TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technology
Department of Software Science
TUT Centre for Digital Forensics and Cyber Security

ITC70LT

Katrin Kukk 132243IVCMM

MAPPING THE BEST PRACTICES FOR DESIGNING MULTI-LEVEL CYBER SECURITY EXERCISES IN ESTONIA

Master's thesis

Supervisors
Rain Ottis, PhD
Lauri Luht

Tallinn 2017

Declaration

I hereby declare that I am the sole author of this thesis. All the used literature and the work of others have been cited. This thesis has not been presented for examination anywhere else.

Author: Katrin Kukk

18.05.2017

Abstract

Instructions for planning cyber exercises exist, but they don't cover the challenges and solutions of how to design multi-level cyber exercises. Multi-level exercises consist of whether technical and operational levels, operational and strategic levels or all the three levels are covered in the exercise. The purpose of the thesis is to map the best practices and to propose an instruction set for designing multi-level exercises, in order to address the problem that national cyber security exercises in Estonia are typically focusing on only one level at a time. An additional aim is to determine the shortcomings of cyber exercises. The outcome of the thesis is a set of instructions for designing efficient multi-level cyber exercises. The thesis objectives are achieved by analyzing the literature review and interview results. The author conducted semi-structured interviews with experts of the field, which brought out relevant information, such as various cyber exercises shortcomings, multi-level exercise advantages, challenges and solutions, etc. Results of the thesis are validated by asking feedback from experts, who have experience in designing and conducting exercises. Feedback showed that proposed instruction set is useful when designing multi-level cyber exercises. As for future work, it is recommended to validate the resulting instruction set in practice when designing and conducting multi-level cyber exercise.

This thesis is written in English and includes 69 pages of text, including 6 chapters, 6 figures and 3 tables.

Annotatsioon

Parimate praktikate kaardistamine mitmetasandiliste küberõppuste korraldamiseks Eestis

Küberõppuste korraldamiseks on küll juhendeid, kuid need ei käsitle mitmetasandiliste küberõppuste korraldamise väljakutseid ja erinevate keerukustega toimetulemist. Mitmetasandilised õppused koosnevad kas tehnilisest ja operatiivtasandist, operatiiv- ja strateegilisest tasandist või kõik kolm tasandit on õppusel kaetud. Käesoleva lõputöö eesmärk on kaardistada parimad praktikad ja välja pakkuda soovituste nimekiri mitmetasandiliste õppuste korraldamiseks, mis lahendaks probleemi, et riiklikud küberõppused korraldatakse Eestis peamiselt ühel tasandil. Lisaks on lõputöö alameesmärk tuvastada ka küberõppuste kitsaskohad. Lõputöö tulemiks on efektiivsete mitmetasandiliste küberõppuste korraldamise soovituste nimekiri. Lõputöö eesmärgid saavutatakse kogutud informatsiooni ning intervjuude tulemite analüüsi tulemusel. Autor korraldas ekspertiga pool-struktureeritud intervjuud, mis tõid välja olulisi aspekte, näiteks mitmed küberõppuste kitsaskohad, mitmetasandiliste küberõppuste eelised, väljakutsed ja lahendused jpm. Lõputöö tulemid on valideeritud ekspertide tagasiside põhjal, kellel on kogemust õppuste planeerimisel ja läbiviimisel. Tagasiside näitas, et soovituste nimekiri mitmetasandiliste küberõppuste korraldamiseks on kasulik. Täiendava tööna on soovituslik valideerida välja pakutud soovituste nimekiri praktikas, kasutades neid soovitusi mitmetasandiliste küberõppuse planeerimisel ja läbiviimisel.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 69 leheküljel, 6 peatükki, 6 joonist, 3 tabelit.

List of abbreviations and terms

ENISA	The European Union Agency for Network and Information Security
NATO	North Atlantic Treaty Organization
EU	European Union
NATO CCD COE	NATO Cooperative Cyber Defence Centre of Excellence
RIA	Estonian Information System Authority
LS	Locked Shields
CC	Cyber Coalition
CE	Cyber Europe
TTXs	Tabletop Exercises
FEs	Functional Exercises
FSEs	Full-scale Exercises
HSEEP	Homeland Security Exercise and Evaluation Program
RT	Red Team
WT	White Team
BT	Blue Team
GT	Green Team
IPC	Initial Planning Conference
MPC	Main Planning Conference
FPC	Final Planning Conference
AAR	After-Action Report
IP	Improvement Plan

Table of Contents

List of Figures

List of Tables

1. Introduction

Europe has attained a great role in cyber security exercises, as being responsible for more than 40% of international exercises in between 2012-2015. Four cyber security exercise trends have been recognized. Firstly, it has been observed, that trend moves towards enhanced complexity of the exercises. This includes rising numbers of involved institutions, participating specialists and stakeholders. Secondly, another outstanding trend is to focus on increasing cooperation between stakeholders. Thirdly, it is also noticed, that both private and public sectors are being involved in order to increase their collaboration through exercises. Finally, trend also moves towards designing "gap-bridging exercises", which refers to the increasing need for multi-level exercises, to enhance cooperation and communication between technical, operational and/or strategic levels. [1]

Importance of cyber security exercises has grown due to the increased growth of cyber threats and various malicious activities both nationally and internationally [1]. During the cyber-attack in Estonia in 2007, government institutions and some elements of the critical information infrastructure (CII) were targeted with Distributed Denial of Service (DDoS) attacks [2]. It demonstrated that attacks could affect multiple organizations and evolve into endangering the whole society and national security [3]. As threat landscape is transforming and attacks are becoming extremely sophisticated [4], they may have severe consequences. For example, "Stuxnet", which is a refined malware, identified in 2010, aimed at Iran's nuclear power station and disrupted the centrifuges [5]. Also, there's advanced malicious code named "Snake", which was discovered in 2014, that infiltrated into several countries government institutions [6].

Since cyber-attacks are becoming more sophisticated, exercises have essential part for gaining experience when there haven't been many large cyber crises so far. They help to enhance awareness and collaboration between technical, operational and strategic levels. [7] Furthermore, if crisis escalation process hasn't been played through before the real crises, in a simulated and safe way, decision-makers might not understand the full picture of the crisis and its potential negative outcomes.

Single-level exercises are good to a certain degree, but when it comes to determining communication issues between entities in cyber crisis situation or shortcomings in

legislation, single-level exercises don't allow to discover all the bottlenecks. The same applies to exercises that appear to be multi-level exercise, but different levels are not conducted simultaneously. Compared to actual multi-level exercises, it's easier to design them, but they still don't give the full picture of the situation in order to ascertain issues.

1.1. Motivation

This thesis focuses on solving the problem that national cyber security exercises held in Estonia are mainly conducted at one level at a time – technical, operational or strategic [8], [9]. The same logic generally applies to European Union (EU) or North Atlantic Treaty Organization (NATO) cyber security exercises [10], [11], [12]. It means that whether there are only technical level exercises for solving hands-on technical incidents, operational level exercises, where procedures and processes are being rehearsed, or strategic level exercises, where higher strategic decision making procedures are being tested.

There have been exercises where multiple levels are included, but their incident escalation to next degree was divided into separate phases, and activities themselves were performed on separate levels. For example, Cyber Europe 2014 exercise covered all three levels and Cyber Europe 2016 concentrated on operational and technical levels, but neither of them were practiced simultaneously. [10], [11] Different level exercises should take place at the same time, because otherwise in case of a real crisis, there will be confusion between entities, their responsibilities and mandates, when coordinating incident resolution.

Although there are handful of international manuals [13], [14], [15] for designing cyber security exercises, they don't cover multi-level exercises or solutions of how to overcome complexities that arise when designing such exercises. **The main research question is which are the best practices for designing multi-level cyber exercises?** There haven't been many efficient national multi-level cyber exercises, where levels are communicating and commands are moving from higher levels to lower ones. It's possibly so, because there is no experience with designing such exercises and there are no guiding instructions.

Multi-level cyber exercises need partially different planning, when compared to single-level cyber exercises, and several essential topics need to be considered. Following sub

questions were formulated by the author when general research question was discussed with thesis supervisors:

- How long should the planning cycle be and which are the milestones;
- How should exercise objectives be set;
- How to choose target groups and staff, who is involved with planning the exercise;
- How to create a scenario which will not get stuck or bring other levels off the desired course;
- How to make different levels to communicate;
- How to break the time dimensions, such as when time on technical level goes many times faster compared to operational or strategic levels;
- How to motivate people to participate in exercises;
- How to audit lessons learned and improvement areas implementation.

Therefore, there is a need for instruction set that would:

- Help with designing multi-level exercises by answering to previously stated questions;
- Bring out helpful tips and various matters to consider when planning multi-level exercises.

1.2. Scope

The purpose of this thesis is to map the best practices and propose an instruction set for designing multi-level cyber security exercises in Estonia. Main focus is on operational and technical levels, because majority of official documents regarding strategic level is classified. Additional objective of the thesis is to determine shortcomings of cyber security exercises. The thesis will not cover any state secrets or materials that are meant only for internal use.

Background information is collected through literature review and experts' interviews, which are conducted with known Estonian specialists in the field. As focus is on the state and bringing out the national view, foreign countries experts are left out of the scope. Additional limitations are logistical inconvenience and possible misinterpretations, due to differences in native languages.

1.3. Methodology

The thesis uses qualitative research methodology and the collection of qualitative data will consist of two phases – gathering background information though literature review (academic papers and official documents) and conducting semi-structured open-ended interviews [16]. The overall strategy is to collect relevant information, process the gathered data, propose solutions to raised questions and validate results based on the analysis.

The author has chosen qualitative research methodology for achieving thesis objectives, because it allows covering the topic in detailed perspective in comparison to the quantitative research methodology. Quantitative research is mainly used for statistical studies whereas qualitative research is used in order to gather comprehensive, in-depth data in narrative way. [16] For those reasons, qualitative research method is used, when finding solutions to the research question. Disadvantage of using qualitative research is that it is less objective, data interpretation is complex, and the quantity of the data makes processing and analyzing time-consuming. Moreover, the sample size is relatively small when compared to quantitative research and results can be difficult to visualize. [16] Those disadvantages are irrelevant in this case, because sample size is purposely planned to be small, as only relevant experts related to cyber exercises on the field are interviewed.

