1.1 Objectives

The research was conducted for the NCSC-FI, and the aim was to support the development of their cyber exercise services. The main objective of this research was to understand how the NCSC-FI could support public and private organizations better in the future with regards to their cyber exercises. Furthermore, via the research, we should understand the most prominent challenges organizations are facing to organize efficient and effective cyber exercises to mitigate the security risks and what kind of tools and services the NCSC-FI could offer in addition to their current exercise services.

1.2 Scope

The theoretical part of the thesis introduces critical infrastructure organizations and their business continuity and preparedness needs. Cyber exercises are an efficient method of mitigating cyber risk and increasing resilience against cyber incidents. The focus is primarily on scalable services like tabletop exercises. Technical cyber exercises which demand virtual platforms such as Realistic Global Cyber Environments (RGCE) are out of the scope. The reason being that there is already one widely used platform in Finland, which is owned by the Jyväskylä University of Applied Sciences and, the NCSC-FI has a specific annual budget that the plans need to suit. The benchmarking for services has been done globally. However, the focus of this thesis is only on developing exercises organized in Finland or by Finnish organizations abroad.

2 Current role of Finnish Cyber Security Centre in cyber exercise services in Finland

The National Emergency Supply Agency (NESA) launched the KYBER2020 project in 2016. The KYBER2020 consisted of several sub-projects for several sectors such as water supply and health care. The projects were, for instance, to develop threat detection and form a common understanding of the situational awareness. The aim was that the organizations would be able to tolerate cyber-attacks better and recover fast from cyber-attacks back to normal operations. The main development areas were developing risk management and business continuity. (Nortio, 2017) KYBER2020 project in 2016 activated the NCSC-FI's systematic support for exercise activities. The personal interviews with current employees of the NCSC-FI confirms that the exercise team have participated in the planning and implementation of many different cyber exercises in Finland and abroad. Since 2016, the NCSC-FI has participated in over 100 exercises organized by companies and, in addition, participated in the planning of national exercises such as TIETO, TAISTO, and KYHA (Traficom, 2019b) and a multinational joint exercise with the Estonian Computer Emergency Response Team (CERT-EE). The main national exercises of Finland are showcased in a table on page 52. Since 2020, systematic support for cyber exercise activities has become part of the permanent and primary services of the NCSC-FI and is now financed by the Finnish Transport and Communications Agency instead of NESA. However, NESA may still support national cyber exercises related services which are introduced in the next chapter. Currently, the NCSC-FI offers various services for organizations introduced in the following chapters. (Traficom, 2020)

The KYBER2020-project has finished, and the NESA has launched a new project called DT2030 which will finance some the NCSC-FI cyber exercise activities until 2030. This time, the project aims to develop the service to meet the current needs of the target group, the critical infrastructure organizations of Finland. (National Emergency Supply Agency, 2021)

In 2019, the NCSC-FI has written a manual for cyber exercise organizers. The aim of the manual is to provide instructions for organizing cyber exercises, explaining what cyber exercises are and how to manage them. This manual's target audience are people responsible for their organizations' information and cyber security. The manual is currently available in Finnish, Swedish, and English. (Finnish National Cyber Security Centre, 2019)

The NCSC-FI has created three cyber exercise scenario booklets in 2020, 2021, and 2022. All three booklets contain 50 different security incidents that organizations can use as simulated scenarios for cyber exercises. Cyber security specialists from organizations such as KPMG, Lähi-Tapiola, Telia, Valmet, and the National Bureau of Investigation have created the scenarios in collaboration with the NCSC-FI. The inspirations for all scenarios have been real-life cyber security incidents. All three scenario booklets are available in Finnish on Kyberturvallisuuskeskus.fi website and are free to use. (Finnish National Cyber Security Centre, 2022)

Consulting organizations are one of the significant services of the NCSC-FI exercise team, which holds the small team very busy. The NCSC-FI offers consulting services in English and in Finnish, and services are free for all companies. In addition, the NCSC-FI has listed companies offering and providing cyber security-related training and exercise services as part of their own services. The list includes redirecting links to 13 company websites. The NCSC-FI can assist the companies in finding a suitable partner for their training needs. (Finnish National Cyber Security Centre, 2021)

The NCSC-FI core services also include creating situational awareness of the significant security events affecting cyber security, such as up-to-date information concerning the current software vulnerabilities and sector-specific threat landscape. These alerts are concerning major information security incidents. The NCSC-FI gathers the data via their global and local networks. With the situational awareness information, the NCSC-FI can assist in finding the most probable threats for each organization. (Finnish National Cyber Security Centre, 2021)

The NCSC-FI services support organizations to detect cyber-attacks, solve the issues, and aid their recovery from the incidents. The NCSC-FI can simulate this actual service in the exercise and the organization can report the incident to the NCSC-FI. One of the NCSC-FI exercise team members will participate in the exercise and act in the respondent's role. (Finnish National Cyber Security Centre, 2021)

Year 2020 brought the most significant changes to cyber exercise activities since the NCSC-FI exercise services started in 2016. The COVID-19 pandemic changed the business model from in-person exercises to remote exercises. Instead of a person from the NCSC-FI joining the exercise in the same room with the participants, one can sit in their own home and participate in the exercise via Microsoft Teams or any other similar video conferencing application. (Traficom, 2021b) In addition, the NCSC-FI personnel can act as an observer during the exercise (Finnish National Cyber Security Centre, 2021). Observers have an essential role in the exercises; the observer creates notes and identifies actions that entities should take to improve their resilience and the observer often identifies challenges such as the incident management process not being followed accordingly. (The Club de la Continuité d’Activité (CCA) & French National Cyber Security Agency (ANSSI), 2021)

The NCSC-FI offers assistance in post-exercise analysis (Finnish National Cyber Security Centre, 2021). The post-exercise analysis lists the exercise findings. It includes all most essential observations from all participants and observers, identifies development tasks and lists recommendations, and states a summary of participant feedback. (The National Cyber Security Centre of UK, 2020)

To promote cyber exercise offerings, the NCSC-FI has created several articles regarding cyber exercises. Articles introduce examples of experiences from KONE, Keva, and Kuopion Energia. These three companies openly shared their knowledge, for instance, why they have been organizing the exercises and what has been their main findings. In addition, they are encouraging other organizations to achieve the same via similar activities. The articles are available in Finnish on the website of the NCSC-FI. (Finnish National Cyber Security Centre, 2021)

3 Research

The NCSC-FI research was conducted in two separate parts. Part one was executed by the NCSC-FI and they used quantitative research methods in their research. They conducted an online questionnaire and phone interviews. This thesis is focusing the part two only and research is introduced in the next chapters.

3.1 The main research question and objectives

The goal of the work was to understand how the training activities of Finnish organizations can be improved and what the role of the NCSC-FI has in supporting the activities now and in the future. The primary target audience for the research were organizations that are either organizing, participating, or having a significant role in the Finnish cyber exercise industry. The research target audience presents both the public and private sectors.

The main research question for this research was:

how could the NCSC-FI better support organizations in the public and private sector in the future in their cyber exercises?

The secondary research questions were:

a. What are the main challenges for the organization and why they are not participating or organizing the cyber exercise?

b. how to get organizations and companies to train more and with better quality?

c. Are cyber exercise organizers interested in using the NCSC-FI services for their commercial service purposes?

The question ‘C’ was essential for the NCSC-FI. Finland has a competitive neutrality regulation to maintain fair competition between the public and the private sector. The basic principle is that a public organization must incorporate its market activities. Under this circumstance, this means that the NCSC-FI is required to carefully consider what kind of services they offer to different organizations. For instance, they can offer them for free or partner with private sector organizations. The NCSC-FI has partnered with the private sector previously. For instance, they provide a national observing and an early warning system, HAVARO, jointly with the private sector. The NCSC-FI delivers the service, and the private sector sells it to their customers. (Traficom, 2021c)

Competitive neutrality regulation is monitored by the Finnish Competition and Consumer Authority (FFCA). There could be consequences if FFCA notices any distortion of the competition. They will first try to solve the challenges by negotiations. If negotiations won’t have a positive outcome, FFCA has an authority to prohibit the operations of public organizations or impose penalty fees to guarantee compliance. (Finnish Competition and Consumer Authority, 2022)

3.2 Research Methodology

The goal for the research was to understand the experiential phenomenon and describe it in such a way that it maintains its means without the researcher's influencing it. We, as humans, understand other people and the world according to how we have experienced it in our own life. A researcher performing research tries to avoid the natural way of understanding things according to prior understanding and replace it with a scientific attitude. (Hirsjärvi & Hurme, 2015, 43, 64; Perttula & Latomaa, 2006, 163-164)

Interviews are one of the primary and most used methods to gather information for research. The interview is an excellent method when there is no expectation for answers and answers are based on the experience of the person interviewed. The main goal of the interview is to gain a deep understanding and new information related to the researched topic. (Hirsjärvi & Hurme, 2015, 35)

The interview is like a discussion in many ways, including nonverbal and verbal communication. Both deliver information about thoughts, attitudes, opinions, knowledge, and feelings. The interview is a method where one answers the questions, and the other asks the questions. It is very flexible, and it fits many proposes. Interviews need a purpose that has been decided in advance. In the interviewing session, the researcher is named the interviewer, and the person who answers the questions is named the interviewee. (Hirsjärvi & Hurme, 2015, 42)

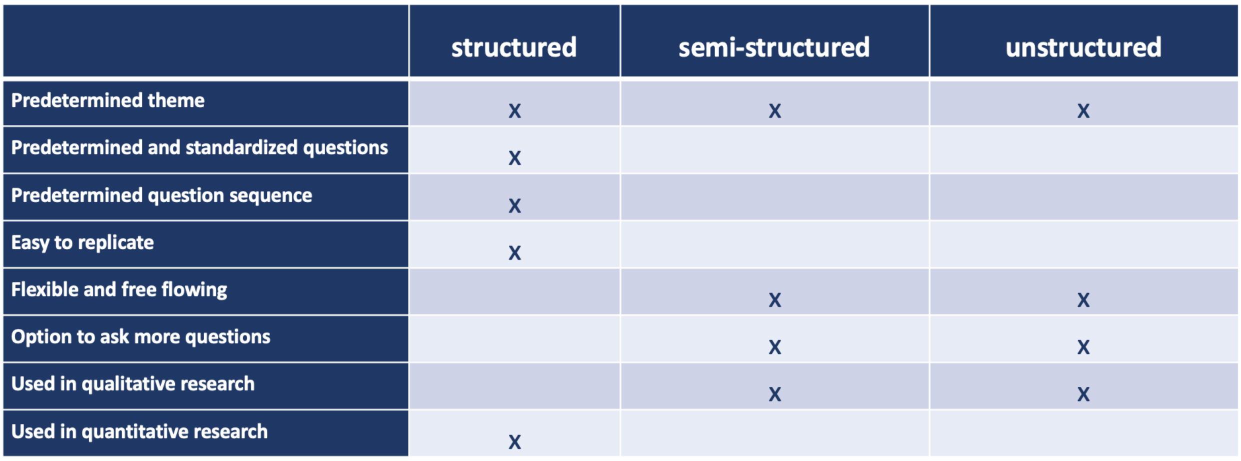
Sometimes the word interview can confuse people and have a negative impact, so it can also be named a discussion instead. However, in research, the interview usually raises positive feelings in the interviewees as they can consider themselves as a subject matter expert in the chosen topic and asking people for an interview may impress people and make them feel important. (Gillham, 2013, 5)

According to Hirsjärvi & Hurme (2015, 43) the perfect interviews have five main typical attributes:

1. The interview has been preplanned, and the researcher understands the research object in practice and theory. The main objective is that interviewer gains reliable information regarding the problems from essential research areas.
2. The interview is started by the interviewer and directed in a controlled manner
3. The interviewer is often required to motivate the interviewee
4. Each party understands their role in the interview
5. The interviewee can trust that information shared is handled in a confident manner

The above attributes describe the perfect interview. It is very rare that the interviews are excellent, usually at least one of the listed attributions is missing. The researcher needs to be open and curious concerning the interviewee. Sometimes the questions can even feel odd to the interviewee, or the interviewee may even lie. The interviewee may have some issues with the topic, and the interviewer cannot help, which can be frustrating for both parties. (Hirsjärvi & Hurme, 2015, 43)

The are many techniques to conduct the interviews. The main methods are structured, unstructured, and semi-structured. In a structured interview, the interviewer has preprepared a theme and set of questions in a preplanned sequence. A structured interview is primarily used to collect data in quantitative research. Unstructured interviews have a decided theme but not necessarily fixed patterns or sets of questions. It is more like a discussion where the conversation flows between interviewer and interviewee. It also typical that there are open questions when structured interview may even have a list of answers from which the interviewee can choose. A semi-structured interview has a predetermined theme, and the questions are not set in order or phrasing. Both unstructured and semi-unstructured interviews are primarily used to collect data in qualitative research. (Gillham, 2013, 6; Hirsjärvi & Hurme, 2015, 45-48) The Figure 5 presents the key differences and similarities of structured, unstructured, and semi-structured interviews.



	structured	semi-structured	unstructured
Predetermined theme	x	x	x
Predetermined and standardized questions	x		
Predetermined question sequence	x		
Easy to replicate	x		
Flexible and free flowing		x	x
Option to ask more questions		x	x
Used in qualitative research		x	x
Used in quantitative research	x		

Figure 5. The main interview techniques and their differences (Hirsjärvi & Hurme, 2015, 45-48)

In the research interview, the researcher must decide how the interviews are conducted. Interviews can be hosted in many ways, for instance, in a group or as in an individual interview. The idea of a group interview is hosting the interview for a several people simultaneously. In contrast, in the personal interview, there are just an interviewee and interviewer present in the situation. Personal interviews are a more used method. The main idea of an individual interview is to prevent other people from influencing or interrupting the discussions. (Hirsjärvi & Hurme, 2015, 61)

It is typical for theme interviews that interviewees are not randomly selected for an interview. Instead, the informants are carefully chosen, and they usually are the experts in the researched topic field. The set of interviewees are selected by the researcher. There is no standard on how many informants there must be. It is purely the researcher's decision to decide what is enough interviewees to gather the needed data. The theme is also decided, and there are some preplanned questions, but the order is not set, and additional questions can be asked. In these interviews, the discussions focus on themes. Typically, the interviewees have experienced a specific situation and reflect on their subjective experiences. With theme interviews, the thought, feelings, experiences, and non-verbal experiences are at the center of research. The focus is on the knowledge of the chosen topic. It is in the nature of the theme interview that the researcher may specify and deepens some discussion during the interview via the researcher's own experiences and expertise. (Hirsjärvi & Hurme, 2015. 47-48)

Theme areas in a research project are displayed in Figure 6. The chosen themes should not limit the versatile nature of researched phenomena. It is unnecessary to present questions in a specific order. Instead, there should be a theme catalogue, a time, and an opportunity to ask more questions related the topic and delve deeper into the subject as far as there is interest in the research. (Gillham, 2013, 161; Hirsjärvi & Hurme, 2015, 66-67)

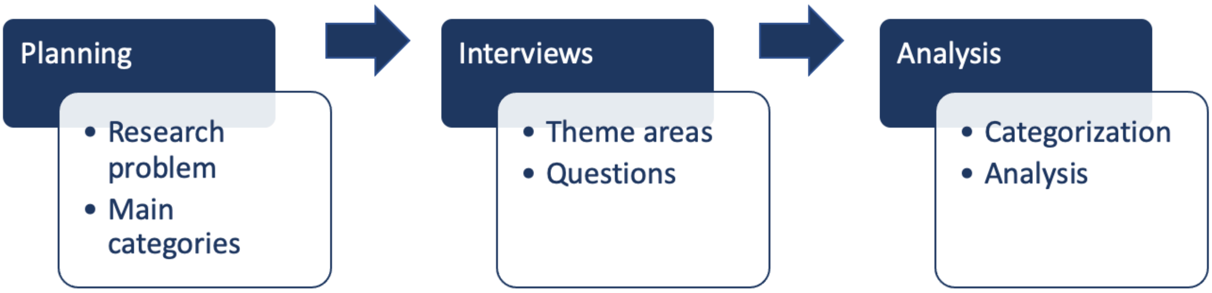


Figure 6. Theme areas in a research project (adapted from Hirsjärvi & Hurme, 2015, 65)

The interview research method has both advantages and disadvantages. For instance, the disadvantages are that the research is very time-consuming and costly compared to online questionnaires. Especially, transcribing is time-consuming. It takes approximately ten times more time to transcribe the interview than the interview time. Especially hosting the interviews, transcribing, and analysis has plenty of manual work which cannot be automated. Sometimes the interviews may take place in other countries or cities, and travelling time is always an extra. Sometimes analyzing, reporting, and concluding can be difficult and the interviews may requirement all separate recording tools and software which will increase the cost. (Gillham, 2013, 9-10)