Semi-structured and open-ended (instead of "yes" or "no" are expected descriptive answers) interviewing method is used, because it allows to gather detailed information about the topic in a narrative way. Although there is a template with questions that should be discussed during the interviews, question asking sequence is not strictly regulated. [17] Time and place for conducting interviews was agreed via e-mails and interviews with 13 experts took place between 17.03.2017-31.03.2017. Interview questions are designed, for example, to gather background information about the specialists, find out the advantages of multi-level exercises and also solutions on how to design such exercises. Also, to identify cyber exercises shortcomings today.

Full list of interview questions is brought out in native language in Appendix 1, but questions are mainly divided into following three categories:

- **Background questions** purpose is to gather information regarding the interviewees' relation to cyber security exercises in which they have participated

or which they have designed. Furthermore, the questions also cover the current shortcomings of planning cyber related exercises.

- **Main questions** purpose is to find out the reasons why it's essential to design multi-level exercises, what makes it difficult and how they should be planned. Moreover, find out whether any of the experts have designed or participated in multi-level exercises and are there time differences on different levels.
- **Decision-making questions** purpose is to determine how decisions are made during cyber crisis and whether the decision-making process is clear enough. Furthermore, whether decisions should be made rather by individuals or collectively, through compromises or chain of command.

The author asked initial list of interviewees from Rain Ottis and Lauri Luht, as they are experts on the field when it comes to cyber security exercises. Additional suggestions regarding who to interview were discussed during the interviews with specialists.

Interview times and names of the experts were as follows:

- Rain Ottis – Tallinn University of Technology (TTÜ) (17.03)
- Lauri Luht – Estonian Information System Authority (RIA) (20.03)
- Estonian Defense Forces specialist (21.03)
- Ministry of Defence specialist (21.03)
- Andrus Padar – Estonian Defence League's Cyber Unit (EDL CU) (22.03)
- Lauri Palkmets – Estonian Defence League's Cyber Unit (EDL CU) (22.03)
- Aare Reintam – NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) (23.03)
- Gert Kaju – Government Office of Estonia (23.03)
- Andres Parve – Ministry of the Interior (24.03)
- Priit Saar – Police and Border Guard Board (27.03)
- Vello Loemaa – BHC Laboratory (28.03)
- Teet Laeks – Estonian Defense Forces (29.03)
- Urmo Sutermäe – Tallinn Airport (31.03)

Interviewees Rain Ottis, Lauri Luht, Andrus Padar, Priit Saar, Vello Loemaa and Teet Laeks allowed to be referenced in the thesis, but to honor other experts' decision to stay

anonymous, all the interview results are anonymized, so their answers couldn't be singled out.

One interview took approximately an hour and total time for the interviews was 14 hours and 16 minutes. Interviews were recorded and transcripts were created, but neither of the recordings nor the transcript documents are a part of the thesis. Writing the transcripts took approximately 42 hours. Based on the transcripts, the author created an excel file, where all the questions and experts' answers were brought out. Most relevant experts' opinions, which help to achieve the thesis goals, are brought out and discussed in Chapter III. In Chapter IV, the author analyses the gathered data from Chapter II (literature review) and Chapter III (interview results) and proposes recommendations for planning multi-level cyber exercises.

Thesis results are validated by specialists, who have experience in designing and conducting exercises. Due to the time and resources limitations, it is not possible to validate the results in practice by designing and conducting separate exercise. As both supervisors are also involved with designing cyber exercises, their feedback provides additional validity. However, for final validation, instructions should be used in real life when designing an exercise.

1.4. Outline

In general, the thesis can be divided into five main sections:

- Researching theoretical background information;
- Preparing and conducting interviews;
- Analyzing the results;
- Proposing an instruction set for designing multi-level exercises;
- Validating results.

Chapter II concentrates on gathering background information through document analysis methods and defining relevant concepts, such as the current situation on the field and the process of planning cyber exercises. Also, different types of exercises and their similarities are covered.

Chapter III reviews and discusses the results of semi-structured and open-ended interviews with experts on the field.

Chapter IV concentrates on the analysis of the gathered data from Chapter II and Chapter III. As a result, instruction set for designing multi-level cyber security exercises in Estonia is proposed.

Chapter V validates the results by asking feedback from experts, who have experience in designing and conducting exercises.

The conclusion summarizes the most important results of the thesis and also brings out additional possible future work.

2. Theoretical background of exercises

According to ISO 22398, which proposes guidelines for exercises, there are multiple reasons for conducting exercises, such as validating existing workflows; testing infrastructure disaster recovery plans; specifying tasks and responsibilities; enhancing collaboration; determining improvement areas and shortcomings in resources; increasing personal skills; rehearsing improvisation in simulated environments. [18]

There should be always objectives to accomplish when designing exercises [18]. For example, performance objectives, which are as follows:

- **"Orientation/demonstration"** – Purpose is to simulate presumable outcome of the situation in order to enhance awareness of existing vulnerabilities and/or emphasize necessity of efficient reactions to various situations [18];
- **"Learning"** – Purpose is to increase personal and/or teams' competencies, such as skills and performance [18];
- **"Cooperation"** – Purpose is to achieve group's mutual goals through working together [18];
- **"Experimenting"** – Purpose is to test new techniques, policies and/or processes in order to make improvements [18];
- **"Testing"** – Purpose is to assess existing techniques, policies and/or processes with the intent to evaluate their adequacy [18].

According to the research made by The European Union Agency for Network and Information Security (ENISA), most cyber security exercises that have been held in recent years, can be divided into four categories based on their objectives:

- "Develop capabilities" [1];
- "Evaluate capabilities of individuals, organizations and systems" [1];
- "Measure knowledge, ability, endurance and/or capacity" [1];
- "Train the participants and provide an opportunity to gain knowledge, understanding and skills" [1].

Although international taxonomy for different types of exercises doesn't exist, there are widely known exercise types in use. As exercises could be planned with different

purposes, their size, price and challenges may vary. It is possible to differentiate between discussion-based exercises and operations-based exercises. [15]

According to Homeland Security Exercise and Evaluation Program (HSEEP) exercise complexity, such as needed capacity and planning time, varies in different types of exercises [19]. Seminars planning require much less time and capabilities when compared to drills, for example. Figure 1 provides insight into the building blocks complexity.

Figure 1. HSEEP building-block approach [19].

2.1. Discussion-based exercises

Discussion-based exercises only concentrate on discussing strategic and policy-focused topics [20]. They enable participants to learn existing policies, processes and/or help to develop new ones and assess decision-making procedures. Discussion-based exercises are for example seminars, workshops, tabletop exercises (TTXs) and games. [15]

2.1.1 Seminars

Seminars could be organized as conferences for example and in general they focus on giving guidelines and/or discussing various topics, such as processes, policies, procedures, different concepts and thoughts for example [15]. Seminars could give essential input to people, who are creating and/or modifying processes and procedures [20]. Seminars could also give insight into the new and/or modified workflows for example [15].

2.1.2 Workshops

Workshops are like seminars, except participant involvement is larger and they focus on creating new procedures and concepts. Workshops are considered to be efficient when there is high participation rate among the important stakeholders. Furthermore, workshops are concentrating on concrete issues and should have clearly stated goals. Workshops results could be, for example, developed standard operating procedures (SOPs), emergency plans and common agreements. [20]

2.1.3 Tabletop exercises (TTXs)

In tabletop exercises, participants play through a theoretical situation or a crisis by discussing processes for reacting to different scenarios [15]. TTXs purpose is to increase overall awareness, ensure plans and procedures preparedness to protection, investigation and mitigation for various incidents. Furthermore, to validate processes for response and recovery, in case of various simulated emergency situations. TTXs aim is also to identify advantages and disadvantages in order to determine needed improvements. [20]

2.1.4 Games

Games are like tabletop exercises, with the difference, that games include simulated operations and participants are divided into at least two teams. Teams are solving their exercise tasks individually in competitive environment. [15] Games focus on players' verdicts and various actions outcomes and they are played relying on different rules and procedures, like the rest of the games. Games are commonly used for validating existing processes and plans. [20]

2.2. Operations-based exercises

Operations-based exercises focus on playing out real reactions and behavior to exercise scenarios. For example, start communication between entities or invite people to the scene. Such exercises are commonly used for validating plans and processes in practice. They allow specifying different roles and tasks, as well as determining shortcomings in resources. Operations-based exercises are for example drills, functional exercises (FEs) and full-scale exercises (FSEs). [20]

2.2.1 Drills

Drills are controlled exercises that focus on rehearsing with new equipment, validating processes and plans or testing and retaining existing skills. The participants should previously know the plans and processes to perform drills. Drill is usually held in an individual organization, but a series of drills allow multiple institutions to participate in full-scale exercises. [20]

2.2.2 Functional exercises (FEs)

Functional exercises are held in a real-time environment, although part of the staff is generally simulated. In order to simulate real events, scenario components are additionally injected. Purpose of functional exercises is to assess existing capabilities and functions. They concentrate on plans, policies, processes and personnel from administration. [20]

2.2.3 Full-scale exercises (FSEs)

Full-scale exercises are generally held in an intensive real-time environment, where personnel and resources are gathered to the field. They start to solve the tasks like there was a real crisis situation. Full-scale exercises are the most comprehensive type of exercises, which require multiple resources and organizations during the designing and exercise execution phases. Issues described in the scenario are realistic and they also require efficient, quick reactions by the participants. FSEs help to assess cooperation, coordination and readiness for crisis situation. [20]

2.3. Levels of exercises

U.S. military doctrine states that in military context, strategic, operational, and tactical levels of warfare connect tactical operations and accomplishments of national goals. Borders between these levels are narrow, but having different levels of commands separated, allow more efficient operations planning. In addition, resources evaluating and distributing, as well as appointing tasks to the corresponding people. [21]

Estonia also recognizes these levels and both U.S. and Estonia uses the same hierarchy model, by categorizing the levels according to the activities and decision making levels [22], [23]. The lowest level from the hierarchy is tactical, middle level is operational and the highest level of power is strategic [21].

- "Tactical level" – On the lowest level, battles and operations are organized and conducted according to the tasks assigned to the forces, with the intent of achieving military goals [21], [22], [23];
- "Operational level" – Medium level is considered to be the bridge between tactical and strategic levels [21] and it focuses on coordinating and executing operations or a set of related operations [22], [23];
- "Strategic level" – On the highest level, national strategy objectives and policies are created, and decisions are highly depended on political objectives [21], [22].