The researcher should carefully consider how the interview is conducted. Typically, people are lazy to write answers to open questions in online surveys but rather give more time to answer in person instead. (Gillham, 2013, 13) All interviews shall be recorded for transcribing. However, sometimes, the interviewees may feel uncomfortable with it. The positive sign is that they usually forget it the moment the interview starts. (Hirsjärvi & Hurme, 2015, 92) Sometimes in phone or video interviews without the camera, there can be silent moments, and it can be difficult for the interviewer to understand what is occurring. Is the interviewee is pondering or doing something else? (Hirsjärvi & Hurme, 2015, 64)

The other disadvantage that interview may include mistakes in references from both ends and the interviewee may feel socially pressured and gives answers that consider are right or in their own benefit. Sometimes people do not dare to answer to open questions truthfully and sometimes they may need more guidance. (Hirsjärvi & Hurme, 2015, 43)

On the other hand, there are many benefits to research interviews. The researcher gains rich and vivid information via the interviews, and the results are practical and concrete. As mentioned before, the response rate is often reasonable. Instead, people give an hour for a personal interview rather than 15 minutes for online surveys. Online surveys have become a very used research tool as it is easy to conduct, and less work is needed, but on the other hand, the negative side is that the response rate can be expected to be poor. In online research, the usual 30 % response rate is satisfactory, and 50 % is good. However, in personal interviews, the success rate in personal interview invitations is often very good, near 100 %. The interviewee often feels impressed and important when asked for an interview, and they like to give their time for a good cause. They also know that the interviewer has committed time for them, and they are there to listen. (Gillham, 2013, 14-15) The research method is also a good method if questions need more explanation so that the interviewer can ask any questions during the interview, and the interview is flexible and gives the researcher an opportunity to understand so much more than online research results. The interviewer can ask for explanations and justifications for opinions which you cannot do in written research either. The response is generic, richer, and more diverse. The method is also one the best when the researcher needs to understand the subject that has no previous research concerning it. (Hirsjärvi & Hurme, 2015, 106-108)

The first task when starting the research project is to create the research plan. A good research plan includes at least these seven parts, showcased in Figure 7 below. (Hirsjärvi & Hurme, 2015, 56)

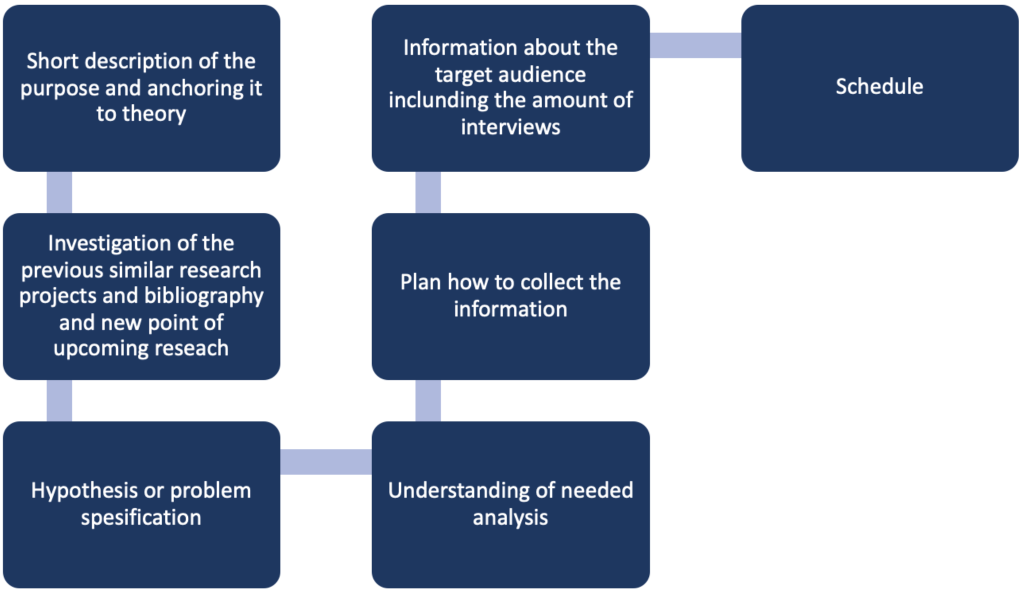

Short description of the purpose and anchoring it to theory
Investigation of the previous similar research projects and bibliography and new point of upcoming reseach
Hypothesis or problem spesification
Understanding of needed analysis
Plan how to collect the information
Information about the target audience inclunding the amount of interviews
Schedule

Figure 7. The parts of the research project (adapted from Hirsjärvi & Hurme, 2015, 56)

The research plan gives good understanding of the objectives and why the research will be necessary. It also creates a clear picture to the researcher what phases the research will include and what is expected from the researcher. The research plan is recommended for both qualitative and quantitative research and it is described as an essential planning tool. (Hirsjärvi & Hurme, 2015, 54)

3.2.1 The role of the interviewer

No one is born with good interview skills; they need to be trained. The interviewer must also understand that they have a strong influence on the whole situation, and the interviewer needs to handle different kinds of people. If there is no trust between interviewee and interviewer, the results may be poor, and there is no information to be used in the research. (Gillham, 2013, 4-5)

Hirsjärvi and Hurme (2015, 68-69) lists the several requirements for a good interviewer:

- Knows the theme very well in practice and in theory
- Understand the meaning of the interview

- Can lead the interview and can naturally host a discussion and know the good and right questions
- Keeps the interview under control, keeps the themes in mind
- Simple and straightforward language, for instance, avoid using slang or professional jargon, and questions shall be simple and easy to understand
- Understand that interviewee may have alternative motives
- Is open-minded
- Is empathetic and confident
- Do not drive attention to themself
- Should be interested in human behavior, and it is a benefit if one can understand the nonverbal signs
- Take the research seriously and behave without causing unnecessary attention

To summarize, the interviewee needs to feel confident that the interviewer is a professional and can be trusted. The interview style will always be very personal and can be practiced. (Hirsjärvi & Hurme, 2015, 68–69)

3.2.2 Practicalities for interview

The date and time for the interview shall be booked in advance and, at the same time, decide the place for an interview jointly with the interviewee. Usually, the interviews are conducted in person in a quiet place where the interviewer can guarantee there are no interruptions. The good places, for instance, are a school, library, or office. If possible, the seating plan shall be considered in advance, and the interviewee should not sit too far from the interviewer. If the distance is too long, the confidentiality of the appointment may suffer. (Hirsjärvi & Hurme, 2015, 73-74, 89-91)

The preparation of the interviews often consumes more time than the interviews themselves. The interviewer shall also prepare the event well in advance. The maximum duration for an interview is two hours, but overall, the duration can vary a lot, and it really depends on the interviewee. It is often ideal to have time for small talk before the interview, so both parties can have time to familiarize with each other. This is also a good opportunity for the interviewer to start creating a positive and reliable atmosphere. It is also advised to leave time for informal discussion after the interview. It is not appropriate to stop the interview straight after the last questions or after own objectives are met. The interviewer should read the situation and maybe even offer a cup of tea or coffee after the interview if possible. The interviewer must also listen if the interviewee says something unrelated to the research project and show respect. However, the interviewer must retain control of the interview as a whole and time reserved for the session. (Gillham, 2013, 13-14; Hirsjärvi & Hurme, 2015, 74-75)

3.2.3 Transcribing the interview

Transcribing shall be completed from the recording word by word, or it can be decoded in themes. Computer software is recommended; however, they have not been widely used by students and researchers. One of the main reasons is the money. Licensed software is expensive, and usually, educational institutes do not have licensees for the software, and software is often considered difficult to use. Sometimes transcribing is conducted by a third party. In these cases, details instructions are needed. If transcribing is not required, the decoding can be done by separating the themes. Computer software is also recommended for this use cases. (Hirsjärvi & Hurme, 2015, 75-77, 138-141)

The researcher shall keep in mind that an hour of an interview may take up to ten hours to transcribe, and analysis may take up to six hours. The recording is usually recommended because, for the analysis part, everything can be recalled. The critical part is also to ask permission from the interviewee to record the session. (Gillham, 2013, 10) Research ethics are also good to bear in mind in transcribing as they often reveal the person who has been interviewed, and the main idea is to preserve that information confidential in the final research. (JAMK, 2018.)

3.2.4 Analysis

There are many ways to analyze the data and analyzing method should be always considered before the data is gathered. It is typical that the researcher has more data that they will use for their analysis. Usually, the interview data is very interesting but at the same time, it is time consuming to analyze the data as a whole and categorizing the data to different themes can be difficult. Especially, the qualitative data analysis has many options, sometimes the analysis phase has already started during the interviews so when data is collected. One of the differences between main qualitative and quantitative research analysis is that qualitative research data is usually saved in written format. For instance, when there has been interview with open questions only. The researcher shall have a good understanding and experience of the main topic so it should be easy to start making observation already during the interview and start creating the themes groups for instance. (Hirsjärvi & Hurme, 2015, 135-136)

Eskola and Suoranta (2015, 202-207) presents three alternative methods to analyze the data; 1) data is decoded and analysis is done based on intuition of the researcher, 2) data is decoded and coded and after that analysis phase is ready to get started, 3) decoding and coding is merged and researcher can start the analysis. Analyzing the data is flexible and researcher can try alternative methods or create own methods.

The analyzing of the data shall be started soon after data has been collected when researcher still has the motivation, and everything is fresh in the memory. If the researcher notices something is missing it will be easier for corrections straight after the interviews than many months later when most likely the interviewee have forgotten the interview. Though, sometimes researcher need to distance them from the research for a while to clear their head. (Hirsjärvi & Hurme, 2015, 135-136)

When the data has been collected and saved, the researcher has two options to decode the data. The first option is to transcribe the data and the second option is to write conclusions or decode the themes from the data. The example of analysis process for interview data is seen below in Figure 8. (Hirsjärvi & Hurme, 2015, 144)

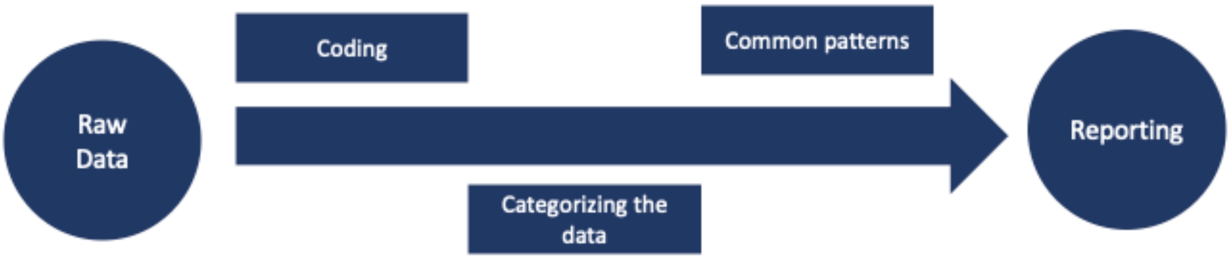


Figure 8. Analysis process for interview data (adapted from Hirsjärvi & Hurme, 2015, 144)

If transcribing is chosen, Hirsjärvi and Hurme (2015, 139-140) recommends a tool for decoding. Often the researchers consider transcribing word for word as the most time-consuming phase which is why sometimes researcher are using assistants or even companies to accomplish this phase. If outsourced resource is used, one should have very good directions on how the work shall be conducted for instance, what needs to be in written format. If the researcher decides not to use transcribing, the alternative option is to create cards to identify themes and common patterns in the data. This coding system will help the researcher to categorize the qualitative data and create meaningful groups. Via this system, the researcher should be able to analyze and find the similarities and differences, common patterns, and relationships between the data. The final stage in the analysis, is to create the conclusions and summarize the findings. (Hirsjärvi & Hurme, 2015, 144-145)

3.2.5 Reliability of the research

When evaluating reliability, the following matters must be considered, among other matters: the object, aim, and purpose of the research. For instance, what is being researched and why, what the researcher's own commitments are in the research and why this research is important. In data collection, it is important which method is used, and if it is done with an interview, then with which interview format. Whether there are one or more interviewers also has an impact on the results and are the interviews conducted individually or in a group. Anonymity must be guaranteed throughout the research process. The researcher should let the participants in the study read the results of the studies before publishing the study and possibly also mention their comments in the study. The duration of the research indicates how long the research has lasted. The method of analysis of the material must also be clarified in the research. The reliability of the research must be evaluated ethically and at a high level. When reporting the research, it is explained how the material was collected. (Tuomi & Sarajärvi, 2006, 135-138)

According to Hirsjärvi and Hurme (2000, 185), the reliability is also affected by the quality of the recordings, the uniformity of the transcription and the regularity of the categorization.

3.3 Related research

ENISA has been researching cyber exercises since 2002, and they have gained insights from nearly 300 cyber exercises, mainly from major joint exercises organized by the public sector. (European Union Agency for Network and Information Security, 2015) They have published two exercise reports in 2012 and 2015, but unfortunately most of the data is already outdated.

Similar research was conducted for the public sector by researcher Hanna Heikkinen in 2019 from Jyväskylä University. Heikkinen's research topic was to understand the current state of the cyber exercises in Finnish public sector organizations. Heikkinen’s research results will be compared to these thesis research results. (Heikkinen, 2020)

Antti Kurittu (2020) has created a cyber exercise guide for the NCSC-FI, and he was researching the usability of the cyber exercise guide for organizations. The thesis was completed in 2020 for Laurea University of Applied Sciences.

3.4 Research ethics and data protection

The researcher has been following Ethical Principles for JAMK University of Applied Sciences (JAMK), which have approved by the Student Affairs Board in 2018. The researcher endorsed objectivity, honesty, and academic research community spirit.

The contract and non-disclosure agreement (NDA) was signed by the researcher, a representative of the NCSC-FI, and Jyväskylä University of Applied Sciences. The researcher had an in-depth discussion concerning the data processing, saving the data, the public nature of the thesis, and the communication tools before starting the project.

After mutual agreement, officially licensed Microsoft Office tools were used for communication and a separate tool for data saving and transfer, which met the requirements for the NCSC-FI. The data were transferred via secure mail between the researcher and the NCSC-FI. The data was only available for personnel who participated in this project, including researchers and representatives from JAMK and the NCSC-FI.

All the parties also understood that approved thesis are published in the public domain in Theseus Open Repository of the Universities of Applied Sciences, so they can not contain any non-public information, and they cannot be used for any criminal purposes. The NCSC-FI had an opportunity to read the thesis before the approval process and ask for needed edits.

The research has been conducted mainly using publicly available material, except the ISO standards, which need to be purchased to access the information. Bibliography and citations have been added accordingly, following JAMK guidelines when referencing other researchers and sources. Reference Manager & Citation Generator Mendeley Site was used to generate bibliography and mark citations. The Mendeley Cite is recommended and licensed by JAMK.

Personal Identifiable Information (PII) was gathered for people who participated in the interviews. The information included the name, email address, and phone number. It is possible that transcribing can also reveal the name of the person interviewed. The data has been processed according to General Data Protection Regulation (GDPR), and the list of personal information was deleted after the interviews took place and replaced with the organization name. The research data is all anonymized. The research data has been saved to guarantee confidentiality and integrity. The research data is anonymous, and interviewees cannot be identified.

All interviews were conducted online because of the problematic COVID-19 situation in Finland. The government recommended remote working to avoid infection. Participation in this research was voluntary for all interviewees, and they had an opportunity to decline the written interview invitation and cancel the interview during it. The interviews were mainly done via officially licensed Microsoft Teams and Google Meet video conference tools, and interviewees had an opportunity to choose if they had their cameras on during the interview. The interviewees also had the opportunity to decline the use of the information they had already given. The researcher worked at the time for Nixu and it was also informed to participants and reminded that there is no need to communicate any business secret that they may not want to share and they can skip any questions if they feel uncomfortable.

Overall, the researcher promoted the responsible conduct of research during the whole project timeline from start to end.