When it comes to decision-making in case of crisis, there are usually two types of decision-making approaches in use:

- "Analytic decision-making" – Multiple solutions are produced and evaluated to various criterias and based on it, the most suitable action is selected. It is a methodological approach and it takes into account the analytical argumentations. It can be only used when no urgently made decision is needed; [24]
- "Intuitive decision-making" – This approach focuses on wider picture and it is evaluating current situation rather than comparing several possible choices. Intuitive decision-making takes less time than analytic decision-making and it is more often used in the tactical level. [24]

Commanders tend to avoid decisions that are done solely based on intuition and combine both approaches in order to be objective and make right on time and efficient decisions [24]. Those approaches are not only useful in military context, but also in other fields, like cyber security.

Three levels of command concept is also brought in to the cyber security exercises and each level represents the different type and decision-making level [25], [26]. European Union exercise called Cyber Europe covered all those levels for the first time in 2014 [10], but on separate phases. Instead of tactical level in military field, technical concept was used and the exercise was divided into three phases [26], each phase covering one the following levels:

"Technical level exercise" (TLEx) participants were technical level specialists from public and private CERTs [25]. Technical level exercise covered, for example, detecting,

investigating and mitigating various incidents consequences, and also exchanging information between the same level experts [26].

"Operational level exercise" (OLEx) participants were crisis management crews from cyber security institutions, private organizations and national CERTs [25]. This operational level exercise phase covered situation assessment, analysis, also collaboration and counselling. Similarly, like technical level, exchanging information between the same level experts and tactical level. [26]

"Strategic level exercise" (SLEx) participants were experienced employees from national institutions, responsible for managing crisis situation [25]. This phase covered the making of strategic decisions, handling effects on high-level and also public relations [26].

2.3.1. Exercise characteristics

Exercises can be also characterized by the roles one or another team playing in different exercises types. Furthermore, complexity level and resource needs also vary. Thomas Svensson, Swedish cyber security exercises expert, have proposed triangle interpretation for showing the differences. [27] See Figure 2, Figure 3 and Figure 4 for illustrations.

On tabletop exercise, which is driven by the scenario, blue team (BT) is playing different roles and includes different areas specialists (technicians, lawyers, public relations, management, etc). Red team (RT) barely exists. White team (WT) is concerned with roleplay and green team (GT) with communication. Scenario plays the important role in tabletop exercise, also BT and WT focus and resource need is high. However, GT and RT resource necessity is low, as they don't have the focus during this type of exercise. [27]

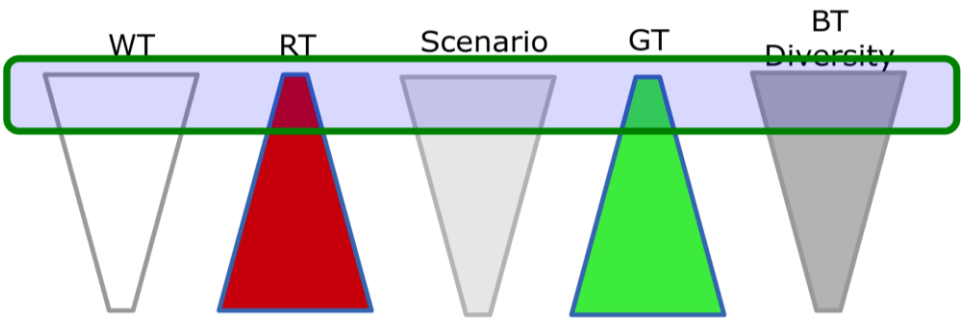

Figure 2. Tabletop exercise characteristics [27].

As for pure technical cyber defense exercise, it is not depending on the scenario, BT plays the same role during the exercise, as it includes uniform profile specialists (technicians). RT pressures at the same. GT is responsible for providing the challenging environment and WT for supervision. During technical cyber defense exercise, GT and RT are on focus and they need the most resources. WT, scenario and BT resource necessity is low. [27]

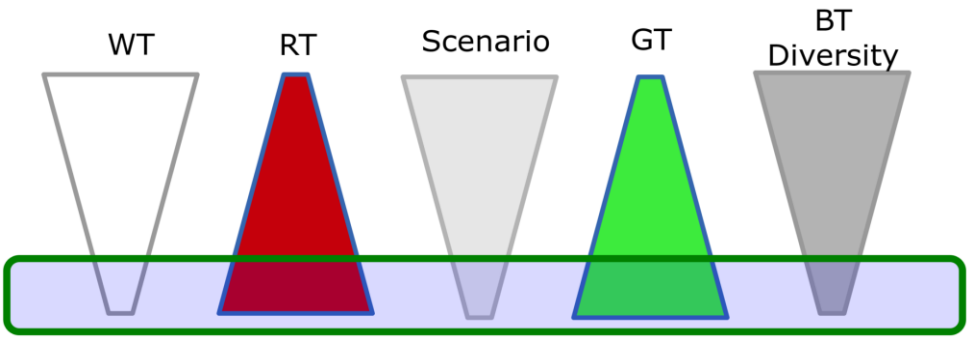

Figure 3. Technical CDX characteristics [27].

When it comes to Locked Shields, for example, then BT is still playing the same role, as it includes uniform profile specialists (technicians). Scenario is driven by RT objectives, it is also a base for injects and the same injects goes to all teams. Scenario and WT resource need is high, similarly like RT and GT, which are even more on focus. BT has the lowest resource need. [27]

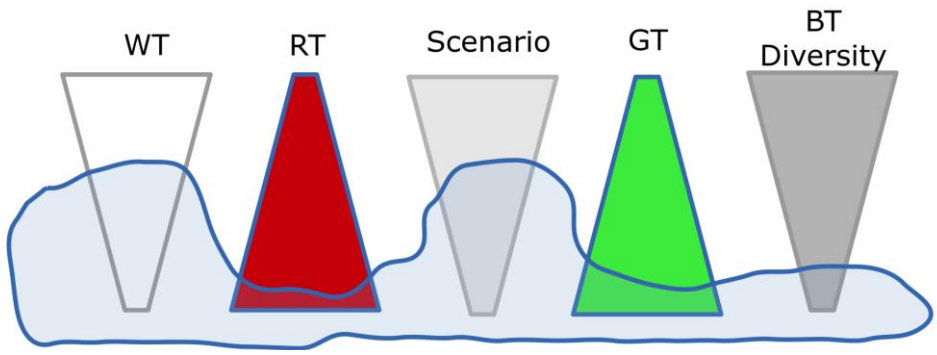

Figure 4. Locked Shields characteristics [27].

2.4. Exercises in Estonia

Both national and international exercises are conducted in Estonia.

2.4.1 KüberSiil (EST)

Kübersiil is so far the biggest cyber security exercise in Estonia that was held in autumn 2015. There were more than 100 people involved in the training and 21 entities took part (including national security, public and private vital service providers). The purpose was

to rehearse the applicability of comprehensive cyber incident's resolution plan. It included emergency response agencies responsibilities and rights, involvement of the partners, readiness, and information exchange arrangements and also the internal processes of RIA. Responding to emergencies, both operational and strategic levels were practiced in headquarters. Even though it was not a technical exercise, emergency management in cooperation with agencies was practiced in real time. [8]

2.4.2 CONEX (EST)

CONEX is a strategic level cyber security exercise that took place in April 2015. The purpose of CONEX was to evaluate existing procedures. Furthermore, the aim was to assess the presence and the use of legal actions in order to resolve the event and to raise awareness of the arising legal gaps. In result, conclusions on different parts of the exercise drew up 120 different proposals, which ministries and agencies could carry out in the coming years. [9]

The main outcomes from the exercise were:

- Increased government awareness of security risks [9];
- Exercises conducting competence were raised [9];
- Identified a number of opportunities within the legal system, ways to increase the ability of different agencies to respond to the risks arising from the events [9].

The exercise scenario included cyber-attacks and data leakages on ID-card infrastructure, data communications networks managed by public and private institutions, population registry, e-residency and vital services (energy and shipping organization). The findings of the exercise resulted in complementing the Government Action Plan. [8]

2.4.3 Cyber Europe (EU)

The Cyber Europe exercises are mimicking cyber incidents, which are so large in scale that they can turn into cyber crises. Exercise participants are investigating technical incidents and also handle severe crisis management scenarios in organizations. European cyber specialists are responsible for developing Cyber Europe scenarios that are crafted from real life situations. First cyber Europe exercise was held in 2010 and it is conducted in every 2 years. [28]

2.4.4 Crossed Swords exercise (NATO CCD COE)

Crossed Swords exercise is technical cyber exercise, which is focused on penetration testing and security experts. During the hands-on exercise in a simulated environment, participants are solving various complex tasks. The main goal of the exercise is developing technical capabilities in a responsive way. [29] Exercise tasks also include various forensics tasks, such as evidence collection, gathered data analyzation, identification of malicious actions [30].

2.4.5 Locked Shields (NATO CCD COE)

Locked Shields (LS) is the largest technical cyber defense exercise, which is held since 2010. Its target group is national security specialists whose profession is to defend IT systems in their organizations. LS exercise is held once a year and it is conducted in real-time. Locked Shields 2016 had more than 550 participants from 26 different nationalities, which was also a highest ever number of participating teams. Locked Shields is outstanding in using real-life technologies, networks and attacks. [31] Additionally, LS scenario consists of media and legal injections, which refers to the fact, that exercises are not only concentrating to forensic and technical network complexities [30]. For the first time in April 2017 LS brings together the decision making with strategic level, while maintaining the focus on technical level [32].

2.4.6 Cyber Coalition (NATO)

Cyber Coalition is the biggest international cyber exercise organized by NATO. It has been held in Estonia already four times. Cyber Coalition exercise in 2016 included over 700 participants from the NATO Alliances. [33] The purpose of the exercise was to rehearse existing processes and collaboration between national specialists handling different scenarios. Exercise was held in a simulated environment and all participants were solving scenarios, which involved various threats, like malware or spyware and hacking of prescribed networks. [12]

2.4.7 Summary of exercises

Cyber security Exercises described in Chapter 2.4 differentiate from each other by the organizer and the level of exercise, which can be seen from Table 1.

Table 1. Exercises differentiation.