4 Cyber exercises as a tool building organizational cyber resilience

Pentagon identified four different operational domains for military conflicts many years ago - land, sea, air, and space. The fifth one, cyberspace, has been added to operation domains after our society has become more reliant on technology and when it was understood that military operations in the cyber domain have become real threats and can cause deaths of people. For instance, attacks from another country can occur in any of these domains after the unintentional or the intentional provocation of another country. In the past, we have already observed organized cyber-attacks from state-sponsored actors such as Russia, China, and Iran. In 2017, Russia attacked cyberspace in Ukraine with NotPetya malicious software that caused disruptions in many governmental and private sector organizations, not only in Ukraine, but globally. The loss for the organizations were counted in billions of dollars. The impacts of the cyber-attack are often eye-opening for many organizations and those usually awaken the organizations to get started with their cyber defense and to build and use more secure systems. (Welch, 2011)

Cyberspace is the only domain made by humans, and it is embedded in all others. Therefore, all issues should be able to change and manage by humans. The matters in cyberspace are more concrete and easier to repair if compared, for instance, climate change. Our goal should be aiming for cyber peace, where criminal actors have no possibility and interest in attacking anyone anymore through cyberspace. It would mean good collaboration and knowledge sharing between the public and private sectors, investments in security, excellent and creative methods, and solutions. Each organization shall promote the best security practices for their staff personnel and avoid the organization-wide solution that causes more harm than good. Proactive work for a more secure world shall be started as soon as possible as it is estimated that the digital economy grows over 30 % faster than the rest of the economy and MC Kinsey (2018) forecasts that 98 % of the economy is being impacted by digitalization. Some challenges in cyberspace are technical but often possible to solve by investment in advance. Currently, it seems the investment in cyber security is typically done after incidents and only when severe impacts are understood. (Clarke & Knake, 2019; Novak et al., 2018, 5-12)

Cyberspace has its differences and similarities to the other four domains. One of the main differences is that all other four operational domains have geophysical nature. The land is surrounded by the sea, and the air surrounds the land and oceans, and the air is surrounded by the space domain. Cyberspace is embedded in all and is humanmade, and it is continuously developing and evolving. Another difference is that threat actors can destroy part of cyberspace, but they cannot destroy parts of the other domains. One of the similarities is that all domains are dependent on technology. (Welch, 2011)

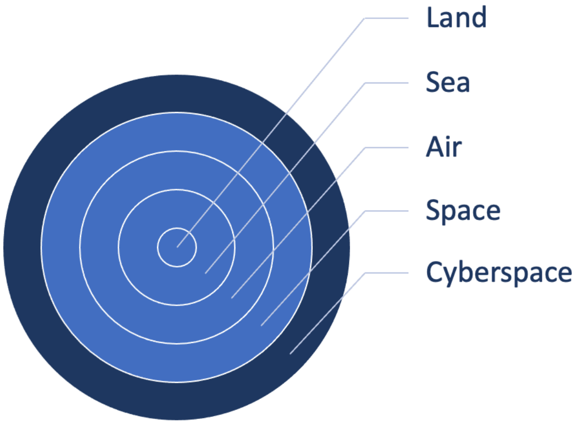


Figure 9. Cyberspace is embedded in all domains, and operation in all domains is dependent on operation in cyberspace. (Welch, 2011)

Cyber security has become a mainstream topic in the news and daily conversation, especially for management of companies. Typically, we can mostly hear and read negative news, headlines such as a company has been hacked, or critical infrastructure such as the power grid of a country has been attacked. Cyber security is a relatively a new topic and word. To this point, the industry has not been able to conclude what is the correct way to spell the word. Is it cybersecurity, or could it also be spelled as cyber security? The meaning of the description of cyber security varies depending on the source. For instance, the definition of information security and cyber security is often the same, and sometimes there is a slight difference.

The National Institute of Standards and Technology (2021) describes cyber security as *"the ability to protect or defend the use of cyberspace from cyber-attacks."*

The International Telecommunication Union also known as ITU (2022) describes cyber security as follows: *"Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity, which may include authenticity and non-repudiation, and Confidentiality."*

ITUs' general security objectives for cyber security are the same that are known as the CIA triad, which is considered the industry standard for information security. Confidentiality means that organizations must preserve their data private, and they must prevent unauthorized access. Integrity contains accuracy and reliability of the data so the data can be trusted, and integrity is not compromised intentionally or unintentionally. Availability means that the data must be available when needed. (Whitman & Mattord, 2012, 8) The CIA triad is often displayed in a triangle as seen below in Figure 10.

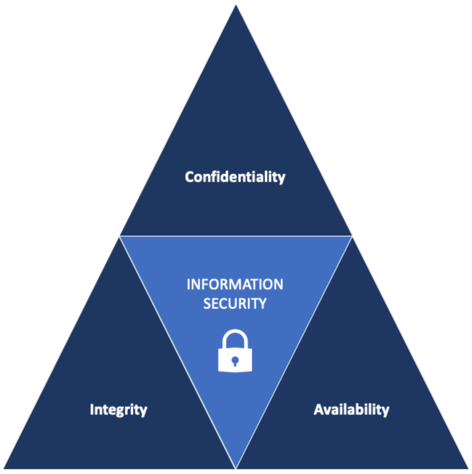


Figure 10. CIA triad for information security

The ISO management system standards mainly describe information security management via the CIA triad. However, they have developed, in 2021, two new cyber security-related frameworks: *ISO 27110,* Information technology, cyber security, and privacy protection – Cyber security framework development guidelines and ISO TS 27100, Information technology – Cyber security – Overview and concepts. Both frameworks aim to help organizations with them to become more cyber secure. (International Organization for Standardization, 2021)

Rossouw von Solms and Johan van Niekerk (2013) claim that cyber security and information security are not a synonym. They have created their own scenario in which they prove that it would be rational to assume that cyber security incidents could also be described in terms of the characteristics used to define information security. Through the chosen scenarios, they prove that incidents are not always led to a breach of confidentiality, integrity, or availability of information. Scenarios include cyberbullying where the target is a human, home automation, for instance, turning off hot water and the target often is a device, and sharing and copying movies and music where the target is digital media. They describe that assets can be many different matters from personal assets to assets of critical infrastructure such as energy or water. The common fact is that all these utilities from household lights to water system can be reached nowadays via cyberspace. Figure 11 displays the difference between information security and cyber security the according von Solms and Niekerk.

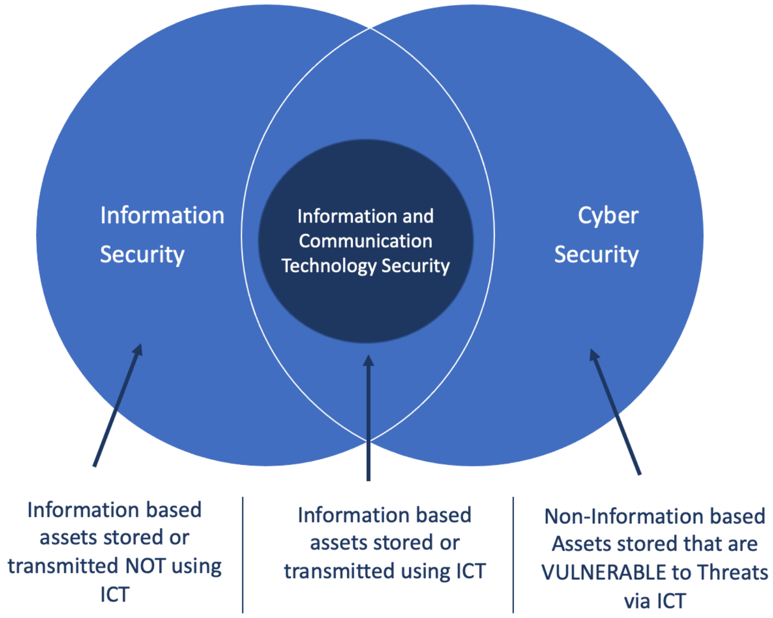

Information Security
Information and Communication Technology Security
Cyber Security
Information based assets stored or transmitted NOT using ICT
Information based assets stored or transmitted using ICT
Non-Information based Assets stored that are VULNERABLE to Threats via ICT

Figure 11. The relationship between information and communication, information security, and cyber security. (adapted from von Solms & van Niekerk, 2013)

For many countries, cyber security has been one of their top priorities for many years, and over 100 countries worldwide have created cyber security strategies and assigned millions from government budgets to develop their cyber security capabilities and defenses, especially for national critical infrastructure organizations (The International Telecommunications Union (ITU), 2022)

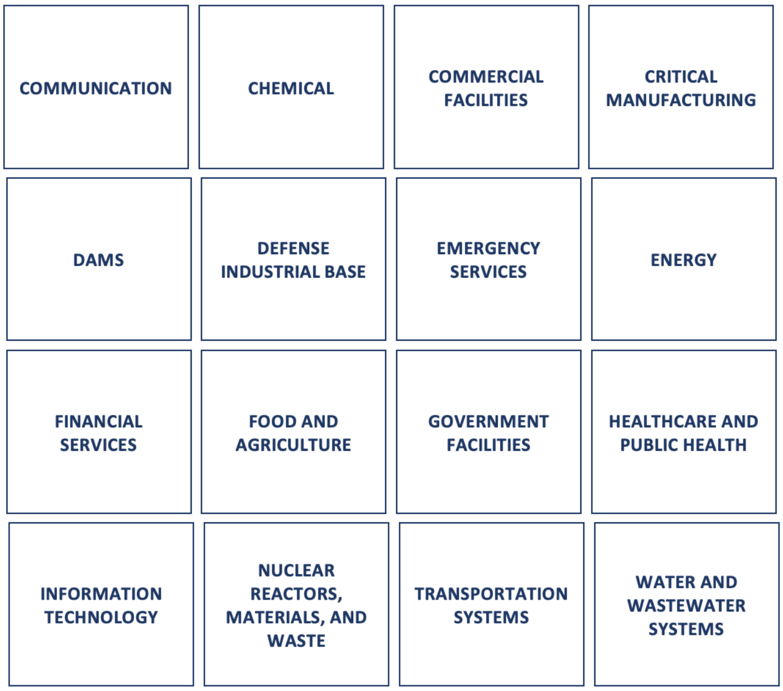
For instance, the USA established in 2018 The Cyber security and Infrastructure Security Agency (CISA), which is a federal agency under the Department of Homeland Security oversight. CISA also coordinates the execution of the USA's national cyber defense, leading ability response to significant cyber incidents and ensuring that timely and actionable information is shared across the public and private sectors. (Cyber security & Infrastructure Security Agency, 2022.)

In conclusion, von Solms & van Niekerk (2013) states that cyber security is far more wide-ranging that just ICT security and humans have a large role in it and current guides and frameworks are not enough to keep the cyberspace secure.

Some companies have already noticed that good cyber security is a competitive advantage for them and their customers. They can build trust and keep the data of their customers safe. Customers are either individuals or commercial clients. Large companies such as Apple, Google, and Microsoft have large security teams and budgets to develop their cyber security capabilities. Some of the companies' solutions have been created by the military and are slowly becoming available for other organizations. (Clarke & Knake, 2019, 8-9)

4.1 Critical infrastructure

An organization has either digital or physical systems, assets or networks. These can be deemed as critical infrastructure when any harm to them can cause a crisis to public health and/or safety and to the security of the national economy. (Cyber security and Infrastructure Security Agency, 2020) For instance, in the USA, CISA has identified 16 sectors introduced in Figure 12.



COMMUNICATION	CHEMICAL	COMMERCIAL FACILITIES	CRITICAL MANUFACTURING
DAMS	DEFENSE INDUSTRIAL BASE	EMERGENCY SERVICES	ENERGY
FINANCIAL SERVICES	FOOD AND AGRICULTURE	GOVERNMENT FACILITIES	HEALTHCARE AND PUBLIC HEALTH
INFORMATION TECHNOLOGY	NUCLEAR REACTORS, MATERIALS, AND WASTE	TRANSPORTATION SYSTEMS	WATER AND WASTEWATER SYSTEMS

Figure 12. Example of critical infrastructure sectors in the USA (Cyber security and Infrastructure Security Agency, 2020)

In Finland, the NESA is responsible for strengthening the capabilities, especially for the critical infrastructure organizations, for possible crises and disruptions. One of their main aims are to develop the business continuity management tools for securing the critical infrastructure organizations so that society and businesses can function, and people can live their everyday life safely. (Huoltovarmuuskeskus, 2022.) NESA has identified a total of eight critical sectors for Finnish society seen below in Figure 13.

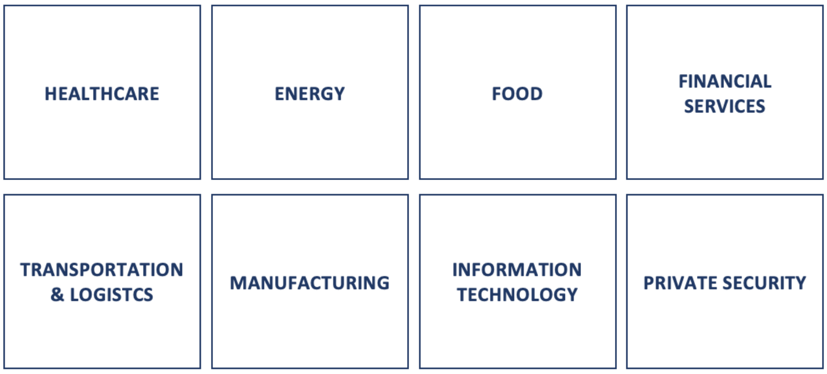


Figure 13. Critical infrastructure sectors in Finland (NESA)

4.2 Cyber threats

The European Union Agency for Cyber security (ENISA) has identified several high cyber threats for the organizations in their Threat Landscape (ETL) report. The main threats are displayed in Figure 14. ENISA describes the threat as *“any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.”* (European Union Agency for Network and Information Security, 2022)

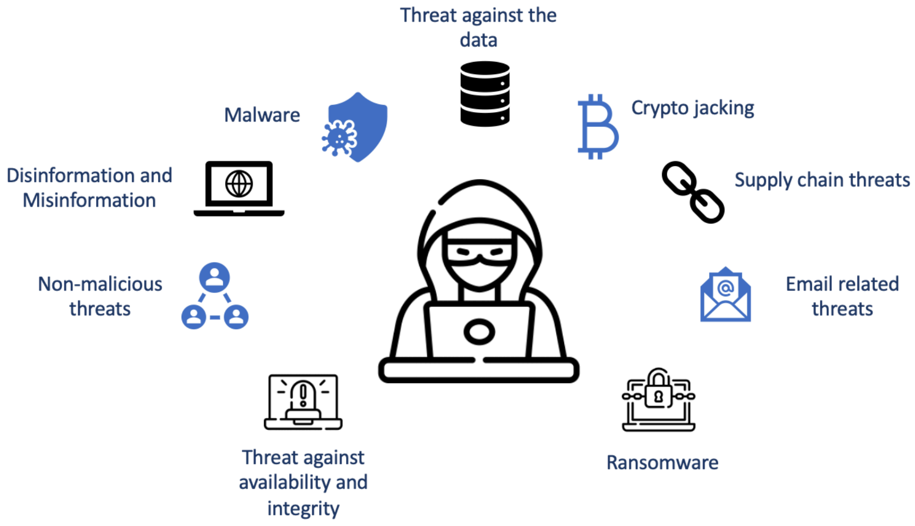


Figure 14. Top Cyber Threats identified by ENISA (adapted from European Union Agency for Network and Information Security, 2021)

We have observed globally many attacks against critical infrastructure. For instance, Israeli water systems have been under attack several times in the past, and the aim of the threat actor was to disrupt the pumping stations and sewer systems and poison the water with chlorine. In Ukraine in 2016, the power grid was attacked, and half of the population were without electricity in the middle of the winter. (Weinberg, 2021)

Microsoft has been closely working with the Ukrainian government during the war in the spring and summer of 2022, and they have been openly publishing the lessons learned since the kinetic war in Ukraine started by Russia. There have been many types of attacks, such as wipers which are meant to destroy all data but only in Ukrainian networks, without the possibility to recover it. Microsoft has published that Russia has been conducting operations in at least 43 countries in 2022, and the United States has been their number one target. The increasing numbers of attacks have also been observed in the Baltics and the Nordics, including in Finland. (Microsoft, 2022)

There has been several publicly noticed cyber-attacks against financial institutions and government organizations in Finland. For instance, on April 8th, 2022, the day when Ukraine's president Mr. Zeleskiy hosted a speech to the Finnish Parliament. Just before the online broadcast, the government websites, including the Ministry of Foreign Affairs, the Ministry of Defence of Finland,

and Finlandabroad.fi websites were attacked by the threat actor and websites were unavailable for the public to use. At the same time also, financial services had issues, and their customers could not access their banking services as usual. (Ilta-Sanomat, 2022b, 2022a)

Cybercrime has been rising in recent years, and cyber criminals are innovating their attack methods quicker than many organizations can develop their defense capabilities. That makes organizations easy targets. Cybercriminals are often hard to track as they understand well how to protect their identity. The public sector is trying to support the private sector with the development, for instance, with research, best practices, guides, and so on. (Clarke & Knake, 2019, 5-12)

The COVID-19 pandemic accelerated cybercrime, and insecurity brought new attacks to the daylight. According to a study, there were, on average, 270 attacks (unapproved access of data, systems, services, networks, or devices) per organization in 2021. Attacks increased by 31% compared to the year before. The increase of both attempted and successful attacks is showcased in Figure 15. (Accenture, 2021)

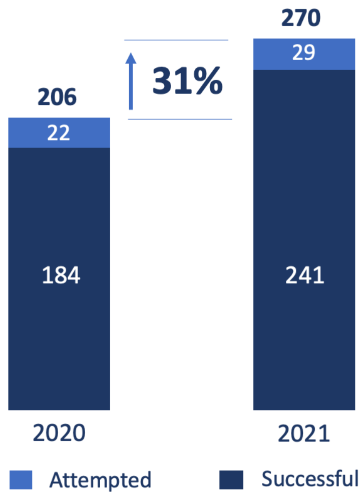


Figure 15. Average cyber attacks per company have increased by 31% from 2020. (Accenture, 2021)

Cyber security threat actors have different motivations. Typical cybercriminals are often motivated by money, but state-sponsored actors have different motivations. They usually conduct cyber espionage operations, for instance, to steal information to use in their intelligence services and cause damage not only to other organizations but also to people. During the COVID-19 pandemic, the state-sponsored actors have been especially interested in COVID-19-related information, such as treatments. The state-sponsored actors have also been attacking the supply chain of the organizations in the past two years. (European Union Agency for Network and Information Security, 2021)

For many organizations, ransomware has become one of the biggest cyber threats, and it is also a threat to national security in every country. Ransomware is a type of malicious cyber-attack where criminals lock the data of an individual or organization and require payment from an entity to return access. Criminals may also steal an organization's information and demand additional fee in return for not disclosing the information to authorities, competitors, or the public. (Barker et al., 2022)

Cybercriminals have created business models such as Ransomware as A Service (RaaS). RaaS is a model which is based on subscriptions, and that enables affiliates to use existing ransomware tools to deploy the attacks. In 2020, over 30% of ransomware attacks were conducted via RaaS. One of the main targets for cybercriminals latterly has been cloud services. Many organizations have been moving the data to cloud services, but the risks of data getting exposed have not been appropriately mitigated. (European Union Agency for Network and Information Security, 2021)

For an organization, the data breach can cost an average of 3.6 million US dollars per incident, and it takes 40 weeks on average to notice and react to a cyber-attack (IBM, 2022). According to the study, both demands, and payments have been rising. The average ransom demand rose 144% to 2.2 million US dollars, while the average payment rose 78% percent to 541,010 US dollars. (Paloalto, 2022)

ENISA (2021) has identified that healthcare, transportation, and energy sectors have been the most attacked critical infrastructure sectors. In the current geopolitical situation, cyber operations are driven by state strategies, the tension between countries, and armed conflicts.