Exercise	Organizer	Level of Exercise
KüberSiil	National exercise of Estonia	Operational, strategic (multiple levels are rehearsed on separate phases)
Conex	National exercise of Estonia	Strategic
Cyber Europe	European Union (EU)	Technical, operational or strategic (multiple levels are rehearsed on separate phases)
Locked Shields	NATO CCD COE	Technical
Crossed Swords	NATO CCD COE	Technical
Cyber Coalition	NATO	Technical, operational or strategic (multiple levels are rehearsed on separate phases)

2.5. Planning components

Prior to planning an exercise, whether it's cyber related or any other field exercise, it is crucial to have clearly stated needs for designing an exercise [13], [15], [34], [35]. Exercise designer should also identify constraints for the exercise, and formulate the process for organizing the exercise. Next step is to agree on measurable goals that should be achieved by the exercise participants and choose the participants. [13] Furthermore, it is thought, that resources needed for the exercise should be planned precisely [15].

2.5.1. Roles in exercises

Different roles for the exercises can be found from Table 2.

Table 2. Roles in exercises [15].

Role	Description
Organizer	This role leads the exercise designing, such as choosing the exercise objectives, organizing teams and assigning resources for conducting the exercise.
Planner	Institutions or people who are a part of designing the exercise.
Participant	Institutions or people who plays their part during the exercise. Some persons could be selected to participate in the exercise, and some to participate in the designing phase.

Exercise Director, Moderator or Leadership Team	Individual or a crew who is leading the exercise, whose obligations are for example to be a central contact in case of questions and concerns, preparing the exercise environment, initiating and finishing the exercise, administrating scenarios etc.
Monitor or Facilitator	Those roles are usually overlapping and obligations are to provide information regarding the situation prior the exercise and to add injects during the exercise. They also observe participants' behavior, verdicts and shortcomings during the exercise. Furthermore, they give relevant input in order to assess the exercise.
Observer	Institutions or people whose purpose is to only observe during the exercise. They can be for example institutions that are left out of the scope, due to not having a role during the exercise.
Evaluator	People whose purpose is to assess the exercise and its effectiveness. They could be the same people or teams who were also participating in the exercise designing phase or during exercise execution.

2.5.2. Lifecycle

According to ENISA report "Good Practice Guide on National Exercises" exercise lifecycle broadly involves following steps:

- **"Identifying the exercise"** – In the first phase determines the designer's reasoning for conducting an exercise. It should, for example, contain the need for rehearsing decision-making levels, improving technical capabilities, procedures or plans. Exercise type and participants are chosen according to the identified need; [15]
- **"Planning the exercise"** – Planning process include multiple activities, such as choosing corresponding teams, receive funding, reserve training location, creating a scenario together with its rules and exercise documentation. Moreover, clarifying participating players, their tasks and responsibilities and also planning exercise assessment; [15]
- **"Executing the exercise"** – In this phase is conducted the exercise, where participants follow the pre-written scenario, developed in the designing phase. It will be done whether by discussing or also playing it out, like it is the real crisis, with the purpose of testing verdicts and processes. Reactions are observed and information is injected to the scenario; [15]
- **"Evaluating the exercise"** – Final step is to assess achieved results, write assessment reports, sometimes multiple ones to various actors. Report gives an

overview of the exercise, determined shortcomings and provides improvement areas and additional suggestions. [15]

Training audience for the exercise is chosen according to exercise needs and goals [13]. It is thought that tabletop exercises are not good for developing competencies, because the rehearsing environment should be close to reality [36].

There are ideally three exercise planning conferences for a single exercise:

- "Initial Planning Conference (IPC)" – 8-9 months before the exercise [37];
- "Main Planning Conference (MPC)" – 5-6 months before the exercise [37];
- "Final Planning Conference (FPC)" – 2-3 months before the exercise [37].

Another aspect to consider during designing an exercise is to make verdicts regarding media as collaboration with media has essential role during the crisis. Media could be, for example, only informed regarding the upcoming exercise or to validate their role and actual procedures during the exercise. [15]

All types of exercises, including technical and operational level exercises, rehearse collaboration. Also, designing phase doesn't differ much between them, only identified objectives and target groups may vary. Decision making exercises should be held regularly, because the capability of making decisions in stressful conditions is generally tricky and unclear. In decision-making exercises decision makers should face circumstances, where mandate related questions, collaboration and information exchange are played through. This also includes reporting and various other activities. [13]

2.5.3. Objectives

Exercise objectives should be created by the rule of SMART (Specific, Measurable, Achievable, Relevant, Time-bound) [20] which are further discussed in Figure 5 .

SMART Guidelines for Exercise Objectives	
Specific	Objectives should address the five Ws- who, what, when, where, and why. The objective specifies what needs to be done with a timeline for completion.
Measurable	Objectives should include numeric or descriptive measures that define quantity, quality, cost, etc. Their focus should be on observable actions and outcomes.
Achievable	Objectives should be within the control, influence, and resources of exercise play and participant actions.
Relevant	Objectives should be instrumental to the mission of the organization and link to its goals or strategic intent.
Time-bound	A specified and reasonable timeframe should be incorporated into all objectives.

Figure 5. SMART guidelines for exercises objectives [20].

The same logic for setting exercise objectives applies to military exercises [20] and as well to cyber exercises for example [13], [15]. It is believed that if objectives are not measurable, is not possible to have efficient assessment in the evaluation phase [37]. Moreover, it's also recommended to limit the amount of objectives to assure exercise manageability [19], [20], [38].

The author of the thesis brings out one simplified hypothetical example that meets these SMART objectives in a technical level of the exercise:

Database administrator must recover corrupted database DATABASEx from server SERVERx backups within 1 hour, to meet database availability and integrity requirements.

It corresponds to SMART rule, as:

- Who – database administrator;
- What – recover corrupted database from backups;
- When – database is corrupted;
- Where – server;
- Why – to meet database availability and integrity requirements.

Furthermore, it is possible to measure:

- Whether the goal is achieved successfully, partially or not at all.
- Whether the task is completed with 1 hour.

This is achievable goal, as database administrator has a responsibility for only 5 databases and as well should have the competency. This objective is relevant, as it shows system

administrator preparedness. System administrator should figure out during the exercise, which database from which server to recover, in order to follow the exercise scenario.

2.5.4. Scenario

Scenario development in the planning phase needs high attention because it has to reflect reality [14], [15], [19], [37], [39]. Organizer is able to do that if she/he comprehends how the participating institutions operate and react to various crisis situations. It is recommended that delegates from cooperating entities would be included into scenario creation. Scenario should also allow some resilience and various reactions by the participants, because people tend to behave in contrary than presumed. [15] Furthermore, it is recommended to have a possibility to insert injects during the exercise, in case of a deflection, which could help to lead back to the planned track [40].

3. Analysis of interview results

This chapter concentrates on reviewing and discussing interview results. Names for interviewees can be found from Chapter 1.3 and interview questions in Estonian language from Appendix 1.

3.1. Identified shortcomings of cyber security exercises

3.1.1. Too many exercises

During the research interview, nine out of thirteen experts agree on that there are currently too many cyber security exercises. It was brought out by one of the interviewed specialists, that most months in a year there are exercises or planning of exercises. Additionally, it was pointed out that there is a tendency in Estonia to conduct a lot of exercises, but the quality of them tends to be rather poor. Two of the interviewees reckon that there should be fewer exercises, but rather consolidated ones. The third expert also agrees, but in comparison, he claims that fewer exercises should contain more different parties. Furthermore, it was stated by the professionals, that exercises should firstly always have a valid reasoning for conducting them and there shouldn't be an exercise for the sake of just having it. The author agrees that there's no reason to conduct an exercise without the actual need. She also believes that if there are too many similar exercises, people might lose interest to participate.

3.1.2. Lack of national strategy

Two interviewed specialists pointed out that Estonia should develop its state-wide cyber security exercises strategy, which would regulate needed exercises, their goals and priorities along with international ones. Also, if there would be inadequate amount of international exercises to choose from, it should be compensated with planning essential national exercises. The author of the thesis agrees that exercises strategy would help to regulate the amount and quality of designed exercises and allow to concentrate on essential domains. One expert brought out that organizers should ideally see their exercise plans four years ahead, because it allows to spread exercises for different sectors between years. The author thinks that if there were national cyber security exercises strategy, various fields would be covered more systematically.

3.1.3. Same organizers and participants

Four out of thirteen interviewed specialists pointed out that there's usually the same group of people who are designing exercises. Two interviewed experts claim it is a problem, because the same people, who organize them, should also be participating time to time instead of always designing them. As Estonia doesn't have people who are concentrating only on planning exercises, they are being designed besides the other tasks at work. As a result, it's not possible to put full effort into planning them. Two interviewees brought out that it would be good if there were special teams who are only responsible for designing exercises, but as Estonia is a relatively small country, this idea probably would not be rational. The author thinks that the quality of exercises would rise, if there were concrete teams whose main and only responsibilities are to design cyber security exercises.

As the same group of people usually organizes exercises, four interviewees brought out that there's likewise a group of people who also generally participate on exercises. The author believes that, on the one hand, it's a good that the same participants are prepared for various incidents, but on the other hand, there are also others who could use the experience. One expert suggested that to cover larger groups, exercises participants should be divided between different years. The author believes it would assure, that instead of narrow target groups, wider number of specialists would have the knowledge. Furthermore, it was suggested that there could be special paid teams, whose main job is to participate on different exercises. The author thinks that it probably would not be feasible, like having special teams for designing exercises. One interviewed specialist pointed out that after-growth for the experts is slow and there should be more promising students. The author shares his opinion, as Estonia has a lack of qualified IT personnel.

3.1.4. Small participation rate

Four experts brought out during the interviews that vital services providers in Estonia tend to have too small participation rate on cyber security exercises. At the same time, one expert pointed out there's no real issue, because some vital services providers are just more passive or active than the others. It was also thought that it's not possible to cover every area at once and each year should concentrate on different areas. One expert thought

that organizations are sometimes chosen to exercises through better familiarity, instead of giving a chance to other institutions, so they could also get exercise experience.

Two interviewees thought that every vital services' provider should participate at least once a year in some cyber security exercise, one of them even proposed they should have this as an obligation. Some vital services providers' awareness is lower than others and they probably don't consider exercises necessity until some bigger incidents happen to them. Two of the specialists suggest that vital services providers should have specific crisis management exercises, rather than general ones. The author thinks that it's essential to cover more vital services providers and raise their awareness that specific cyber security exercises are also needed for them.