Microsoft is one of the only reliable sources that has published data concerning the cyber operations in 2022 in Ukraine. It identified that Russia has been penetrating networks and cyber operations outside Ukraine, and 19% of them have been targeting the critical infrastructure which are displayed in Figure 16. (Microsoft, 2022)

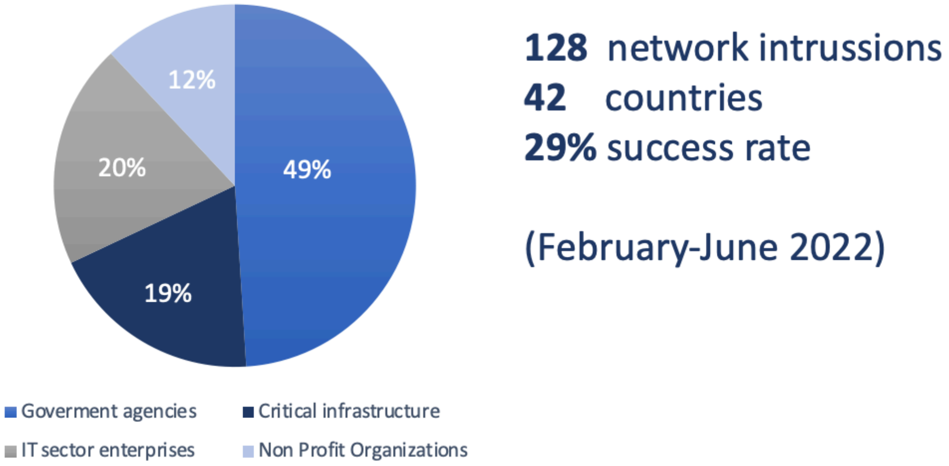


Figure 16. Recent Russian network penetration and cyber espionage operation outside Ukraine, including intrusion targets. (Microsoft, 2022)

4.3 Business continuity

One of the operational capabilities of organizations is business continuity (BC), which means that organization has an existing plan to manage out-of-ordinary situations so that it can continue its critical business function with the minimum disruption possible before, during, and after the incident. It is not only the cyber incident that can cause the interruption, but it could also be a utility outage, such as an organization does not have access to electricity, water, or internet. The disruption can be caused not only by cyber issues but also, for instance, natural disasters, technology, and human. The business continuity plans typically focus on technical solutions and challenges. (The Business Continuity Institute (BCI), 2022.)

A good example of disruption was the COVID-19 pandemic, which forced many employees of organizations suddenly to work from home. Many organizations needed to ask themselves; can their staff members perform necessary tasks from home, and do they have mandatory hardware and systems available to work with at home? (Burch et al., 2021)

Many organizations, such as NIST and the International Organization for Standardization (ISO), offer the best practices for organizations to get started with their business continuity planning. They have set the best practices and requirements for organizations to implement, maintain and develop their business continuity. Typically, business continuity planning starts with risk assessment, which means that organizations understand their potential threats and analyze what the disruption impact could be on daily operations. The threat list shall contain all threats that potentially impact the daily operations. (Swanson et al., 2010; ISO 22301:2019.)

In Finland, NESA (2022) has created tools and methods, especially for critical infrastructure entities, and they define business continuity as a process that improves the security of the supply chain for any kind of organization, either in the public or private sector. The aims of the business continuity process are:

- identify business threats, risks, disruptions, and dependencies
- understand the effects of the threats on the organization and its operator network
- organize and implement operating procedures in the event of disturbances
- ensure the ability of critical associates to function during disruptions
- protect its business functions and value-creation capacity.

Continuity management is only mandatory for some industries due Finnish legislations to guarantee the continuity of business operations in abnormal situations. (National Emergency Supply Agency, 2022.)

4.4 Building Organizational Cyber Resilience via Cyber exercises

The terminology used to concern cyber exercises can sometimes be confusing. Exercises are often named either cyber exercises or cyber security exercises, but they may have another name depending on what methodology is used and what type of exercise is the focus. (European Union Agency for Network and Information Security, 2012) Based on ISO-22398 standard and involvement from subject matter experts, the typical types of exercises are capture the flag, discussion-based game, drill, red team / blue team, seminar, simulation, tabletop, or workshop.

Homeland Security Exercise and Evaluation Program (HSEEP) defines the cyber exercise *as "a planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to, or recovering from the disruption. "* (Homeland Security, 2020)

MITRE Corporation defines the exercise as *"a simulated wartime operation involving planning, preparation, and execution that is carried out for the purpose of training and evaluation."* MITRE Corporation is an American company that consults the federal government in engineering and technical matter and is a respected organization in information security. (Kick, 2015)

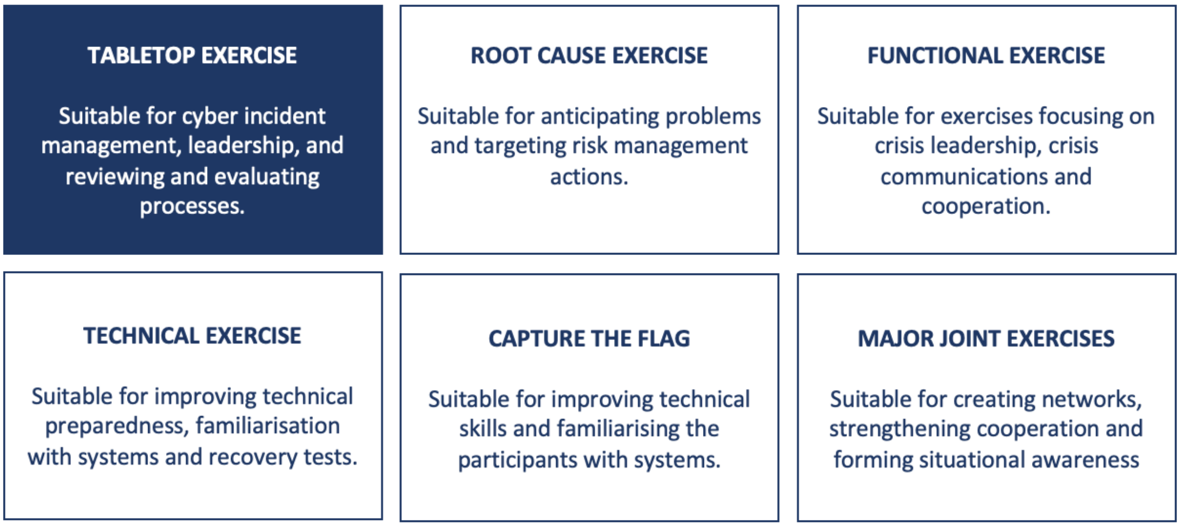
SANS Institute, another valued organization offering cyber security advice and training for organizations and individuals, describes the cyber exercise as an event where participants are placed in a fictitious situation or scenario that can be caused by a cyber threat or a situation that is difficult to handle for the organization. Then the participants must train how to handle the situation. The scenario could be, for an example data breach or denial-of-service attack that prevents the system from being used commonly. (Risto, 2015)

The cyber exercises are always fictitious, and they should never result in actual harm to organizations during the simulated events. The only impact should be that participants are absent during the exercise, and it demands time and effort to organize. (The Club de la Continuité d'Activité (CCA) & French National Cyber Security Agency (ANSSI), 2021)

As showcased in above, the naming of the cyber exercise is not standardized. The name depends on who is discussing the cyber exercises, and the term can also include the type of exercise. ENISA (2012) uses the same categories as the ISO-22398 standard: capture the flag, discussion-based game, drill, red team / blue team, seminar, simulation, tabletop, or workshop.

The government of the State of Victoria in Australia has created a handbook concerning cyber exercises. They have categorized the cyber exercises into two types: discussion and functional exercises. In the first one, the participants respond to imagination cyber incident with discussions, and in the functional exercise, participants respond operationally. The functional exercise demands an operational environment, usually a technical environment such as RGCE. (Victorian Government Cyber Incident Response Service, 2019)

The cyber exercise guide by the NCSC-FI has identified six different types of exercises which are presented in Figure 17 below. These categories are based on international benchmarks. In this thesis, the focus is on tabletop exercises which often are named discussion-based exercises without technical environments. (Traficom, 2019a)



TABLETOP EXERCISE

Suitable for cyber incident management, leadership, and reviewing and evaluating processes.

ROOT CAUSE EXERCISE

Suitable for anticipating problems and targeting risk management actions.

FUNCTIONAL EXERCISE

Suitable for exercises focusing on crisis leadership, crisis communications and cooperation.

TECHNICAL EXERCISE

Suitable for improving technical preparedness, familiarisation with systems and recovery tests.

CAPTURE THE FLAG

Suitable for improving technical skills and familiarising the participants with systems.

MAJOR JOINT EXERCISES

Suitable for creating networks, strengthening cooperation and forming situational awareness

Figure 17. The NCSC-FI has identified six types of cyber exercises in their guide (Traficom, 2019a)

The researcher noticed during this project that most of the guides that introduce cyber exercises that are publicly available information in mainly created by governments, institutions, and companies that consult the public sector. In many countries, including instance, USA, Australia, the UK, Sweden, and Finland public sector is creating cyber security services for organizations, and cyber exercise guides are one of them. Typically, these same guides also categorize the types of exercises, and they have sometimes referenced each other. For instance, the French Cyber Security Agency (ANSSI) promotes the importance of cyber exercises via the handbook “organizing a cyber crisis management exercise,” and it is targeted primarily at management. (The Club de la Continuité d’Activité (CCA) & French National Cyber Security Agency (ANSSI), 2021)

Most of the global and national organizations which offer tools for business continuity planning have recognized cyber exercises as one the most efficient tool to test the plans and readiness of the organizations. Many public organizations, such as ENISA, have been recommending regular cyber exercises for organizations to be part of their preparedness against cyber threats. ENISA issued its first recommendation in 2009 highlighting the importance of cyber exercises and has also organized several European-wide exercises since 2010, Cyber Europe being one of the biggest ones. In addition, they have been researching nearly 300 cyber exercises since 2002. (European Union Agency for Network and Information Security, 2010, 2015)

In the USA, the CISA Cyber Exercise Act was introduced and proposed to Senate in Autumn 2021. The aim was to establish the National Cyber Exercise Program to evaluate the National Incident Plan. The National Cyber Exercise Program became part of the US law in December 2021 as part of the National Defence Authorization Act and under section 1547. The part of the program is that CISA shall create example exercises that public and private sector organizations can utilize in their planning, implementation, and valuation of incident response plans and exercises. The program is targeted especially at the government and critical infrastructure organizations to improve their readiness. In section 1508, tighter public and private partnerships are planned, and section 1510 demands the Department of Defence conduct assessments to defend against the ransomware attacks and create a recommendation on how to deter and counter such attacks. The quick pass-through for the law has been the result of the recent severe cyber-attacks against their critical infrastructure in USA. (European Union Agency for Network and Information Security, 2012; National Defense Authorization Act for Fiscal Year 2022, 2021)

Previously, Homeland Security Exercise and Evaluation Program (HSEEP) in the USA have identified that exercises are one the crucial elements of national preparedness, and they have introduced the preparedness cycle. The cycle includes many same components that business continuity has, starting from identifying threats and identifying priorities and it has the common aim to evaluate and improve. The preparedness cycle is presented in Figure 18. (Homeland Security, 2020)

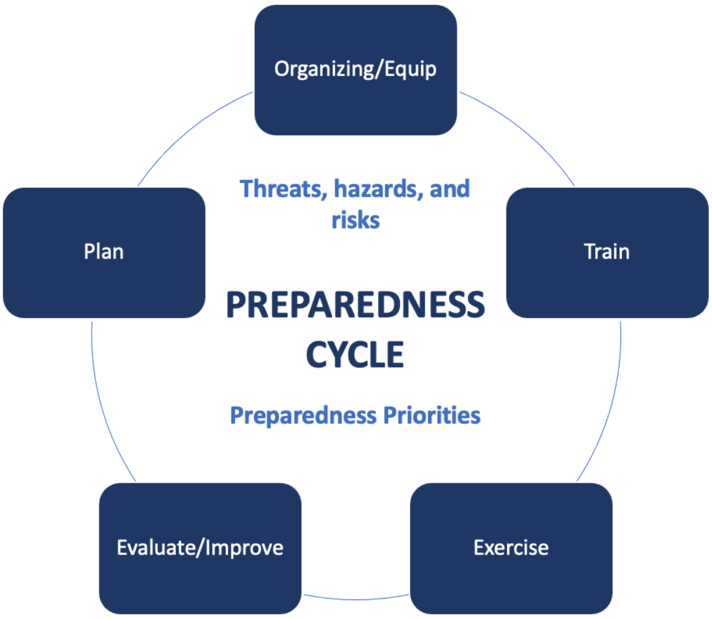


Figure 18. The Preparedness Cycle by HSEEP (Homeland Security, 2020)

The Victorian Government Cyber Incident Response Service and the Victorian Government Cyber Incident Management Plan have been recommending that their public sector bodies undertake at least an annual cyber exercise to improve their incident response capabilities. (Victorian Government Cyber Incident Response Service, 2019)

Militaries all over the world are known for the exercises they perform on a regular basis to maintain and learn new skills since the military forces have been formed. Organizing and participating in the exercises are one the ways to prepare for the real-life situation that may interrupt our society's life. In these exercises, knowledge is shared, and it is also an opportunity to learn new skills and keep the personnel ready for the disruptions which typically come unexpectedly. (Skripnichuk, 2015)

The benefits of cyber exercises have also been recognized in Finland. The Jyväskylä University of Applied Sciences has been a forerunner in organizing technical cyber exercises with their RGCE platform. The RGCE platform has been funded by European Regional Development Fund (ERDF) and several other entities since 2011. (JYVSECTEC, 2015)

One of the most significant projects for NESA since the late 1980's has been to organize major exercises for different critical infrastructure sectors biannually. The exercise is the most extensive exercise in Finland, and the main objective is to test collaboration between the public and private sectors in a situation where cyber-related issues disrupt normal activities. (National Emergency Supply Agency, 2020) The investment for the NCSC-FI exercise services was budgeted by NESA, so it is logical that critical infrastructure organizations are in the core target audience (National Emergency Supply Agency, 2021).

The benefit of the cyber exercise depends on its objectives and scope. The overall objective typically is strengthening how the organization responds effectively to a cyber incident to minimize the impacts such as financial, operational, and reputational. (The Club de la Continuité d'Activité (CCA) & French National Cyber Security Agency (ANSSI), 2021)

When starting to plan the exercise the question why the exercise should be conducted shall be asked. The purpose for the exercise could be for instance,

- understand how collaboration works between internal and external stakeholders such as IT, communication, management, and legal & compliance,
- test the plans such as the business continuity and crisis communication,
- develop cooperation between management levels,
- test routines and systems,
- practise keeping the situational awareness of the incidents,
- sharing knowledge between crisis management team and their substitutes. (The Swedish Civil Contingencies Agency (MSB), 2016).