3.1.5. Objectives measuring tends to be subjective

Smallness of Estonia has its magic and pain, because in cyber security community everyone usually knows each other by the name and they know who to turn to in case of issues. Unfortunately, at the same time there seems to be a tendency of giving soft feedback to exercise participants. One expert brought out that usually in Estonia, if partner institutions don't exactly succeed in exercises, they get illustrated feedback instead of strict and constructive one. He also asserts that institutions should get strict and measurable feedback, what is comparable to others, so every organization would see which their weaknesses are and where they should make improvements.

Four interviewees out of thirteen stated that measuring objectives in Locked Shields exercise is objective, because points are given in seven different categories, which allow seeing categories with weaker results and also providing feedback about what went wrong. However, one expert pointed out that evaluation is not standardized in different levels and as a result, evaluation is rather subjective than objective. Eight specialists out of thirteen brought out that objectives set to exercises are often not well measurable or measuring is rather subjective. The author believes that if objectives are stated qualitatively and vaguely, for example, to develop cooperation or gain knowledge, it makes objectives difficult to measure. At the same time one expert brought out that strategic level exercises are not assessed purely on the basis of the metrics. Usually there are evaluation teams who observe the exercise and make notes. The author thinks that

such measuring is rather subjective, because it depends on the people, who are on the evaluation teams, and whether they are measuring adequately.

When it comes to measuring objectives, for example, NATO exercise Cyber Coalition, three experts out of thirteen brought out that this exercise has specific role called local trainer, who measures goal achievements. One of the interviewee pointed out, that such measuring is rather subjective and it requires trust towards the local trainer to believe measuring is done objectively. In comparison to the first expert, another expert claims that in Cyber Coalition technical level exercise objectives are well measurable, whereas setting and measuring indicators are subjective. The author believes that exercises feedback and measuring should be time to time reviewed and improved. Furthermore, measuring should be objective rather than subjective. One expert pointed out, that too much bureaucracy should be avoided, because it would become more important than exercise itself and this is not something to desire.

3.1.6. Conclusions are rarely taken seriously

Six out of thirteen experts pointed out that in Estonia results gathered from exercises are not always taken seriously and they don't make it into the work plans. Few of the reasons why this happens, according to the interviewees, is that some modifications need bigger resources, there is a lack of motivation and interest or changes in legislation takes time. Even the final report for the exercise might be left undone. One expert brought out that there's no central crisis management institution, which would deal with lessons learned. Furthermore, usually exercise organizer deals with lessons learned, but it's not standardized procedure and it may vary in different institutions. At the same time, another expert has an opinion that exercise recommendations implementation should be looked as different audits, where tasks are divided between multiple people, who keep an eye on the tasks and ask feedback from time to time in order to see if there is any progress. The author believes it is a great idea, because if there's no supervision after the exercise, some important changes might be left undone.

3.2. Exercises planning

Two interviewed specialists brought out that when planning exercises there's often a problem with methodological choices. They believe that exercise organizers sometimes don't think through the exercise planning methodology, such as which objectives to set and how to evaluate the results. One specialist pointed out that resources should be evaluated and planned more precisely and it would be interesting to see a business case and cost for designing one exercise. He asserts that it's essential to agree on how to design the exercise, because it's not always clear whether the exercise will be for only technical specialists or it should also include operational level. Moreover, when planning an exercise, all of the counterparties should be aware of the times and tasks, which are expected from them. It was also pointed out that there are currently no instructions in Estonia for designing multi-level cyber security exercises. To avoid misunderstandings and resentment, concrete time frames and milestones should be agreed on beforehand. The author agrees that there will be fewer surprises afterwards, if agreements are previously coordinated and thought through.

Four interviewed experts out of thirteen pointed out that exercises scenarios have to be realistic, flexible and organizers should be able to react accordingly, if scenarios need additional injects or time plan needs to be modified. Three interviewees brought out that when everything goes during the exercise like previously planned, exercise planning is questionable, because then there's no room for real life. Even during exercises has to happen something unexpected for the players, because in real life nothing happens like it's planned. On the contrary, one expert pointed out that exercise is well designed if there is no need to make changes to scenarios or to the exercise logic during the exercise. The author of the thesis claims that it all comes down to the proportions of needed changes. It was also brought out that exercise is well organized when objectives are being reached and when players and organizers are pleased as well as they have learned something new. The author agrees and thinks that if exercise didn't teach participants anything, the exercise shouldn't have been held.

When it comes to the international exercises, then Locked Shields and Crossed Swords exercises planning cycle is one year. On contrary, in case of Cyber Europe, planning cycle is two years. One interviewed specialist pointed out that it takes eighteen months in order to plan a perfect exercise. He adds that it might be also possible to plan an exercise with

less time, but it all depends on the quality of scenario, objectives and whether all the necessary people are included. The author believes that the main organizers may have the designing experience, but participating counterparties, who have also tasks for the exercise, may not have the know-how. As a result, hurrying may affect exercise negatively.

Two interviewed specialists brought out that designing of international exercises is mainly divided into four parts. Those are initial, main, final planning conferences and after action review. Some exercises also include test-run and between conferences are various other actions. They also pointed out that national exercises' planning is not that strictly structured. The logic for planning those exercises is to meet and talk, but concrete separable milestones are not being set. However, another two specialists disagreed, they reckon that exercises in Estonia have similar international planning conference system. Specialists brought out that after action review is always essential in international exercises, but there's a tendency to leave this part out in national cyber security exercises. Even if suggestions are proposed, they rarely make it to the action plans. The author believes there is a need for such after action review, to summarize the exercise and what went well, what could be improved etc.

3.2.1. Reasoning for conducting exercises

Two interviewed specialists pointed out that the purpose of exercises is to always gain new knowledge that wasn't known before. On the contrary, another two experts say that exercises covering already known issues can help to solve the issue or to convince higher managers that various changes are needed. It is so because in case or real incidents, the situation can escalate quickly and may result in great material damage or even a human loss for example. The author agrees, because exercises can be both either conducted to discover something new or to demonstrate certain issues. One expert brought out that there are serious problems with not only cyber security exercises, but also with other fields' exercises. This is due to the fact that people don't understand the real purpose for planning these exercises and formulating exercises objectives. Sometimes it's enough to just carry out an analysis instead of the entire exercise.

3.2.2. Target audience selection

Nine interviewees pointed out that the target audience is generally chosen based on the exercise objectives, but it's always a challenge with who to include or leave out. Three specialists brought out the train as you fight principle, so exercise participants should also be the ones responsible for solving the incidents in real life. When it comes to international exercises, one expert brought out that countries tend to send their representatives to participate, rather than those who should be actually solving the incidents in real life. This happens because countries want to show themselves from a good perspective, as after the exercise, media releases will cover who "won". One interviewed specialist pointed out that if substitutes were participating on exercises, they would also consult in the case of real life incidents. In contrary, another expert thinks that if the key person is missing from the training, he/she doesn't have the knowledge in case of a real-life event and things can go wrong. The author agrees that key personnel should participate instead of substitutes and gain the knowledge, how to react in different cases, because substitutes may not be available to assist in real crisis.

3.2.3. Well-organized exercises

In terms of international exercises, four interviewees consider Locked Shields and Cyber Coalition to be the two best cyber security exercises. Locked Shields' advantages are its stable exercise management team who know what they want to achieve and their technical platform is efficient and good. Moreover, objectives are well defined and measured. Similarly, Cyber Coalition has well defined objectives, but differences rise from its interesting structure, which makes possible to choose incidents from different story lines. The only disadvantage to Cyber Coalition is its continuously changing exercise management, which leads to scenarios that are not that strongly connected. In regards to Estonian exercises, two interviewees pointed out Kübersiil, which has been the biggest cyber security exercise so far. Objectives set for the exercise were precise. One expert believes that exercises which cover all the levels should be planned at least once every two years, whereas other expert pointed out they should be designed no often than once every four years.

3.2.4. Exercises criticism

Two experts pointed out that CONEX exercise, that included five different focus areas, had the weakest objectives when compared to Kübersiil. However, CONEX exercise focus areas had different people responsible for the objectives. The exercise tried to solve unreasonably large number of incidents and issues, and as a result, exercise planning quality and exercise itself suffered. At the same time, one expert disagrees and asserts that all the formalized objectives and sub-objectives were assessed. Moreover, future improvement areas and related tasks were identified and divided between entities. When it comes to the international exercises and Cyber Europe for example, then representatives from different countries should collaborate, in order to propose suggestions that would be taken into account. Furthermore, Cyber Europe 2016 had both technical and operational levels represented during the exercise, but coherence between the levels was not identified. The author asserts it shows that even though multiple levels could be included into the exercise, the levels are not that strongly connected as they should be.

3.3. Multi-level exercises

All interviewed experts brought out that at least two levels should be represented in one exercise in order for it to be multi-level exercise. Nine interviewees brought out that during multi-level exercises information should move between levels and commands should be sent from upper levels to lower ones. Also, if all the levels are included, but they don't influence each other, they are rather single level exercises that are conducted in parallel on the same time. On contrast, one specialist has an opinion that it is the matter of agreement, whether different levels communicate between each other or not. The author agrees with majority and believes that if levels are not communicating like they do in real life, those exercises could be as well conducted separately and in this case, they are not called multi-level exercises.

Two interviewees have participated in Cyber Europe, but according to them, connection between different levels was weak. Three interviewed specialists have participated in Cyber Coalition and one expert brought up that likewise with Cyber Europe, different levels connection was weak. Three interviewees have also participated in Kübersiil and another three in Baltic Host. Two interviewed experts have experienced multi-level exercise, where CMX and Cyber Coalition were brought together. As the exercises were

put together without fully organizing them from scratch, in the end exercise was not successful. Also, there are multiple Police and Border Guard Board and Estonian Defence Forces non-cyber exercises, where multiple levels have been practiced simultaneously and successfully, but they are not further discussed during the thesis.

3.3.1. Advantages of multi-level exercises

Six specialists claim as there are multiple levels in real life, they should be also rehearsed together in order to avoid bottlenecks that may occur during incidents. There should not exist so-called "exercise world", where different laws of physics apply as opposed to real life. Those exercises help test procedures and legislation, because exercises are the only safe way to find out shortcomings without actual loss in real life. Exercises also allow testing of communication between parties and seeing how information changes within hours. The author agrees with interviewed experts and thinks that different levels communication procedures and bottlenecks should be discovered before major real-life incidents occur.