The benefits for the organizations are the improvements and learnings in numerous areas. Organizations will understand the problem areas better, they gain new ideas to update their processes and plans, identify missing documentation, strengthen the cooperation between stakeholders required in crisis management, key personnel understand their roles and responsibilities better for instance who is responsible for certain decisions. (The Club de la Continuité d'Activité (CCA) & French National Cyber Security Agency (ANSSI), 2021)

DNA, a Finnish telecommunication group, participated the TIETO20-exercise and through the exercise, they now can understand their role and criticality in the entire supply chain of service production in the whole society. A discontinuity situation in the telecom industry could at worst even paralyze many operations, and the difficulties would be reflected as multiple impacts on the rest of society. The further our society becomes digitalized, the more far-reaching the disruptions to the operator's operations would be. (Vartiainen, 2022)

Fingrid, the transmission system operation in Finland, has been participating and organizing cyber exercises for many years. They have learned useful lessons via exercises; figured that they have improvements areas in communication coordination. Exercises have made the cyber threats more realistic. Their employees can now understand how the cyber-attacks occur and how better to defend against them. Another benefit has been that the organization now understand that cyber security crisis management is not only concerning technical capabilities to defend the assets. The communication and decision making have large impact on the result and must be successful in the incident situation. (Pajunen, 2017)

The organization receives the after-action report after the exercise, and it includes the observation including strengths and areas for improvements. Organization shall start the improvement planning process and turn the recommendation to concrete actions. (Homeland Security, 2020)

The development of preparedness of organizations and companies for cyber-attacks and developing cyber security skills of professionals are both parts of Finland's cyber security strategy, which the Security Committee has created. The Security Committee published the first version of the cyber security strategy in 2013, and it was reviewed and updated in October 2019. The new version is setting three national targets for the development of the cyber environment and for securing critical functions:

1. development of international collaborations,
2. improved coordination in cyber security management, planning, and preparedness,
3. development of cyber security skills.

The first goal concentrates on international collaboration between nations and organizations such as United Nations (UN), Organization for Economic Co-operation and Development (OECD), and co-operation in Europe (OSCE). Cyber threats and attacks are global issues without country borders, and it is essential to co-operate with other countries and share information and knowledge. (Secretariat of the Security Committee, 2019)

The second goal underlines especially the collaboration between public and private partnerships, in topics such as preparedness, business continuity, and situational awareness. The Ministry of Transport and Communications appointed a new role of Director of Cyber security. Roles' responsibilities include coordination of the development, planning, and preparedness of cyber security. The Director of Cyber Security also acts as an advisor to the state administration in all cyber security-related matters and strengthens the relationships between public and private organizations and companies. (Secretariat of the Security Committee, 2019; The Ministry of Transport and Communications of Finland, 2020) The Director of Cyber Security has been participating the cyber exercises, he was leading the Finnish State Administration National Cyber Security Exercise in 2021 (KYHA21VH) (Lötjönen, 2021).

The third goal is to strengthen our national cyber security skills in daily lives among citizens and cyber security professionals. All areas of Finnish society, including public and private sectors, need cyber security skills. Continuous education, training, and research for everyone are vital for learning these competencies. Cyber exercises are part of the training of the cyber security professionals. (Secretariat of the Security Committee, 2019)

Investments by Finnish government has been witnessed also in other areas. DVV have done research concerning cyber exercises in recent years and has been hosting one of the largest annual cyber exercise TAISTO in Finland since 2018. The exercise is targeted especially for public sector entities. TAISTO exercise remains in the schedules also for year 2022. TAISTO, TIETO and KYHA are the most important cyber exercises organized in Finland according the DVV report published in 2020 as seen in the Figure 19. (Heikkinen, 2022)

NESA (2021) has provided funding for DT2030 projects until 2030. The previous project KYBER2020 was set for three years which started the NCSC-FI exercise services which are introduced in the section 2. The DT2030 includes funding for four projects supporting cyber exercises and the NCSC-FI is the main partner for these. The projects are:

1. The NCSC-FI exercise service development,
2. cyber exercises for critical infrastructure sectors in Information Sharing and Analysis Centre groups (ISAC),
3. organizing national TIETO-exercise biannually,

4. Health Care Cyber Range, the extension for JAMK RGCE to model healthcare systems and processes to organize sector specific cyber exercises.

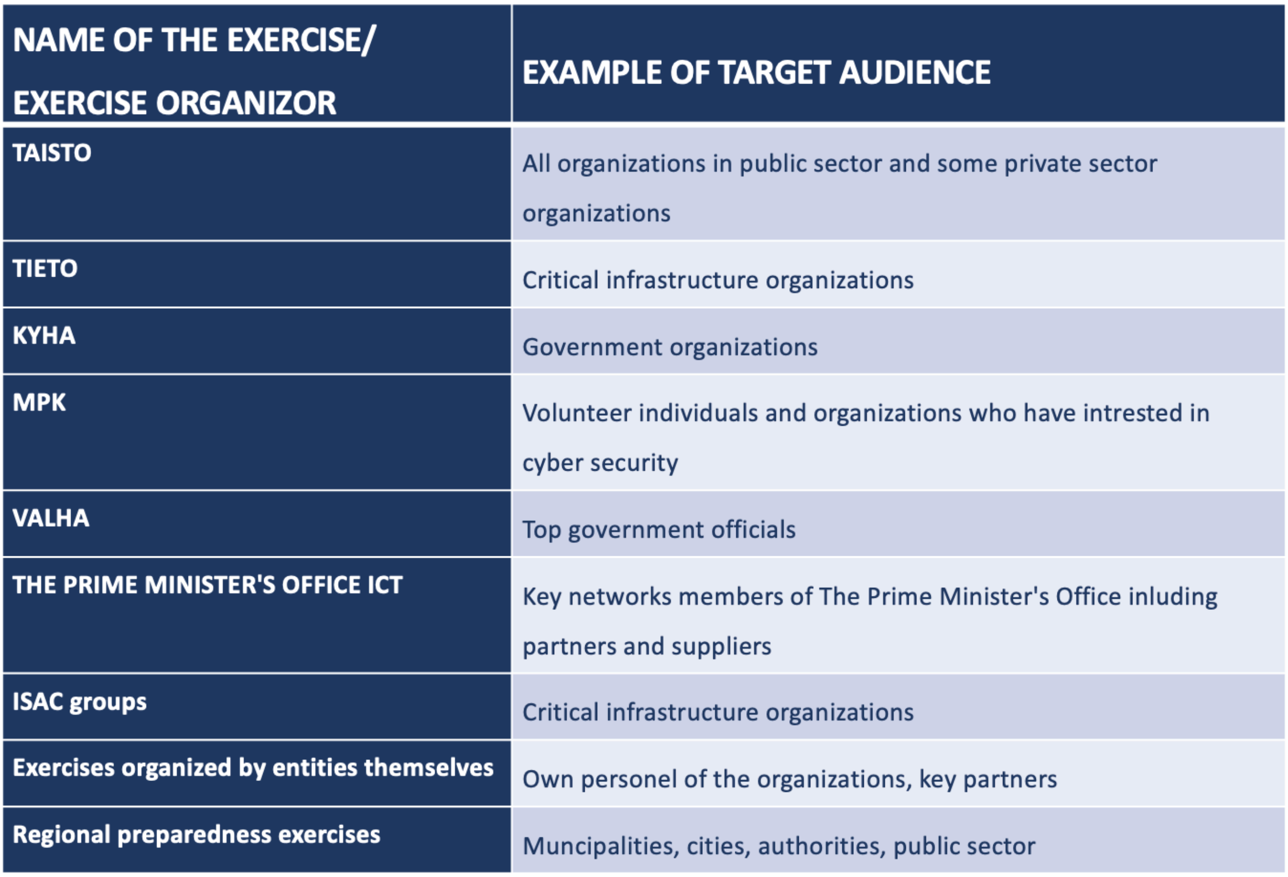
ISAC groups have been established by the NCSC-FI and the purpose for the groups is to share information and knowledge to protect their assets against cyber threats. Currently there are eleven active sector specific ISAC groups. All groups are created for critical infrastructure organizations. (Traficom, 2021a)

The Finnish government is not providing the annual budget for NESA even though NESA's objectives and funding are written into law. Instead, NESA is managing the National Emergency Supply Fund which covers the security of supply cost. NESAs role is between public and private sector. (National Emergency Supply Agency, 2022.)

The National Defence Training Association of Finland (MPK) has been organizing cyber exercises for over ten years for Finnish citizens and reservists. The exercises are part of the cyber security training path that any Finnish citizen can apply to. MPK has been a participant to the global exercises such as Locked Shields. (Jalava et al., 2017) The Locked Shield is one of the biggest cyber exercises in Europe, organized by The NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) in cooperation with NATO and private companies. Locked Shields is a real time technical exercise where defending teams are competing on the Cyber Range. (The NATO Cooperative Cyber Defense Centre of Excellence, 2022)

The budget for MPK is provided by several sources, including the Ministry of Defense and by donations from private and public organization or even individuals. Finnish Defense Forces is a strategist partner of MPK, and they are ordering and compensating for the training courses which are targeted especially for reservists. (Jalava et al., 2017)

DVV has collected all the information concerning the known public sector exercises which are presented in Figure 19. The ISAC group exercises have been added, they were not standard exercise at the time the information was collected by DVV.



NAME OF THE EXERCISE/ EXERCISE ORGANIZOR	EXAMPLE OF TARGET AUDIENCE
TAISTO	All organizations in public sector and some private sector organizations
TIETO	Critical infrastructure organizations
KYHA	Government organizations
MPK	Volunteer individuals and organizations who have intrested in cyber security
VALHA	Top government officials
THE PRIME MINISTER'S OFFICE ICT	Key networks members of The Prime Minister's Office inluding partners and suppliers
ISAC groups	Critical infrastructure organizations
Exercises organized by entities themselves	Own personel of the organizations, key partners
Regional preparedness exercises	Muncipalities, cities, authorities, public sector

Figure 19. The known annual cyber exercises and organizers (adopted from The Digital and Population Data Services Agency's services, 2022)

JYVSECTEC has been organizing technical cyber exercises on their RGCE for several years and has been focusing mainly for public sector's technical exercises. The funding for the RGCE was given by European Regional Development Fund (ERDF) and private companies. (JYVSECTEC, 2015; Lötjönen, 2021)

Overall, the public sector has selection of exercises which are organized either annually or every second year. Some of the exercises remains confidential and public information is not available. Private organizations are sometimes invited to participate these exercises as seen in Figure 19. For instance, the international Cyber Europe 2022 organized by ENISA, had healthcare entities from public and private sector, including Finnish organizations. In total, over 800 professionals attended the event. (European Union Agency for Network and Information Security, 2022; Istekki, 2022)

Private sector is responsible to organize their own exercises. If they do not have a capability to produce them by themselves, there are several companies in Finland offering exercise consulting services. The NSCI-FI have published the names of the consulting companies and published articles concerning exercise experiences by private sector on their website. (Finnish National Cyber Security Centre, 2021)

4.5 Requirements and Compliance

The cyber exercises are not currently part of the Finnish Act of Parliament. However, there are several decrees that have exercises or trainings as part of the decree. Typically, trainings or exercises are mentioned as part of the planning for incident or risk management or business continuity. For instance, the Finnish Act of Parliament 1109/2015, lists the exercises in the eighth part, named preparedness. It states that, to ensure the continuity of the security network's services in normal conditions, in the event of disturbances, and in exceptional conditions, the service provider must, to the extent required by the requirements regarding high preparedness and security, in cooperation with other service providers and users if necessary: handle the staff training and incident training. (1109/2015) In addition, the Finnish Act of Parliament 683/2017 lists regular crisis situation rehearsing as a mandatory activity (683/2017).

Even though there is no national-level law, the importance of cyber exercises is a visible part of preparedness and risk management, especially for government organizations. For instance, Finnish cyber security strategy lists cyber exercises as one of the strategic activities and national competence development (Secretariat of the Security Committee, 2019). In addition, the DVV had a cyber exercise-related project since 2018, which for instance, included hosting the annual exercise named TAISTO for public sector organizations. In 2021, there were over 300 participating organizations in the exercise. DVV has also set objectives and actions for the national-level exercise program for 2021-2022. (The Digital and Population Data Services Agency’s services, 2022)

Private and public sectors are also joining forces in the exercises. For instance, the finance sector FATO exercise was organized by Emergency Supply Organization (HVO) in Autumn 2021, and it included participants such as the Bank of Finland, Finnish Financial Supervisory Authority, Financial

Stability Authority, and Finnish banks, which are part of the are critical infrastructure. A similar exercise was organized for the finance sector also in 2015. (National Emergency Supply Agency, 2021)

In addition, sometimes organizations must not only comply with the national laws and regulations, but there are several international standards in information and cyber security that require compliance from the companies. A good example is the finance sector, which is highly regulated in Finland (Financial supervisory Authority, 2022), and Payment Card Industry Data Security Standards (PSI DSS). PCI DSS is a set of requirements that aim to increase the security of payment card account data. It represents carefully chosen steps that give the companies the list of the best security guidelines (PCI Security Standards Council, 2009b). According to the PCI Security Council website, at least Nordea and Danske Bank, which both are operating in Finland and other market areas, are PCI compliant, which means they need to fill the requirement to comply, including security training for all company personnel. (PCI Security Standards Council, 2009a)

To summarize, currently, Finnish law does not require organizations and companies to organize or participate in mandatory cyber exercises in any given timeframe. (1109/2015) However, the international standards may bring other requirements, such as security training which can also be cyber exercise as it is one of the training methods in cyber security.

5 Research implementation

The research implementation was conducted in two separate parts. The first part was conducted by the NCSC-FI and the second part by the researcher. The first part was conducted by the NCSC-FI because they cannot share the contact lists and all data with the researcher. Non-disclosure agreement was signed at the start of the project, and it was cautiously agreed what can be included and published in the thesis and what data the researcher can handle and where is it stored during the project. The tools were chosen carefully which are presented in the section 3.4.

It was clear from the start that the cyber exercise business is a niche industry in Finland and that may limit the scope and results of this research project. After investigating the possible research methodologies, the theme research interview was the best option for the research objectives. According to Hirsjärvi and Hurme (2015, 35), the theme interview is an excellent method when interviewees can communicate by expressing their own experiences and show their subject matter expertise.

Other large benefits were that the informants can be decided by the researcher. Both, the researcher, and the chosen informants are subject matter experts in the cyber exercise area. The objective for the interviews was to gather new information that the researcher can then analyze and present new ideas to the NCSC-FI on how they could develop their own cyber exercise services. The answers are based on the experience of the informants when they have been either participating, organizing or being involved in the cyber exercise business in any other way.

The chosen subcategory of the chosen theme interview method was the semi-constructed interview method. It is a flexible method, where the theme is predetermined, and the interview can have standardized and preplanned questions. However, the interviewer has a flexibility to ask more open questions if necessary and the question order is not set. All general conclusions are only hypotheses, and the theme interviews were qualitative research which produced information only on the subject researched. (Hirsjärvi & Hurme, 2015, 47-48) A case study was considered as an alternative method for this project.

The project timeline was drafted at the start, and it included a total of ten various phases. The interview phase had subcategories for more in detail schedules. The research plan was drafted for the project which included three main parts: the problem, information gathering and then, planning of the actions which are presented in detail in Figure 20 below. The project plan was integrated to the research plan.

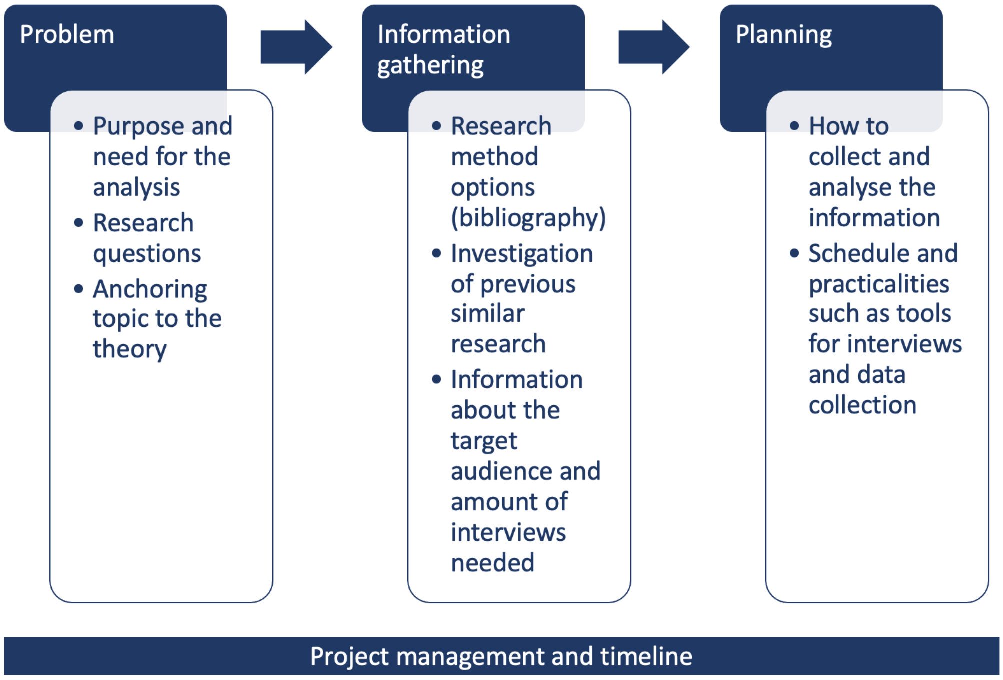

Problem
Purpose and need for the analysis
Research questions
Anchoring topic to the theory
Information gathering
Research method options (bibliography)
Investigation of previous similar research
Information about the target audience and amount of interviews needed
Planning
How to collect and analyse the information
Schedule and practicalities such as tools for interviews and data collection
Project management and timeline

Figure 20. The research plan phases

The target audience, the interviewees, were either cyber exercise organizers, participants or any relevant organization that is involved in the cyber exercise business in Finland. A total of twenty interviewees, were chosen but one organization was excluded because they had finished their cyber security exercise services. 17 interviews were conducted between November 2020 and April 2021. The response rate was 90 % which can be considered as an excellent response rate according to Gillman (2013, 14-15). The company which did not have cyber exercise services in their selection have also been excluded from this response rate figure.

When the plans were in place, the research themes were decided. The three chosen themes and related questions to each theme are introduced in Table 1. These themes and open questions should give enough source material for the researcher to analyze and give answers to the main research questions. Closed questions were avoided and open questions such as “why” and “what” questions were prioritized. “Why” and “what” are the questions for basic research and “how” is a main question for theoretical base for the research (Toikko & Rantanen, 2009, 19).

Table 1. The pre-planned questions for interviewees

Themes	Description
Challenges	1. What are the main challenges and reasons why it is so rare that organizations are not participating in cyber exercises? 2. What are the reasons behind organizations not being able to host their own exercises? 3. How can we overcome these challenges?
Role of NCSC-FI	4. What are the current cyber exercise services offered by the NCSC-FI? 5. What is the role that the NCSC-FI should have in the future of the Finnish cyber exercises industry? 6. Who should be partnering with the NCSC-FI exercise services?
Tools	7. Can you suggest any tools, such as “Exercise in the Box” in UK or guides and templates that the NCSC-FI should investigate in to more or could be used as a benchmark? 8. What kind of tools would be beneficial for your organizations that the NCSC-FI could offer? 9. Is your organization interested in using any tools that the NCSC-FI offers?

All interviews had the same theme which was cyber exercises. Depending on the background of the chosen interviewee, either all questions or part of the questions were asked. The questions were not asked in a certain order however they were asked during the natural conversation. Additionally, all interviews had extra questions by interviewer, which were not pre-planned. To note, interviewees also had questions for interviewer.

The researcher interviewed all interviewees herself. Hirsjärvi and Hurme (2015, 72) recommended that the interviewer should never have a personal relationship with the interviewee but in this project, it was impossible to follow this recommendation due to the minor industry network in Finland. The researcher personally was familiar with several interviewees in advance through her work. It was considered if someone else could host the interviews in absence of the researcher, but that idea was discarded because of the semi-structed format. If the theme interviews would have been structured, then a third-party host would have been hired to conduct the interviews.

5.1 Collection of Data

The COVID-19 pandemic restricted in-person interactions between people, so the in-person interviews were not an option. Only personal interviews were considered in this research, instead of group interviews. The group interviews were discarded as not a suitable method for the research, because they would have made analysing the results more difficult and then interviewees could have influenced other interviewees opinions and views. On the other hand, the result could have been richer when interviewees can discuss with each other and share their thoughts and opinions.

The interviewees received the invitation to the interviews via personal phone call or as an email. All interviews were scheduled several days after the first connection with the interviewee. After the time and date was scheduled, the interviewees received a calendar invitation to their work calendars. Most of the interviews were conducted via the video conference tool, Microsoft Teams, and only two were conducted over the phone. The duration of each interview was between 30 minutes to 120 minutes. Those interviews which were conducted via phone, were shorter in duration. All interviews were conducted in Finnish.

The researcher prepared for each interview carefully. A quiet room was chosen to host the interviews and tools such as microphone, camera and internet connection were tested in advance. Interviewer had all needed equipment previously, so interviews did not cause any extra cost. During one interview, there were technical disruptions due to a global outage in the chosen video conference tool. Otherwise, all interviews were hosted without technical issues. The interviews started with the introduction of either party and interviewer summarized in the beginning the reason for the meeting, objectives for the research, introduced the partner for the research and asked permission for a recording. If the interviewees where from the organization that was seen as a competitor to Nixu, the interviewer informed that there was no need to communicate anything that were company secrets or confidential information or any other information that would make the interviewee feel uncomfortable. All interviewees were informed they have an option to cancel or reschedule the interview. In most instances, the interviewer had very good discussions with the interviewee. For most of the interviewees, the topic was very close to their heart, and they were excited to share their thoughts and experiences.

After the interview, the interviewer thanked the interviewee for their participation and presented an estimation of the deadline for the research project and informed that if any personal references were needed for the research, they would receive information in advance and they would have possibility to approve it before publishing.

The number of theme interviews were relatively small however there were only a handful of people in the public and private sectors who work mainly with cyber exercises. All targeted key industry personnel were reached and interviewed. The questions were chosen for each interviewee by relevancy which meant that all participants would not answer every question which was known fact beforehand.

5.2 Analysis of data

The researcher considered multiple options to present the data. The options were for instance, grouping according to the theme, counting, and organizing the data with numerical statistics. The researcher in turn, used the counting system to categorize the data and to find common patterns, similarities, differences, and relationships between the data. The counting was done according to the number of times the phenomena were mentioned in each answer. The researcher created a frequency list in each theme which is presented below in Table 2. The frequency has been divided into three categories: low, medium, and high and percentage values are presented in the Table 2 below. The three themes for the analysis were challenges, role of the NCSC-FI and tools. The questions of each theme are displayed in the Table 1. Table 2 displays the frequency percentages.

Table 2. Subject frequency categories

Frequency category	Percentage (%)
Low	0,0 - 33,3 % of interviewees mentioned the subject at least once
Medium	33,4 - 66,7 % of interviewees mentioned the subject at least once
High	66,8 - 100 % of interviewees mentioned the subject at least once

A total of seventeen interviewees were interviewed. 71% of interviewees were representing the private sector and 29% were representing the public sector which is displayed in Table 3. The response rate was 90 %. Interviewees were chosen mainly from different organizations, but some organizations had more than one interviewee. All interviewees have a role in the cyber exercise business in Finland. They either organize, plan, participate or invest in cyber exercises.

Table 3. Comparison of public and private sector intervieewees

Organization	Percentage (%)
Private sector	71 %
Public sector	29 %

The first two questions are grouped together as they both have similar themes to their answer. The questions for the interviewees were: what are the main challenges and reasons why it is so rare that organizations are not participating in cyber exercises?

The most frequents answers recorded were, organizations do not understand why cyber exercises are important and what are the benefits of them, organizations do not have enough resources such as time and money and there is no support for management. The results are presented in Table 4.

Table 4. The results of the main challenges and reasons why organizations are participating the cyber exercise so rarely

subject	frequency	challenge
Organizations do not understand why cyber exercises are important	high	challenge
Organizations do not understand what the benefits of cyber exercises are	high	challenge
There are not enough resources within the organization including money, time**,** and people to execute the cyber exercises	high	challenge
There is no support for management for the cyber exercises	high	challenge
Cyber exercise has a negative image: it is not worth the return of investment	medium	challenge
The cyber exercise has a bad reputation. For instance, they are time consuming, and it is too difficult for organizations to get started on their own	medium	challenge
Cyber exercises are ad hoc projects and organizations do not create long term exercise plans	medium	challenge
It is too challenging and time consuming to participate in the cyber exercise, when the requirement is to learn to use a new platform	medium	challenge
There are no skilful people to host the exercises	low	challenge
Cyber exercises are no one’s responsibility for critical infrastructure organizations	low	challenge
All public sector organizations have their own agenda	low	challenge
A cyber exercise is too much of a stressful experience	low	challenge
The organizations do not know how to purchase the cyber exercise consulting service from a third party	low	challenge

When comparing the data between the public and private sector, there are several similarities even though in all the category lists importance is low. A high number of public sector interviewees mentioned that the main responsibility of cyber exercises for critical infrastructure organizations are not anyone's responsibility and participants of TIETO-exercises could provide their organizations a wrong image towards cyber exercises if it is the only exercise, they have ever participated in. TIETO is one of the largest cyber exercises organized in Finland and it has hundreds of participants. The duration of the project can be over two years for participants. (National Emergency Supply Agency, 2020) A high number of interviewees from the public sector mentioned that organizations have no skilful people to start the cyber exercises within their organization and they do not know how to purchase them from service providers. A high number of private sector interviewees mentioned that exercises should be conducted in their own environment instead of some unknown platform that exercise participants must learn even though they are using their own platforms when real incident happens.

Heikkinen has been researching the exercises for the public sector and shares similar findings. In 2018, 94,3 % of public sector organizations did not have enough resources to organize exercises and 13,3 % had reserved an annual budget for cyber exercises. Another finding was that only 5,7 % of the public sector organizations were using the private sector to organize exercises. (Heikkinen, 2020, 38-40)

The next question of the challenge category was to identify what the reasons behind organizations are not being able to host their own exercises. The results are presented in a visual format in Table 5. The highest frequency in the responses were that organizations are used to large exercises and consider it as their only format available. Other findings showed that participating to exercises draws too much organizational resources, exercises are too costly, and exercises has never identified as an important activity that it would have been added to annual strategy plans. TIETO exercise was also mentioned in this part several times as an example for a large exercise.

Table 5. Results of the reasons why organizations are not able to organize their own cyber exercises

subject	frequency	challenge
Organizations assume that large cyber exercise is only format	high	challenge
Cyber exercises are not continuous and part of the annual planning	high	challenge
Participating to exercises draws too much organizational resources	high	challenge
There is no time and money	high	challenge
Simulators confuse people and organizers think simulator tools are a must	medium	challenge
CISO has too much of an operational role and doesn't understand the business and real topics to improve	medium	challenge
There are no ready-made exercise paths where to get started	medium	challenge
NCSC-FI materials are difficult to find and there is no marketing for them	medium	challenge
No management support for cyber exercise	medium	challenge
Organizations are scared to fail, and they don't want to hear what they should develop	low	challenge
The same people are always participating the national exercises and they don't pass information on	low	challenge
Exercise is always the same and it is boring. Instead, there should always have surprise elements	low	challenge
CISO doesn't understand why exercising is important	low	challenge
Organizations do not want to use services which are created by NCSC-FI because they are considered as an authority	low	challenge
Cyber exercises are bad business for private organizations, and they don't actively offer their services	low	challenge
Lack of organizers especially for critical infrastructure	low	challenge

The last question for the challenge category was to find solutions and ideas on how we can overcome these challenges and the results are displayed in Table 6. The highest frequency was to support organizations when they are starting their exercise journey and to teach them different formats such a light tabletop exercise. The light tabletop exercise was mentioned by all private sector interviewees. Good and open communication has been seen as a positive change and TAISTO and TIETO, were both mentioned several times as an example. DVV was mentioned as a good example for their knowledge sharing attitude because they have published all TAISTO exercise materials on their public website and have created TAISTOmaatti, which is currently available for all organizations in DVV's learning platform eOppiva. (DVV, 2021)

One of the frequent answers given was that marketing should be increased to change the image of the cyber exercise from negative to positive. The information classification was another one the frequent subjects; the interviewees were wondering why the NCSC-FI is not sharing more threat intel and information of cyber incidents because they have all the information organizations need. According to the interviewees, this prevents organizations from learning from each other.

Table 6. Ideas and suggestiong to encourage organizations to participate in exercises.

subject	importance	challenge
Organize light and short tabletop exercise	high	challenge
Be more open about the cyber exercises, internally and externally (TAISTO and TIETO was used as an example)	high	challenge
Marketing (objective shall be to create a more positive reputation for exercises and understanding of the exercise formats)	high	challenge
Increase discussion about cyber incidents, threat landscape and to stop labelling everything as a secret	high	challenge
Support especially the organizations who are starting their exercise path	high	challenge
Identify the business areas that need the help the most with digitalization and create light tabletop formats	medium	challenge
Share knowledge about cyber exercise experiences from companies	medium	challenge
Include business services more often and motivate them excited about the exercising	medium	challenge
Gamify the experience	low	challenge
The companies that are running behind from digitalization shall be identified and conducting exercises could be one of the best tools to assist them to understand the cyber threats	low	challenge
Participant number should not be the key factors when hosting an exercise	low	challenge
Create a maturity model: what kind of exercises shall be hosted and when, what are the themes and when include partners and authorities	low	challenge

The second theme of the interview concerned the services and the role of the NCSC-FI in the cyber exercise business and the results are presented in Table 7, 8 and 9. The first question's aim was to understand if interviewees know what the current cyber exercise services of the NCSC-FI are. 53 % of interviewees knew one or two of the services, mentioning either scenario booklet or consulting. The scenario book was done together with the private sector while the rest of the services are offered by the NCSC-FI (Finnish National Cyber Security Centre, 2022). The private sector was better aware of the NCSC-FI services rather than the public sector and the smaller the company was, the more they use the services while the larger companies had their own tools.

Table 7. The results for the question, what are the current cyber exercise services offered by NCSC-FI

categories	percentage (%)
Interviewee does not know any of the services	18 %
Interviewee is aware of the whole service catalogue	29 %
Interviewee is aware of 1-2 services	53 %

The next question was what the role is that the NCSC-FI should have in the future of the Finnish cyber exercises industry. The most common answer was that the NCSC-FI should share more information with the private sector and collaborate with international organizations such as Computer Emergency Response Teams (CERT) and private entities. Several interviewees were wondering why the NCSC-FI is already actively collaborating with CERTs but the information is not shared with national peers. A high number of respondents were happy with the current services such as keeping the supporting role in the exercise and to focus on critical infrastructure organizations only. However, while consulting the organizations, those which are not categorized as critical infrastructure, shall be consulted to get started with their cyber exercise journey which is seen in Table 8.

Table 8. The results of the questions what is the role that the NCSC-FI should have in the future of the Finnish cyber exercises industry.

observation	frequency	theme
NCSC-FI should start sharing even more information especially with the private sector. Too much information is unnecessarily labelled as confidential	high	role of NCSC-FI
NCSC-FI should work closely with other public sector organizations such as DVV	high	role of NCSC-FI
NCSC-FI should have more international co-operations	high	role of NCSC-FI
NCSC-FI should actively benchmark their own services with international organizations	high	role of NCSC-FI
Focus only in critical infrastructure sector, while private sector is handling the rest of the organizations	high	role of NCSC-FI
Same role that they have now, only have a supporting role in cyber exercises	high	role of NCSC-FI
Consult the organizations that are starting with their cyber exercises	high	role of NCSC-FI
Support the cyber exercise services on national level	medium	role of NCSC-FI
NCSC-FI is seen as a regulator and not as an organization that consults other organizations. A regulator often controls and restricts the activities of private sector companies. This mindset should be changed	medium	role of NCSC-FI
Create a network for public and private sector cyber exercise service providers which gather to share knowledge and ideas	medium	role of NCSC-FI
NCSC-FI should organize cyber exercises	low	role of NCSC-FI
NCSC-FI should have only a supporting role, instead of cyber exercise, their focus should be in security awareness because it would have a higher impact	low	role of NCSC-FI
NCSC-FI should become a forerunner in cyber exercise advisory	low	role of NCSC-FI
NCSC-FI should have a larger role in all national exercises	low	role of NCSC-FI

The last question in the role theme of the NCSC-FI was concerning their partners and who they should partner with. The NESA, CERTs and DVV received the highest mentions, and the results are displayed in Table 9. Most of the interviewees identified NESA as a key partner, which is logical because their services are focusing on helping critical infrastructure and they have been behind the investments of the NCSC-FI cyber exercise activities. The public sector interviewees all suggested that co-operation between public and private entities should be stronger.

Table 9. The organizations that the NCSC-FI should partner with identified by interviewees.

observation	frequency	theme
NESA	high	role of NCSC-FI
International Computer Emergency Response Teams (CERT)	high	role of NCSC-FI
DVV	high	role of NCSC-FI
Exercise organizers in Finland	high	
Large companies	medium	role of NCSC-FI
Digipooli	low	role of NCSC-FI
Confederation of Finnish Industries (EK)	low	role of NCSC-FI
MPK	low	role of NCSC-FI
Ministry of Transport and Communication	low	role of NCSC-FI
Finance sector	low	role of NCSC-FI
Start-ups	low	role of NCSC-FI
Work closely with universities to improve its services	low	role of NCSC-FI
NATO Cooperative Cyber Defence Centre of Excellence	low	role of NCSC-FI

The NCSC-FI wanted to understand if there is a demand for new tools, they could possibly create for the private sector to use, and the results are presented in Table 10. The tools in this case could be for instance, guides, templates, surveys, and platforms. The NCSC-UK's Exercise in the Box was used as a reference. It was not a good benchmark because the low number of respondents identified it. Only a handful of the interviewees could mention benchmarks, so it seems that international benchmarking is not something that Finnish organizations are doing on a regular basis. The smaller companies could not identify any benchmarks.