Additionally, it was brought out that because there haven't been many large international cyber crises so far, the international multi-level exercises can provide that experience for future sake. It will assure that in case of real crisis countries have tested their procedures and know how to act. Although exercises allow teams to see their behavior in stressful situations, one expert thinks that causing stress in people shouldn't be the purpose of the exercises. The author disagrees, because if people are used to calm situations, they might discover, that they cannot handle the pressure in crisis. Essential people, who are responsible for solving the crisis, should be prepared for stressful situations and exercises are a good place to increase their readiness.

Two interviewed specialists assert that multi-level exercises help managers to realize, that actions on lower levels could affect higher levels. There's a saying in military sphere that plans are efficient until the first bang and as a result, all the plans needs to be changed. This is said because things never happen in real life as planned. Moreover, one specialist claims that multi-level exercises also help to save time, because it's possible to play through the whole escalation along with procedures and decisions, during a short period of time. It brings out bottlenecks and gives a clear overview on how a country reacts to different occasions. Furthermore, one interviewee asserts that multi-level exercises

produce more learning outcomes. He also adds that organizers cannot produce as much real-life injects, like technical level could, during multi-level exercises.

On contrast to the opinion of twelve interviewees, one expert pointed out that it's generally more useful to focus on one concrete level, because additional levels change the overall structure of the exercise more difficult. According to the expert, world exercises trend is heading to the direction where exercises are focusing on concrete levels. He also adds that people are more and more starting to use tabletop exercises, but one specialist commented that tabletop exercises are only good for the exercise pre-phase. Also, two other specialists agree that it's not possible to test information exchange or solve technical incidents on papers. The author agrees and thinks that, according to the exercise type, various exercises require different approaches.

3.3.2. Challenges and solutions

Seven interviewed specialists brought out that designing multi-level exercises require more resources, such as people and money. When compared to single-level exercises, adding more institutions and levels make the overall cost higher. As for planning multi-level exercises, there should be a long planning cycle for identifying possible bottlenecks and their mitigation possibilities. At the same time, one expert reckons that if multiple institutions are participating, at least one person per institution is also needed for the planning phase. According to two interviewees, when comparing to single-level exercises, organizers should add approximately six months to the planning phase in case of multi-level exercises. One specialist asserts that multi-level exercise can't be a tabletop and technical exercise at the same time, it should rather be a collection and combination of elements from different levels, which results in something completely new. Moreover, two experts pointed out that people should be trained to be flexible and dynamic. As a result, they are not only able to read the manuals, but can also act according to the situations.

Five interviewees brought out that it's a challenge to create a scenario for different levels so that the levels don't get stuck or bring other levels off the desired course. One interviewee pointed out that it's difficult to think of an incident into the exercise scenario, that requires higher-level participation. Moreover, another specialist asserts that it is a challenge to make different levels communicate and to escalate the situation to higher

levels. It helps when different level specialists would also be included into scenario creation. In addition, it was suggested to leave room for improvements whether there's a defect that needs elimination during an exercise. The author agrees that when planning multiple level exercises, people from different levels should be also participating in scenario development and in overall planning process.

In addition, seven interviewees reckon that it's a challenge to make higher-level people to participate. One interviewee suggests that if they are already participating, things should be played through a little bit faster than they actually take in real life. Also, it was suggested to put strategic and technical levels together for approximately an hour to allow strategic level to see what's going on during the exercise on technical level. Another proposition is to allow people start solving their exercises tasks from the location where they are currently located. It also applies for the other levels, but if people aren't together, they might be less motivated. The author thinks that it's worth trying different involvement measures on the higher-level decision makers, because if it's difficult to make people to participate, it means that the current measures to gather people today are not working.

Five people pointed out that sometimes people are not motivated to participate in exercises. In addition, people could be motivated to participate in exercises via bonuses, like getting a day off from work. In a worst-case scenario, if they decide to ditch the exercise without a valid excuse, they could be fined. Some people would also consider it as a motivation, if during the exercise there's food and some social elements included. The author thinks that sometimes people indeed need a little additional motivation. It may be an excellent idea to offer a day off, free catering during the exercises or similar bonuses. According to the author it's also fine to assign repercussions, if people don't take vital exercises seriously.

Furthermore, six experts brought out that there's a language barrier between technical level specialists and upper management. It's sometimes difficult to understand what is important to different levels. In addition, if exercise participants and/or planners don't speak English as their native language, it makes things even more complicated, because mistakes could be easily made already in exercise planning phase. Three people suggest solving the different level communication problem with advisors, who provide translation between levels. One specialist pointed out that sometimes even advisors are not

competent enough. He claims that people should be hired through competence exams, to ensure their suitability for certain positions. Moreover, he believes it would be the ideal case if managers and advisors were raised from lower levels into higher ones.

Another challenge for planning multi-level exercises is to break timely dimension, which means that time on technical level goes many times faster compared to operational or strategic levels. One expert pointed out that there are also different reporting cycles, when different levels obtain new information. Eleven interviewees agreed that there is a time difference on different levels. Six experts suggested that for trying to tie those time dimensions, technical level should start an exercise a little earlier than operational level and synchronize during contact points. Four specialists suggested playing with time jumps that allow time to move faster on different levels. On contrast, one expert claims that time jumps are rather confusing than helpful. In order to use time jumps, different level contact points should be determined. In addition, one interviewed specialist says there is also a way, which is not very good, to let players consciously wait as decisions are being played out in higher levels. Similarly, one specialist believes that incidents and escalation process should be fully played out as in real life. According to him, if there were only 1-3 incidents during an exercise, not like in todays' exercises, it would be doable. The author believes that solving fewer incidents during the exercise would help to keep participants focused. Although she disagrees with the expert who is suggesting to fully play out escalation process in real life, because even if there were less incidents during the exercise, it would be still too time-consuming.

One expert pointed out that it's not possible to design one exercise, where all the levels would be included. For example, timely measurements are together, commands move from up to down, the information accumulates and be sent back up – which just takes too much time for one exercise. The author believes that the statement is valid to some extent. It's right that escalation process, decision-making, information exchange between levels takes time. Although, if exercise would solve only few incidents, contact points would have been previously determined and also time jumps are used, it's possible to plan that sort of an exercise.

Finally, it was brought out by one of the interviewees that exercise's technical environment and licenses are quite costly. For one technical solution to pay off, it should be used at least once every two months. What makes it more difficult is that the platform

and its exercises should be improved continuously. The author agrees that buying an exercise environment might be expensive, but as there already exist various exercise platforms, it's probably less expensive to rent an already existing environment rather than buying one.

3.3.3. Summary of multi-level exercises advantages, challenges and solutions

Summary of multi-level cyber security exercises advantages that were discussed in Chapter 3.3.1 are as follows:

- As there are multiple levels in real life, they should be also rehearsed together in order to discover bottlenecks that may occur during incidents;
- Multi-level exercises help to test procedures and legislation, because exercises are the only safe way to find out shortcomings without the actual loss in real life;
- Multi-level exercises also allow testing of communication between parties and seeing how information changes within hours;
- As there haven't been many large international cyber crises so far, the international multi-level exercises can provide that experience for the future sake;
- Exercises allow teams to see their behavior in stressful situations;
- Multi-level exercises help managers to realize, that actions on lower levels could affect higher levels;
- Multi-level exercises allow to play through the whole escalation along with procedures and decisions during a short period of time;
- Multi-level exercises produce more learning outcomes for different levels.

Summary of multi-level exercises challenges and solutions that were discussed in Chapter 3.3.2 are presented in Table 3.

Table 3. Summary of multi-level exercises challenges and solutions.

Topic	Challenges	Solutions
Resource	• Multi-level exercises require more resources, such as people and money	• Planning cycle should be long enough for identifying possible bottlenecks and their mitigation possibilities • At least one person per institution is needed for the planning phase
Exercise type	• Multi-level exercise can't be a tabletop and technical exercise at the same time	• It should rather be a collection and combination of elements from different levels
Scenario	• It's a challenge to create a scenario for different levels so, that the levels don't get stuck or bring other levels off the desired course • It's difficult to think of an incident into the exercise scenario, that requires higher-level participation. • It is a challenge to make different levels to communicate and to escalate the situation to the higher levels	• Different level specialists should be also included into the scenario creation • There should be room for improvements and additional injects whether there's a defect that needs elimination during an exercise

Participation among the higher levels	• It's a challenge to make higher-level people to participate	• Things should be played through a little bit faster than they actually take in real life • Strategic and technical levels should be put together for approximately an hour to allow strategic level to see what's going on during the exercise on technical level • Allow people to start solving their exercises tasks from the location where they are currently located
Participation generally	• Sometimes people are not motivated to participate in exercises	• People could be motivated to participate in exercises via bonuses, like getting a day off from work • Also, food and some social elements could be included into the exercise • If people decide to ditch the exercise without a valid excuse, they could be fined
Language barrier	• There's a language barrier between technical level specialists and upper management.	• Different level communication problems could be solved with advisors, who provide translation between levels
Time difference on different levels	• Time on technical level goes many times faster compared to operational or strategic levels • There's a different reporting cycle, when different levels obtain new information	• Technical level should start an exercise a little earlier than operational level and synchronize during contact points • Playing with time jumps allow time to move faster on different levels • Let players consciously wait as decisions are being played out in higher levels.
Licenses	• Exercise technical environment and licenses are quite costly • The platform and its exercises should be improved continuously	• It's probably less expensive to rent an already existing environment rather than buying one.

3.4. Decision-making levels

Eight interviewed experts reckon that the lowest decision-making level is tactical level, whereas five specialists called it technical level. It's just the matter of representation because all the interviewees agree that action happens in the lowest level, where people deal with technical incidents or soldiers on the battlefield like in military sphere. Action plans for solving incidents are being decided on the operational level. As for strategy level, which is almost overlapped in Estonia with policy level, long-term strategic plans and political decisions are being decided. Four experts brought out that often it's not possible to draw the clear line, where one level ends and other begins. It is so, because Estonia is relatively small and actions between different levels tend to overlap. Two specialists pointed out, that information should never move directly from technical level to strategic and vice versa, there should always be operational level in between. It will evaluate the information and send only essential to either up or down.