Table 10. Named tools or organizations that the NCSC-FI could use as benchmark.

observation	frequency	theme
Krivat	low	tools
Start-ups in Estonia	low	tools
Swedish MSB	low	tools
Enisa	low	tools
Platforms for technical exercises such as FOI, CRATE, Cybexer, Kypo Cyber Range Platforms, JYVSECTEC RGCE, Cyberbit, Cyberwiser, RHEA's Next Generation Cyber Range	low	tools

In the tools section, the next question was concerning what kind of tools would benefit the organizations that the interviewees represent. The high frequencies in the answers that were observed already in the previous questions such as sharing the information, market the exercises in regular basis, collaboration, and partnerships, which is visible in Table 11. The organizations that were not interested in the NCSC-FI tools were still interested in networking opportunities with other cyber exercise providers and showed an interest to develop the services on a national level. The information classification was also one of the most mentioned subjects in this question.

Table 11. Results of the frequencies for questions for what kind of tools would be beneficial for your organizations that the NCSC-FI could offer?

observation	frequency	theme
Share with organizations the threat intel that is not available in any other way. Generic information should not be labelled as confidential	high	tools
Presales activities: Marketing such as monthly webinars about cyber exercises including case studies, help CISO to build a cyber exercise culture and increase the budget for continuous exercise program	high	tools
Plan activities with objectives to create a positive image of cyber exercises and more exposure	high	tools
Network for exercise organizers	high	tools
More public-private partnerships	high	tools
No tools needed; organizations have their own methods and tools, and they are more advanced	medium	tools
Generic guides and templates that every organization can customize for themselves	medium	tools
Success measurements for each scenario in the scenario booklets	medium	tools
Maturity model that organization can compare their results to other	medium	tools
Annual exercise calendar	medium	tools
More scenarios	medium	tools
Script for tabletop exercises that include injections	medium	tools
Maturity model for management on how to act when handling incidents	low	tools
Sector specific threat intel library	low	tools
Injection playing cards to create engaging stories to exercises	low	tools
Marketplace for cyber exercises *(Table continues in the following page)*	low	tools

(Table is displayed in two pages) Awareness campaign for citizens on how to report an incident and why to report them. This helps the NCSC-FI to build situational awareness	low	tools
National threat and risk assessment that can be utilized in cyber exercises	low	tools
A tool that automates the role of authorities in the cyber exercises	low	tools
Share sector specific situational awareness	low	tools
Automatic analysing tool	low	
Maturity model for leadership	low	tools
Maturity model (such as kybermittari)	low	
Objectives and measures to each scenario	low	
Benchmark tool (how did the organizations succeed compared to other organizations in the same industry)	low	
Roadmaps for cyber exercise planning	low	tools
We have better tools ourselves and they have been offered to the NCSC-FI	low	tools

The last, but not the least important questions aim was to understand if the interviewed organizations are interested in using the NCSC-FI exercise services and tools that they provide. The most frequent remarks given were that organizations already have all the tools and services they need as displayed in Table 12. Especially the larger private companies said that they do not need support. However, the smaller companies answered the opposite. They are happy to get all the help that is available.

Table 12. Results to the question, is your organization interested in using any tools that the NCSC-FI offers?

observation	frequency	theme
No, we have built our own tools and services	high	tools
So far, the tools NCSC-FI are very limited and difficult to use in practice	medium	tools
Yes	low	tools
No interest to use, for instance any technical platforms. The exercise should be always conducted in a real environment where the organization is handling real incidents	low	tools
We have created better tools and they have been offered to NCSC-FI to use	low	tools

6 Discussions and conclusions

The main objective of this research was to understand how the NCSC-FI could support public and private organizations even better in their cyber exercises and to answer why organizations so rarely organize and participate cyber exercises. The NCSC-FI was also interested to identify if commercial companies have an interest to use their tools and services. The analysis had three main categories: challenges, the role of the NCSC-FI and tools. All three categories contained many similarities within the answers.

The chosen interviewees identified four key challenges: organizations do not understand that what are the key benefits and why cyber exercises are essential, organizations do not have enough resources to execute exercises, and there is no support from management. Finnish Standards Association (SFS) highlighted in 2019 that if management do not support the idea of hosting cyber exercise, it will be challenging to execute any plans. (Finnish Standards Association, 2019)

According to the results researched by Heikkinen (2020), only 35 % of organizations can independently plan and host exercises, and only 10 % are investing money to get external support. Furthermore, in nearly 90 % of the cases, the exercises are not part of the strategies. The lack of resources and support from the management are also key findings in Heikkinen's study. Another key finding in the study of Heikkinen was that most of the organizations need support to get started with exercise planning and execution, but at the same time, exercises are not part of the competence development and mainly they only participate to exercises organized by someone else. Each research provides a similar finding of these challenges, even though Heikkinen conducted the research only for public organizations.

The public and private sectors have some differences. For instance, more annual joint exercises are available in Finland for the public sector than for the private sector. Currently, the public sector feels that organizing exercises is not anyone's responsibility.

The interviews have also highlighted other challenges. For instance, organizations often assume that cyber exercises are only massive joint exercises and that efforts to organize them take a long time and is a huge undertaking. Some of the organizations have only participated in joint exercises, and they are not aware that a discussion-based cyber exercise can be something more minor and manageable such as when the NCSC-UK introduces the exercise in the box tool. The simpler version of the tool could be part of the he NCSC-FI services. The tool shall be easy to use, fully automated and self-serving and it should not save any data, to avoid any possible GDPR issues.

The interviewees suggested many good ideas to solve the challenges. Marketing is needed to change the mindset of exercises, and every organization should focus more on small and short exercises instead of the large exercises. Open communication of the exercises and more knowledge sharing of actual incidents and threat landscape is encouraged. The classification of materials was highlighted in many categories, and it seems to be a challenge that information is not shared actively.

The role of the NCSC-FI was more evident for private sector organizations, especially smaller ones. The smaller organizations used services more than the larger ones, which often have their own methods and tools. However, the research found that public sector participants did not know the role and benefits that the NCSC-FI have, and none of them could name all publicly available services on the NCSC-FI website. The recommendations for the growth of the NCSC-FI are to have a more active collaboration and information sharing with their peers. It is important that the NCSC-FI collaborates with international organizations and shares the critical learnings among Finnish organizations. Especially these questions brought the distortion of the competition into discussion and how it may limit services. The competitive law is introduced and explained in section 3.1

The tools section included three questions, and the first question concerned benchmarking and used the NCSC-UK Exercise in the box as an example. The concept was new to all interviewees; one had heard of it but did not know what it was. The benchmarking section only got a low amount of mentions of tools. All benchmarks mentioned were international examples, except for Krivat.

Most interviewees said they have no interest in using the NCSC-FI tools and services because they have their own or build the tools themselves if needed. However, smaller organizations were interested in the services, especially in the private sector. In addition, organizations are interested in threat intel, support in marketing activities and collaboration provided by the NCSC-FI. These same answers were repeated in many questions throughout this research.

This research has several ideas for the NCSC-FI to develop their services. The way how the ideas are presented in the table are showing how many times each idea was suggested and they shall suggest if we can see similar ideas from the research participants. The table does not consider if the idea is good or not or if it is it easy or hard to execute.

Some of the ideas need larger efforts than others and some even need an own project with own budget. On the other hand, the list has several ideas that can be executed as part of the daily work of an exercise team. Here are some suggestions that could be implemented to an exercise team's work:

- Share the threat intel with organizations that is not available any other way. Generic information should not be labelled as confidential.
- Marketing such as monthly webinars about cyber exercises including case studies, help CISO to build a cyber exercise culture and increase the budget for continuous exercise program.
- Start a network for exercise organizers

The NCSC-FI already shares knowledge via their newsletters and especially the threat intel is interesting for exercise organizers. (Traficom, 2022) The exercise organizers are not always present in Information Sharing and Analysis Centre groups, so they do not receive the information. This information could be shared via networking events with organizers. The NCSC-FI could be the main organizer and they could get support from the private sector with venues, agendas etc. Collaboration with other public sector organizations is essential. Currently there are a hand full of people executing partly similar activities in different organizations. The impact of the collaboration could mean more activities for a wider audience. A service that the NCSC-FI could offer are keynotes at events to present the exercises related to topics that clarify to the audience what they are and what are the benefits.

This research project was conducted over a two-year period. The time between the research and writing part was very long. That was due to the researcher having other commitments such as work and leisure time activities. The COVID-19 pandemic caused a new twist when all the work was conducted at home instead at the office. The days started to be more intensive with video conferences and often work was done after eight hours of work-related conference calls. This had an impact especially on the results because the world changed during this time, for instance Russia had attacked Ukraine. The result may have been different if the research interviews had been conducted after the war had started. The other main challenge was that the cyber exercise industry is small in Finland and people know each other. It was easy to get interviewees but at the same time, the researcher knew some of them in advance. The decision was made that the researcher will still conduct the interviews herself even though this was not recommended by research professionals. As the number of candidates was minor, it would have been interesting to read the results of a similar research which would have international participants and to see if we could find any similarities or differences.

6.1 Reliability

The reliability of the research was evaluated based on research methodology literature and previous research conducted in Finland concerning cyber exercises. The topic was chosen because the researcher is a subject matter expert in the same field and has a high interest to develop the services for a common good.

The researcher chose the theme analysis to conduct the research and content analysis to analyze the interview data. The answers for the research questions were found from sentences and words and they were counted and listed in the three theme categories according to frequency. The same model was used for ideas to see if there were common pattern and similarities in the replies. This gives an indication of the need for new services.

The personnel chosen to participate in the interviews were chosen carefully and they had a proven record of being the subject matter expert in cyber exercises. The ethicality was also an important part of the process and specially to protect the anonymity of the participants. The content of the interviews including recording and the transcripts were kept in a safe place and was only available to the researcher.

The results have been compared to previous research results of the same topic. There are many similarities which have been announced in the results section. Finding similarities from previous research increases the reliability of the results of this research. On the other hand, there was several months between analyzing the data and conducting the interviews which may affect the results. During this time, the researcher had gathered more experience related to the topic.

6.2 Different approaches and further studies

During the process of the project, there has been several ideas to research this topic further. The research around the general cyber exercises field is very limited globally. One of the most interesting topics could be to research the methodologies that are used for light tabletop exercises and investigate carefully what materials are globally available. Cyber security as a topic can be sometimes sensitive and the best practises are often kept secret.

It would be important to ask why management is not seeing the importance of cyber security and why they do not implement cyber security into business strategies. When researching possible references for the thesis, it quickly came clear that cyber exercises seem to be a well-kept secret for many private companies who offer the service, and the publicly available content is usually created by public organizations and offered to private sector to use.

Google search engine analytics proved that cyber exercise as a topic is not very common and there is barely any search history available. Someone with a marketing background could research the topic on how to make the cyber exercise a national phenomenon and increase the awareness and mindset of the cyber exercises. Lastly, one future topic could also be to follow the development of the organizations that are participating in exercises on a regular basis. The research could showcase interesting results of the benefits and importance, or on the other, prove that there is no return of investment at all.

References

1109/2015. Decree of the Government on public administration security network operations. Accessed 13 July 2022. Retrieved from https://www.finlex.fi/fi/laki/alkup/2015/20151109#Pidm45949344815968

683/2017. Decree of the Government on public administration security network operations. Accessed 27 November 2022. Retrieved from https://www.finlex.fi/fi/laki/alkup/2017/20170683

Accenture. 2021. *How aligning security and the business creates cyber resilience State of Cybersecurity Resilience 2021*. Accessed 13 April July. Retrieved from https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf

Barker, W. C., Fisher, W., Scarfone, K., & Souppaya, M. 2022. *Ransomware Risk Management: A Cybersecurity Framework Profile.* Accessed 30 July 2022. Retrieved from https://doi.org/10.6028/NIST.IR.8374

Burch, G., Fezzey, T., Batchelor, J., Reid, R., CISA, & CISSP. 2021. *The Pandemic Exposed a Lack of Business Continuity. How Business Must Change.* Accessed 30 July 2022. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/how-the-lack-of-business-continuity-is-changing-enterprises-following-the-pandemic

Clarke, R., & Knake, R. 2019. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Penguin Press.

Cybersecurity & Infrastructure Security Agency. 2022. *Cybersecurity.* Accessed 29 July 2022. Retrieved from https://www.cisa.gov/cybersecurity

Cybersecurity and Infrastructure Security Agency. 2020) *Critical Infrastructure Sectors.* Accessed 14 July 2022. Retrieved from https://www.cisa.gov/critical-infrastructure-sectors

DVV. 2021. TAISTOmaatti - digitaalinen harjoitus organisaation toiminnan ja jatkuvuuden mahdollistamiseksi. *[TAISTOmaatti -. a digital exercise to enable the operation and business continuity of the organization].* Accessed 3 September 2022. Retrieved from https://www.eoppiva.fi/koulutukset/taistomaatti-digitaalinen-harjoitus-organisaation-toiminnan-ja-jatkuvuuden-mahdollistamiseksi/

European Union Agency for Network and Information Security. 2022. *Glossary.* Accessed 14 July 2022. Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

European Union Agency for Network and Information Security. 2010. *Cyber Europe 2010.* Accessed 31 July 2022. Retrieved from https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/ce2010

European Union Agency for Network and Information Security. 2012. *National and International Cyber Security Exercises: Survey, Analysis & Recommendations — ENISA*. Accessed 31 July 2022. Retrieved from https://www.enisa.europa.eu/publications/exercise-survey2012

European Union Agency for Network and Information Security. 2015. *Exercises global survey.* Accessed 31 July 2022. Retrieved https://www.enisa.europa.eu/topics/cyber-exercises/trainings/cyber-exercises/cyber-exercise-surveys

European Union Agency for Network and Information Security. 2021. *ENISA Threat Landscape 2021*. Accessed 31 July 2022. Retrieved https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021?v2=1

European Union Agency for Network and Information Security. 2022. *Cyber Europe 2022: Testing the Resilience of the European Healthcare Sector*. Accessed 5 August 2022. Retrieved https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2022-testing-the-resilience-of-the-european-healthcare-sector

Financial supervisory Authority. 2022. FIN-FSA regulations and guidelines - Regulation. Accessed 13 July 2022. Retrieved https://www.finanssivalvonta.fi/en/regulation/FIN-FSA-regulations/

Finnish Competition and Consumer Authority. 2022. Competitive neutrality. Accessed 11 July 2022. Retrieved https://www.kkv.fi/en/competition-affairs/competitive-neutrality/

Finnish National Cyber Security Centre. 2022. *Kyberharjoitusskenaariot.* [Cyber exercise scenarios]. Accessed 11 July 2022. Retrieved https://www.kyberturvallisuuskeskus.fi/fi/s/kyberharjoitusskenaariot

Finnish National Cyber Security Centre. 2019. *Instructions for organizing cyber exercises.* Accessed 11 July 2022. Retrieved https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Instructions%20for%20organising%20cyber%20exercises.pdf

Finnish National Cyber Security Centre. 2021. *Exercises.* Accessed 11 July 2022. Retrieved https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta?toggle=Harjoitus-%20ja%20koulutuspalveluita%20tarjoavat%20yritykset

Gillham, B. 2013. *The research interview (Real world research).* Dawson Books.

Heikkinen, H. 2020. *The current state of the digital security exercise program in public administration in Finland.* Master thesis, University of Jyväskylä. Accessed 31 July 2022. Retrieved https://jyx.jyu.fi/handle/123456789/68760

Heikkinen, H. 2022. *The current state of the digital security exercise program in public administration in Finland.* Accessed 5 August 2022. Retrieved https://dvv.fi/documents/16079645/0/Julkishallinnon+digitaalisen+turvallisuuden+harjoitustoiminnan_nykytilakuvaus.pdf/3eb82429-37c9-feff-69f5-8155dcec0a77/Julkishallinnon+digitaalisen+turvallisuuden+harjoitustoiminnan_nykytilakuvaus.pdf?t=1606740671856

Hirsjärvi, S., & Hurme, H. 2015. *Tutkimushaastattelu : teemahaastattelun teoria ja käytäntö* [Research interview: theory of and practice of research interview]. Gaudeamus Helsinki University Press.

Homeland Security. 2020. *Homeland Security Exercise and Evaluation Program (HSEEP).* Accessed 31 July 2022. Retrieved https://www.fema.gov/sites/default/files/2020-04/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf

IBM. 2022. *Cost of a Data Breach Report 2021.* Accessed 14 July 2022. Retrieved https://www.ibm.com/security/data-breach

Ilta-Sanomat. 2022a. Nordean verkkopalveluissa häiriö, tilin saldo voi näyttää nollaa. *[Disruption in Nordea's online services, the account balance may show zero].* Accessed 30 July 2022. Retrieved https://www.is.fi/taloussanomat/art-2000008738817.html

Ilta-Sanomat. 2022b. Ulko- ja puolustusministeriön verkkosivuihin kohdistui palvelunestohyökkäys. *[The website of the Ministry of Foreign Affairs and Defense was hit by a service denial attack].* Accessed 30 July 2022. Retrieved https://www.is.fi/digitoday/art-2000008738925.html

International Organization for Standardization. 2021. *Keeping cybersafe - New guidance on cybersecurity frameworks just published*. Accessed 29 July 2022. Retrieved https://www.iso.org/news/ref2629.html

ISO 22301:2019. 2019a. *The International Organization for Standardization. Security and resilience — Business continuity management systems — Requirements.* https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en

ISO 22301:2019. 2019b. *The International Organization for Standardization. - Security and resilience — Business continuity management systems — Requirements.* https://www.iso.org/standard/75106.html

ISO 22398:2013 2013. *The International Organization for Standardization. Societal security — Guidelines for exercises.* https://www.iso.org/standard/50294.html

ISO 27001:2013. 2013. *The International Organization for Standardization. Information technology — Security techniques — Information security management systems — Requirements.* https://www.iso.org/standard/54534.html

ISO 27002:2022. 2022. *The International Organization for Standardization. Information security, cybersecurity and privacy protection — Information security controls.* https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en

Istekki. 2022. Cyber Europe 2022 -harjoitus testasi kykyä vastata kyberhyökkäyksiin. *[The Cyber Europe 2022 exercise tested the ability to respond to cyber attacks].* Accessed 5 August 2022. Retrieved https://www.istekki.fi/web/guest/ajankohtaista/-/asset_publisher/H6eGzJ2flC3R/content/cyber-europe-2022-harjoitus-testasi-kykya-vastata-kyberhyokkayksiin?inheritRedirect=true

Jalava, J., Raisio, H., Lahtinen, H., Puustinen, A., & Norri-Sederholm, T. 2017. Kolmas sektori viranomaisten turvallisuustoiminnan tukena. *[The third sector in support of the authorities' security activities]*. Accessed 5 August 2022. Retrieved https://tietokayttoon.fi/documents/10616/3866814/76_Loppuraportti+kolmas+sektori+viranomaisten+turvallisuustoiminnan+tukena_editoitu+22.12.2017.pdf/8ae646dd-b4b7-49a3-86f3-ee86001fdcf2?version=1.0

JAMK. 2018. *Ethical Principles for JAMK University of Applied Sciences*. Approved by the Student Affairs Board on 11 December 2018. Accessed 29 July 2022. Retrieved https://www.jamk.fi/fi/file/ethical-principles

JYVSECTEC. 2015. *JYVSECTEC Center RGCE.* Accessed 31 July 2022. Retrieved https://jyvsectec.fi/2015/02/jyvsectec-center-rgce/

Kick, J. 2015. *Cyber Exercise Playbook.* In The MITRE Corporation. Accessed 11 July 2022. Retrieved https://www.mitre.org/publications/technical-papers/cyber-exercise-playbook

Kurittu, A. 2020. *Cyber training guide to support the training of organizations.* Master thesis, Laurea University of Applied Sciences. Theseus. Accessed 31 July 2022. Retrieved https://www.theseus.fi/handle/10024/347180

National Defense Authorization Act for Fiscal Year 2022. 2021. *Testimony of Library of Congress.* Accessed 31 July 2022. Retrieved https://www.congress.gov/bill/117th-congress/senate-bill/1605/text?q=%7B%22search%22%3A%5B%22S.1605%22%2C%22S.1605%22%5D%7D&r=1&s=1

Lötjönen, J. 2021. *The National Cyber Security Exercise 2021.* Accessed 5 August 2022. Retrieved https://jyvsectec.fi/2021/05/the-national-cyber-security-exercise-2021/

Microsoft. 2022. *Defending Ukraine: Early Lessons from the Cyber War.* Accessed 11 July 2022. Retrieved https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

National Emergency Supply Agency. 2022. *Overview of security of supply.* Accessed 30 July 2022. Retrieved https://www.huoltovarmuuskeskus.fi/en/security-of-supply/overview

National Emergency Supply Agency. 2022. *Continuity management.* Accessed 30 July 2022. Retrieved https://www.huoltovarmuuskeskus.fi/en/security-of-supply/continuity-management

National Emergency Supply Agency. 2022. *Funding and legislation.* Accessed 5 August 2022. Retrieved https://www.huoltovarmuuskeskus.fi/en/organisation/funding-and-legislation

National Emergency Supply Agency. 2020. TIETO20-harjoitus testaa yhteistoimintaa laajassa kyberhäiriötilanteessa. [*The TIETO20 exercise tests cooperation in a large-scale cyber attack situation].* Accessed 30 July 2022. Retrieved https://www.huoltovarmuuskeskus.fi/a/tieto20-harjoitus-testaa-yhteistoimintaa-laajassa-kyberhairiotilanteessa

National Emergency Supply Agency. 2021. Pankit ja viranomaiset kehittävät varautumistaan yhteisellä suurharjoituksella. [*Banks and authorities develop their preparedness with a joint large-*

scale exercise]. Accessed 13 July 2022. Retrieved https://www.huoltovarmuuskeskus.fi/a/pankit-ja-viranomaiset-kehittavat-varautumistaan-yhteisella-suurharjoituksella

National Emergency Supply Agency (NESA). 2021. *DT2030 Projects.* Accessed 13 July 2022. Retrieved https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio/huoltovarmuuskeskus/4962-2/digitaalinen-turvallisuus-2030/dt2030-projektit

National Institute of Standards and Technology (NIST). 2021. *Cyber Security - Glossary.* Accessed 29 July 2022. Retrieved https://csrc.nist.gov/glossary/term/cyber_security

Nortio, J. 2017. Kyber 2020 – Yhteistyöllä suojaan kybermyrskyiltä. *[Kyber 2020 - protect against cyber storms with collaboration]*. Accessed 11 July 2022. Retrieved https://erveuutiset.erillisverkot.fi/kyber-2020-yhteistyolla-suojaan-kybermyrskyilta/

Novak, J., Purta, M., Marciniak, T., Ignatowicz, K., Rozenbaum, K., & Yearwood, K. 2018. *The rise of Digital Challengers: How digitization can become the next growth engine for Central and Eastern Europe.* Accessed 14 July 2022. Retrieved https://www.mckinsey.com/~/media/mckinsey/featured%20insights/europe/central%20and%20eastern%20europe%20needs%20a%20new%20engine%20for%20growth/the-rise-of-digital-challengers.ashx

Pajunen, D. 2017. Kyberturvallisuus varmistetaan aidoilla harjoituksilla. *[Cyber security is ensured with real exercises].* Accessed 5 August 2022. Retrieved https://www.fingridlehti.fi/kyberturvallisuus-varmistetaan-aidoilla-harjoituksilla/

Paloalto. 2022. *Ransomware Threat Report 2022.* Accessed 30 July 2022. Retrieved https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2022-unit42-ransomware-threat-report-final.pdf

PCI Security Standards Council. 2009a. *Official PCI Security Standards Council Site.* Accessed 13 July 2022. Retrieved https://www.pcisecuritystandards.org/get_involved/participating_organizations/financial-institution/europe/all

PCI Security Standards Council. 2009b. *PCI DSS Quick Reference Guide.* Accessed 13 July 2022. Retrieved https://listings.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf

Perttula, J., & Latomaa, T. 2006. *Kokemuksen tutkimus: merkitys, tulkinta, ymmärtäminen* [Study of experience: meaning, interpretation, understanding]. Dialogia.

Risto, J. 2015. *Exercise - Not just for Your Body Anymore.* Accessed 11 July 2022. Retrieved https://sansorg.egnyte.com/dl/LeDbLIPz9I

Samonas, S., & Coss, D. 2014. *The cia strikes back: redefining confidentiality, integrity, and availability in security.* Accessed 14 July 2022. Retrieved https://www.proso.com/dl/Samonas.pdf

Secretariat of the Security Committee. 2019. *Finland's Cyber security Strategy*. Government Resolution 3.10.2019. Accessed 11 July 2022. Retrieved https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

SFS- ISO 22398:2019. 2019. *Finnish Standards Association. Societal security — Guidelines for exercises.* Accessed 31 July 2022. Retrieved https://sales.sfs.fi/en/index/tuotteet/SFS/ISO/ID2/2/821351.html.stx

Skripnichuk, A. 2015. *Soldiers prepare for live-fire exercise. New Forthood Sentinel.* Accessed 31 July 2022. Retrieved http://www.forthoodsentinel.com/news/soldiers-prepare-for-live-fire-exercise/article_14f482c6-1df3-55aa-827b-d601a95b71d9.html

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. 2010. *Contingency planning guide for federal information systems.* NIST Special Publication 800-34 Rev. 1. https://doi.org/10.6028/NIST.SP.800-34R1

The Business Continuity Institute (BCI). 2022. *Introduction to Business Continuity.* Accessed 30 July 2022. Retrieved https://www.thebci.org/knowledge/introduction-to-business-continuity.html

The Club de la Continuité d'Activité (CCA), & French National Cyber Security Agency (ANSSI). 2021. *Organizing a cyber crisis management exercise.* Accessed 11 July 2022. Retrieved https://www.enisa.europa.eu/topics/cyber-exercises/trainings/20210906_np_anssi_guide_exercice_crise_en_v4.pdf

The Digital and Population Data Services Agency's services. 2022. JUDO-hanke, *Väliraportti 2019-2021.* Accessed 13 July 2022. Retrieved https://dvv.fi/documents/16079645/110183105/JUDO-hanke+v%C3%A4liraportti+2019-2021.pdf/f3af086e-452e-be51-4fde-10a90a5abfed/JUDO-hanke+v%C3%A4liraportti+2019-2021.pdf?t=1645172899292

The International Telecommunications Union (ITU). 2022. *Cybersecurity.* Accessed 29 July 2022. Retrieved https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

The Ministry of Transport and Communications of Finland. 2020. Valtion kyberturvallisuusjohtaja on nimitetty. *[The state cyber security director has been appointed].* Accessed 11 July 2022. Retrieved https://www.lvm.fi/-/valtion-kyberturvallisuusjohtaja-on-nimitetty-1033603

The National Cyber Security Centre of UK. 2020. *Effective steps to cyber exercise creation.* Accessed 11 July 2022. Retrieved https://www.ncsc.gov.uk/guidance/effective-steps-to-cyber-exercise-creation

The NATO Cooperative Cyber Defense Centre of Excellence. 2022. *Finland Wins Cyber Defence Exercise Locked Shields 2022.* Accessed 5 August 2022. Retrieved https://ccdcoe.org/news/2022/finland-wins-cyber-defence-exercise-locked-shields-2022/

The Swedish Civil Contingencies Agency. 2016. *Exercise Guidance: Basic Manual - An Introduction to the Fundamentals of Exercise Planning.* Accessed 11 July 2022. Retrieved https://rib.msb.se/filer/pdf/28402.pdf

Toikko, T., & Rantanen, T. 2009. Tutkimuksellinen kehittämistoiminta: näkökulmia kehittämis-prosessiin, osallistamiseen ja tiedontuotantoon [*Research and development activities: perspectives development process, participation and information production]*. Accessed 5 August 2022. Retrieved https://trepo.tuni.fi/handle/10024/100802

Traficom. 2019a. *Instructions for organising cyber exercises.* Accessed 11 July 2022. Retrieved https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Instructions%20for%20organising%20cyber%20exercises.pdf

Traficom. 2019b. Tietoturvan Vuosi 2018. *[Year of Information security 2018].* Accessed 11 July 2022. Retrieved https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Vuosikatsaus_2018_tulostettava_sivuttain.pdf

Traficom. 2020. Tietoturvan vuosi 2019. *[Year of Information security 2019].* Accessed 11 July 2022. Retrieved https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_tietoturvanvuosi_2019_WEB_sivuittain.pdf

Traficom. 2021a. *ISAC information sharing groups.* Accessed 5 August 2022. Retrieved https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups

Traficom. 2021b. Tietoturvan Vuosi 2020. *[Year of Information security 2020].* Accessed 11 July 2022. Retrieved https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2020_210212_FIN.pdf

Traficom. 2021c. *HAVARO service.* Accessed 16 July 2022. Retrieved https://www.kyberturvallisuuskeskus.fi/en/havaro-service

Traficom. 2022. *Situation awareness and network management.* Accessed 11 July 2022. Retrieved https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management

Tuomi, J., & Sarajärvi, A. 2006. Laadullinen tutkimus ja sisällönanalyysi *[Qualitative research and content analysis]* (4th ed.). Tammi.

Vartiainen, H. 2022. Erikoistilanteisiin varautuminen on vastuullisuutta. *[Being prepared for special situations is responsibility].* Accessed 5 August 2022. Retrieved https://www.dna.fi/blogi/-/blogs/erikoistilanteisiin-varautuminen-on-vastuullisuutta

Victorian Government Cyber Incident Response Service. 2019. *A guide to cyber exercises: plan + conduct + evaluate.* Accessed 11 July 2022. Retrieved https://www.vic.gov.au/sites/default/files/2019-08/Vic-Gov-Cyber-Exercise-guide.pdf

von Solms, R., & van Niekerk, J. 2013. *From information security to cyber security. Computers & Security.* https://doi.org/10.1016/j.cose.2013.04.004

Weinberg, A. 2021. *Analysis of top 11 cyber-attacks on critical infrastructure.* Accessed 30 July 2022. Retrieved https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/

Weiner, S. 2021. *The growing threat of ransomware attacks on hospitals.* Accessed 14 July 2022. Retrieved https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals

Welch, L. 2011. *Cyberspace - The fifth operational domain. The Institute for Defense Analyses.* Accessed 29 July 2022. Retrieved https://www.ida.org/-/media/feature/publications/2/20/2011-cyberspace---the-fifth-operational-domain/2011-cyberspace---the-fifth-operational-domain.ashx

Whitman, M., & Mattord, H. 2012. *Principles of information security* (3rd ed.). Course Technology.

World Economic Forum. 2022. *Global Cybersecurity Outlook 2022.* Accessed 13 July 2022. Retrieved https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

Appendices

Appendix 1. Data samples

Examples of the answers. Answers are translated from Finnish to English

Category: Challenges

what are the main challenges and reasons why it is so rare that organizations are not participating in cyber exercises?	“There seem to be issues in publish sector who is responsible of cyber exercises. It seems that each organization is doing their own thing and they do not even know that someone else planning similar activities elsewhere. Collaboration between organization shall be strengthen.” “Cyber exercises shall be part of every organization’s activity, but it is not like that at all. For instance, the need has not been recognized and there is no understanding what should be developed. Organization exercises is too big effort and too difficult.”
What are the reasons behind organizations not being able to host their own exercises?	“Exercises are too big and difficult to organize, organizations do not have resources to organize exercises.” “Cyber exercises are often too big and take too much time.“
How can we overcome these challenges?	“There shall be light exercises, which are not defined by how many people will attend. “

	“There shall be maturity model: what kind of exercises shall be done, when is good time to ask partners and authorities to participate the exercises and so on. “

Category: Role of NCSC-FI

What are the current cyber exercise services offered by the NCSC-FI?	“They are authority so the role can be quite difficult.” “I only know scenario tool. “ “I have no clue and I do not know anyone there.”
What is the role that NCSC-FI should have in the future of the Finnish cyber exercises industry?	“NCSC-FI should organize cyber exercises for another organizations. “ “They could support organizations who wants to get started with exercises, could be something light and simple. “
Who should be partnering with NCSC-FI exercise services?	“The Confederation of Finnish Industries and its members and global CERT network. Maybe actually NCSC-FI is already working with global instances but why it is not visible to anyone else?" “Global CERTs for instance in France, UK, Holland, Norway, Australia, New Zealand and US.”

Category: Tools

Can you suggest any tools, such as “Exercise in the Box” in UK or guides and templates that NCSC-FI should investigate in to more or could be used as a benchmark?	“Only thing I can think of is NCSC in UK and their service exercise in the Box.” “Only organization I can think of is ENISA.”
What kind of tools would be beneficial for your organizations that NCSC-FI could offer?	“The Public-Private partnership should work even better. Tools that scale.” “No new tools are needed because they usually confuse the participants of the exercises. Like for instance Trasim. The tools that customer is using in real crisis shall always be used. “
Is your organization interested in using any tools that NCSC-FI offers?	” I like scenario bank; I hope it develops further.” “No, we build our own tools.”