3.4.1. Decision-making in cyber crisis

Interviewees brought out that Emergency Act, Emergency Response Plan and Cyber Incident Response Plan help to solve crisis situation in Estonia, but three interviewed experts reckon that it's not completely clear, who makes decisions during the time of cyber crisis. Moreover, it was asserted that RIA and CERT are probably the first institutions, which will have the first awareness of a crisis. RIA can include Estonian Defence League's Cyber Unit in solving cyber incidents, but it has limited authority allowing to interfere into organizations processes. Although RIA can still coordinate and offer suggestions. Organizations should have disaster plans and processes in place, so they would know how to act in case of crisis. In addition, one interviewee pointed out that Budapest Convention states whom to contact in case of international crisis. Furthermore, two experts pointed out that it's not clear how and when the collaborative tasks are transferred from RIA to defense forces.

One expert thinks that there wouldn't be a need for cyber law if people were aware of various laws and legislations. As there are so many of them and they are too complicated for regular people to understand, unified cyber law would make overall legislation easier and clearer in concrete areas. The author agrees with the expert, that it would help to make overall legislation easier to grasp. One interviewed specialist believes that in a democratic

country, it's not thinkable that RIAs' or any other institution head director could have the mandate to decide that there's a cyber crisis.

Eight interviewed experts pointed out that in the matter of solving the situation, lowest level should be able to make the decisions. Still, they should have pre-set limits and authority, which regulates until they can decide themselves. Three specialists brought out that people should be able to understand on their own, what they are allowed to decide or not. Whereas two experts pointed out that it's common for technical level experts to act as needed, even if those actions are out of their decision-making range. At the same time three interviewees claim that it should be operational level who decides, because technical level tends to get stuck when the decision starts to affect business. Technical level specialists might ruin things with their lack of knowledge in business processes. In addition, one interviewed expert believes that decisions should be sent to so-called horizontal level, which combines technical-operational levels and also includes managers. He adds that multi-level management is good for other areas, except in cyber, where situations need quick responses.

One expert believes that in real crisis situation things are done differently than rehearsed. He says that we can exercise as much as we want, but decisions in real crises will be done differently. Four interviewees believe that it's enough for one person to make operational decisions in crisis situations. Another four experts in contrast think that such decisions can't be ever made by one person alone, but rather groups of people prepare reasons why one or another decision is better. In addition, one interviewed specialist brought out that the lower the level, the more is for one person to decide.

Five experts pointed out that Estonia should have a system that allows for both – chain of command and compromise making. It was brought out by three experts that decisions should be always made by compromises. In addition, four people pointed out that decisions should be made through chain of command, although another four interviewees argue that it should be applicable only on a crisis situation.

Eight experts brought out that it's essential that ISP-s technical level experts from different countries could communicate between each other without operational level. Four experts assert that as long as it's agreed on beforehand, it's acceptable. On contrast, one interviewee disagrees. He believes that technical level specialists might not

understand the potential harmful effect to business when they communicate and act without the operational level awareness. An author agrees with majority, that technical level experts from different countries should have the right to communicate between each other without operational level.

4. Instruction set for designing multi-level exercises

This chapter focuses on analyzing literature review from Chapter II and interview results from Chapter III. As a result, an instruction set for planning multi-level exercises is proposed. Overall list of recommendations is brought out in Appendix 2.

4.1. Exercise needs analysis

According to the literature review in Chapter 2.5 the first phase for planning an exercise should always start with the need analysis and finding out the reasoning for having the exercise. Interviewed experts also think that way (Chapter 3.1.1) and they pointed out that there's no reason to conduct an exercise without the actual need. The author agrees and adds that the resources could be used in more beneficial ways instead of using them for conducting an exercise that has no necessity. As experts and literature review confirms that the exercise planning should start with needs analysis, the author also recommends to add this point to the instruction set for designing multi-level exercises, because this logic applies for both single and multi-level exercises.

4.1.1. Exercise objectives

Literature review (Chapter 2.5.3) has brought out that exercise objectives should be detailed, realistic and measurable, because otherwise it's not possible to effectively evaluate achieved goals, but in reality, according to interview results (Chapter 3.1.5) currently set objectives are not always well measured or the measuring tends to be rather subjective. Interviewees pointed out that in general, objectives for technical exercises are formulated well and are measurable when compared to tabletop exercises. It was also brought out from interview results (Chapter 3.2), that exercise organizers don't always think through the exercise designing methodology, how to set objectives or evaluate them. The author believes that the reason, why cyber exercises are currently not well measured, is caused by the fact that objectives are set vaguely and organizers have the lack of knowledge how to formulate strong objectives, which are also clearly defined, detailed and measurable. Likewise, Chapter 3.2.1 proves that people don't always seem to understand the actual purpose for conducting exercises or how to formulate objectives. Similarly, states literature review from Chapter 2.5.3, that having fewer objectives makes objectives better to measure and interview results from Chapter 3.2.4 proved, that exercise

quality will suffer, if there are too many objectives. As there is a problem with setting clear and measurable objectives for the exercises, the author recommends to add following points into the instruction set for designing multi-level exercises:

- Objectives should be set according to the rule of SMART (specific, measurable, achievable, relevant, time-bound) (Chapter 2.5.3);
- Exercises' organizers should limit the number of objectives set to the exercise in order to sustain exercise manageability.

4.1.2. Target audience selection

Both interview results (Chapter 3.2.2) and literature review (Chapter 2.5.2) brought out that target audience for the exercise is chosen based on the exercise objectives. Approaches are the same, but if target groups are chosen according to objectives, it leads to a problem, which also came out from interviews (Chapter 3.1.3), that there are usually the same group of people participating on exercises. The author believes, that on the one hand, it's good that the same participants are prepared for various incidents, but on the other hand, there are also others experts who could be trained and would use the experience. It was suggested during the interviews (Chapter 3.1.3) that for overcoming the issue, exercises participants could be divided between different years. The author thinks this solution would assure that instead of narrow target groups, wider number of specialists would have the knowledge, how to act in different crises. Also, additional suggestion was to form special teams, who are paid for participating on exercises. The author believes that this is probably not feasible and better solution would to divide exercise participants between different years.

Furthermore, was pointed out during the interviews (Chapter 3.2.2) an issue regarding target audience selection within international exercises. The problem is that countries tend to send their representatives to participate, rather than those who are actually solving incidents in real life. It is so, because after the exercise media releases will cover who "won". It came out from the interviews (Chapter 3.2.2) that one expert believes substitutes could be used in participating in exercises and they would also consult in the case of real life incidents. In contrary, another expert thinks that if key person is missing from the training, he/she doesn't have the knowledge how to act in case of a real-life event. The author agrees that key personnel should participate instead of substitutes and gain the

knowledge, how to react in different cases, because substitutes may not be available to assist in real crisis. Although, there should be wider number of specialists ready to act, in case of different cyber crises. As a result, if exercises' participants are divided between different years, it will assure a larger number of knowledgeable experts.

Based on the analysis, the author suggests to add following points into the instruction set for designing multi-level exercises:

- Target audience should be chosen based on the exercise objectives, but exercise participants should be divided between different years;
- Main participants should be the ones, who should be also solving incidents in real life situation.

4.1.3. Exercise type

There are two types of exercises: discussion-based and operations-based exercises (Chapter 2.1 and Chapter 2.2) and literature review (Chapter 2.5.2) brought out that exercise type is usually chosen according to the purpose of the exercise. As multi-level exercise is complex and involves different single levels, such as technical, operational and/or strategic levels, it was pointed out during the interviews (Chapter 3.3.2) that multi-level exercise can't be a tabletop and technical exercise at the same time, but it should rather be a collection and combination of elements from different exercises types. The author agrees and states that if multiple levels are involved, exercise type should be mixed from different single level elements.

Furthermore, it was brought out by interviewee (Chapter 3.3.1) that it's more useful to focus on concrete levels and to create tabletop exercises, although there were experts who disagreed and stated that tabletops are good for exercise pre-phase. Moreover, it was thought that information exchange can't be tested or technical incidents can't be solved on papers. At the same time, literature review (Chapter 2.5.2) brings out that in such exercises, where skills and experiences are being developed, exercise environments should be closer to real world and this is the reason, why tabletop exercises are not the best choice. The author believes that as interview results were contradictory, but literature review brought out, that tabletop exercises shouldn't be used for developing skills and experience, then the right exercise type should come from the exercise objectives and it should be mixed from single-level exercises elements.

Based on the analysis, the author recommends to add following point into the instruction set for designing multi-level exercises:

- Exercise type should be chosen based on the exercise objectives and mixed from different single level exercises elements.

4.1.4. Scenario creation

According to the literature review (Chapter 2.5.4) scenario has to be as realistic as possible. It also brought out that scenario should allow flexibility to add injects, so in case of deflection, it would be possible to get back to the desired track. Likewise, it was concluded by interviewed experts (Chapter 3.2) and furthermore, it's especially important when designing multi-level exercises, because it's complex to create a scenario, so the levels don't get stuck or bring different levels off the desired course. Additionally, as there are different levels to consider when planning multi-level exercise, it was suggested during the interviews (Chapter 3.3.2) to determine contact points where different levels meet during the exercise. It allows to plan the scenario to consider different levels. The author also agrees that previous points regarding realistic scenario and its intended flexibility are valid, as interview results and literature review are stating the same.

Literature review (Chapter 2.5.4) showed that it's essential to gather representatives from participating entities to scenario creation for allowing the scenario to be realistic. As it's even more complex to design a scenario for multi-level exercises, interview results (Chapter 3.3.2) suggested, that there should be one person per institute to participate in the planning. Also, different level experts should be involved into scenario creation, to avoid levels getting stuck. The author agrees that when designing multiple level exercises, different level experts should be involved into scenario creation, because they help to determine contact points for the levels and scenario will be more realistic.

Additional suggestion was pointed out during the interviews (Chapter 3.3.2) that exercise scenario should concentrate on small number of concrete issues by solving, for example, only 1-3 incidents during the exercise. It will assure enough time for all of them and the exercise will be more manageable. The same suggestion came out from literature review (Chapter 2.5.3). The author agrees, as both literature review and interview results confirmed the necessity of having limited number of incidents in the scenario.

Based on the analysis, the author recommends to add following points into the instruction set for designing multi-level exercises:

- Scenario should be realistic;
- Scenario should allow flexibility to add injects during the exercise to avoid deflection from the desired course;
- Scenario should limit a number of incidents to sustain exercise manageability;
- When multiple entities are involved in the exercise, there should be at least one person per institute to participate in the planning phase;
- Different level experts should be involved into scenario creation, because they help to make scenario more realistic, by determining contact points when levels meet during the exercise.

4.2. Planning cycle

Interview results (Chapter 3.3.2) show that when designing multi-level exercise, the planning cycle should be approximately six months longer when compared to single-level exercises. Also, it was pointed out (Chapter 3.2) that LS exercise planning cycle is one year and CE is two years. Furthermore, it was brought out that 18 months is required for planning a perfect multi-level cyber exercise. The author thinks that there should be a common ground for how much time should be planned for designing an exercise.

Literature review shows different planning lengths for the exercises. For tabletop exercises for example 1-2 months [14], 3 months [34] and 6 months [37]. For hybrid exercise 3-6 months [14] and for exercise, that covers all the levels 6-12 months [14], 12 months or for perfect exercise 18 months [37]. So, medium time for tabletop exercise should be planned according to the literature review with ~3 months, hybrid exercise with 3-6 months, exercise including all the levels with 6-12 months or in ideal case with 18 months.

When taking interview results and literature review into account, then organizers should consider 9 months for designing national multi-level cyber exercise and 12 months for exercise that covers all the levels. As Estonia is relatively small, time for planning a multi-level exercise was calculated based on the minimum time and 6 months were added according the suggestions made by the interviewees. As there haven’t been many national

multi-level cyber exercises before, then after gaining some experience, the exercise planning duration shortens.

According to interview results (Chapter 3.2) there's controversy between whether national cyber exercises in Estonia follow the planning conferences system or not. As for literature review (Chapter 2.5.2), IPC should be conducted 8-9 months before the exercise, MPC 5-6 months before the exercise, FPC 2-3 months before the exercise. It is stated in both interview results and literature review, that it's essential to have concrete planning system. The author thinks that as interview results and literature review both brought out the necessity of the system, it should be used and proposed conferences time-frames from literature review sounds reasonable.

Based on the analysis, the author suggests to add following points into the instruction set for designing multi-level exercises, that:

- 9 months should be considered for designing national multi-level cyber exercise and 12 months for exercise, where all the levels would be included;
- Exercises should use exercise planning conferences system, where:
  Initial Planning Conference (IPC) should be conducted 8-9 months before the exercise;
  Main Planning Conference (MPC) 5-6 months before the exercise;
  Final Planning Conference (FPC) 2-3 months before the exercise.

4.2.1. Overall planning questions

According to the literature review (Chapter 2.5) resources needed for the exercise should be planned precisely. Likewise, it was pointed out in interview results (Chapter 3.2). It was stated that counterparties should be aware of the tasks expected from them and time frames together with milestones should be divided into smaller pieces. The author agrees that efficient resource planning should be precise and people involved in the planning, should have full overview of their tasks, timeframes and milestones. It doesn't only make planning coordinated, but helps to avoid unpleasant surprises afterwards.

It came out from literature review [7] and interview results (Chapter 3.3.2) that multi-level exercises have language barrier between technical level specialists and upper management. It means that it's sometimes difficult to understand what is important for

different levels. For example, upper management doesn't tend to care about too many details and, at the same time technical experts don't know how to serve their findings to upper levels. Furthermore, if there are people planning or participating in exercises, whose native language isn't English, it also makes things more complicated. It was suggested to include advisors into the planning phase, who could translate between levels. The author thinks it's an excellent idea to fill language gaps by using this solution.

Also, interview results (Chapter 3.3.2) pointed out that it's a challenge to make higher-level people to participate. It was suggested, that if they are participating, things should be played through a little bit faster than they would actually take in real life, by using time jumps for example. As a result, exercise won't take so long and it might be easier to get higher-level people to participate. It was also suggested to allow people start solving their exercise tasks from the location where they are currently located. The author thinks that, on one hand, it would be good to try this solution, because it would be less time-consuming for the participants, but on the other hand, if people are not together, they might be less motivated. In conclusion, it's worth trying different involvement measures on the higher-level, to get them easily participating on exercises.

Additionally, it was pointed out during the interviews (Chapter 3.3.2) that strategic and technical levels should be put together for approximately an hour, to allow strategic level to see what's going on during the exercise on technical level. It came out from interviews (Chapter 3.4.1) that information should never move directly from technical level to strategic and vice versa, but when using this solution, information wouldn't be moving between levels, upper level just sees what's going on in technical level during the exercise. The author thinks that this suggested proposition would allow to raise upper management situational awareness by letting them see, that actions on lower levels could affect higher levels tremendously. It also came out from interviews (Chapter 3.3.2) but not from literature review, that information should move between levels and commands should be sent from upper levels to lower ones during multi-level exercises.

Furthermore, what was covered in interview results (Chapter 3.3.2) but didn't come out from literature review, one level (technical) should start exercise earlier and higher level (operational and/or strategic) joins the exercise during previously determined contact points. The proposed solution with time jumps allows playing through the whole crisis escalation quicker than it would actually take and also makes people easier to participate.

The author agrees that if it's possible to play through the whole escalation process much quicker than in real life, it is less time-consuming, but still allows to find out shortcomings from legislations or procedures.

Based on the analysis, the author recommends to add following points into the instruction set for designing multi-level exercises:

- Resource planning should be precise. People involved in the planning should have full overview of their tasks, planning timeframes and milestones;
- Timeframe and milestones should be divided into smaller pieces;
- Advisors should be included into the multi-level cyber security exercise planning phase, who are able to translate between levels and help to fill language gaps;
- Things should be played through a little bit faster during the multi-level cyber exercise than they would actually take in real life, by using time jumps, for example, and/or one level starts earlier than the other;
- Exercise planning should allow people from different levels to start solving their exercise tasks from the location where they are currently located;
- Exercise planning should allow putting strategic and technical levels together during the exercise for approximately an hour, to increase situational awareness in upper management;
- Exercise designer should consider, that commands should be sent from upper levels to lower ones during multi-level cyber security exercise, and information should move between levels, but never directly from technical level to strategic and vice versa.

4.2.2. Increasing motivation to participate

Chapter 3.3.2 addressed the problem that people are sometimes not motivated to participate in exercises. It was suggested that for increasing motivation, people could get bonuses, such as getting a day off from work or offer food and some additional social elements during the exercise. Moreover, if people decide to ditch the exercise without a valid excuse, they could be fined. The author agrees with previous statements and thinks that sometimes people indeed need a little push for an extra motivation and this is definitely the point that should be consider already in the planning phase in the exercise.

Based on the analysis, the author suggests to add following point into the instruction set for designing multi-level exercises:

- Different methods for increasing motivation to participate (bonuses, such as getting a day off from work or offering food and/or social elements during the exercise. In worst-case scenario, assign repercussions if people decide to ditch the exercise without a valid reason) should be considered when planning an exercise.

4.2.3. After the exercise

Literature review in Chapter 2.5.2 states that evaluation should be planned already in the exercise planning phase and it came out from Chapter 2.5.3 that if objectives are measurable, it's more efficient to assess achieved results. It was pointed out during the interviews (Chapter 3.1.5) that evaluation is not standardized in different levels and in general, besides technical exercises, measurement tends to be rather subjective. Moreover, there's a tendency in Estonia to give illustrated feedback to participating institutions, instead of strict and constructive one. As for LS (Chapter 3.1.5), the exercise evaluates participants in seven different categories, which allow to see in which categories have weaker results. The author believes that similar measuring system could be used for different cyber exercises, because illustrated feedback is not constructive. It was also suggested during the interviews (Chapter 3.1.5) that feedback should be strict and comparable to others, so every institution could see their weaknesses and improvement areas. The author agrees with the statements.

According to literature review [41] during the after-exercise *hot wash*, evaluators can collect some additional information they might have missed during the exercise. After that will be created After-Action Report (AAR), that consists of two parts: exercise observations, post-exercise implementation recommendations and Improvement Plan (IP), that includes improvement actions for different parties and also target dates for completion. As for interview results (Chapter 3.2) there's a tendency with national exercises, that ARR will be left out, but experts still think it's needed. The author also agrees, that it's essential to sum up the exercise, make improvements list with target dates, when changes need to be implemented.

At the same time, interview results (Chapter 3.1.6) show, that there is no central crisis management institution that would deal with learned lessons. It was also stated that results

from exercises and improvement areas are not taken seriously and they won't make into the work plans. It was suggested to look at exercise improvement suggestions as audits, where tasks are divided between people, who keep an eye on completing the tasks and ask feedback from time to time to see if there is any progress. The author believes this is a good idea, which should be enforced and also considered already in the exercise planning phase.

Based on the analysis, the author suggests to add following points into the instruction set for designing multi-level exercises:

- Measurement between entities should be comprehensive and constructive, so they could see their weaknesses in compared to other institutions and know their improvement areas;
- After-Action Report (AAR) should be created after every exercise, which would also include improvements areas and list;
- Improvement tasks should be divided between multiple people, who keep an eye on the tasks and ask feedback from time to time and see if there is any progress.

5. Results validation

It's essential to validate the outcome of the thesis, which is a combination of instructions for designing cyber security exercises in Estonia. There are two identified possibilities to validate the results:

Firstly, a cyber exercise should be planned by using these instructions proposed by the author. This solution assures full validity of the instruction set, as it can be practically tested in the real-world exercises. Unfortunately, due to the time and resource limitations this measure cannot be tested at this time, although the author believes that these recommendations will be tested in future exercises.

Secondly, as an alternative, results could be validated by asking feedback from the people who have experience in designing and conducting exercises. As 13 experts were interviewed during the research, who meet these requirements, their opinion gives sufficient validity. Additionally, feedback was asked from two Swedish cyber security experts on the field of exercises. Chapter IV analysis and achieved results were sent to experts for review and their feedback were collected through questionnaire. Provided analysis gave an insight to the logic behind the instructions development process. E-mail with feedback questionnaire that was sent to the experts is brought out in Estonian in Appendix 3.

Experts were asked to evaluate instruction set by providing numeric value from scale one to five, where:

1 - Not useful at all

2 - Somehow useful

3 - I don’t know

4 - Useful

5 - Very useful

Additionally, they were asked to comment:

1) Is there anything to add into the instruction set?

2) Is there anything the author could have done differently for achieving the thesis results, besides conducting expert interviews and analyzing results with existing literature?

Figure 6 gives an insight into the validation results, where the number of feedback received from experts is displayed vertically and instruction set usefulness is shown horizontally.

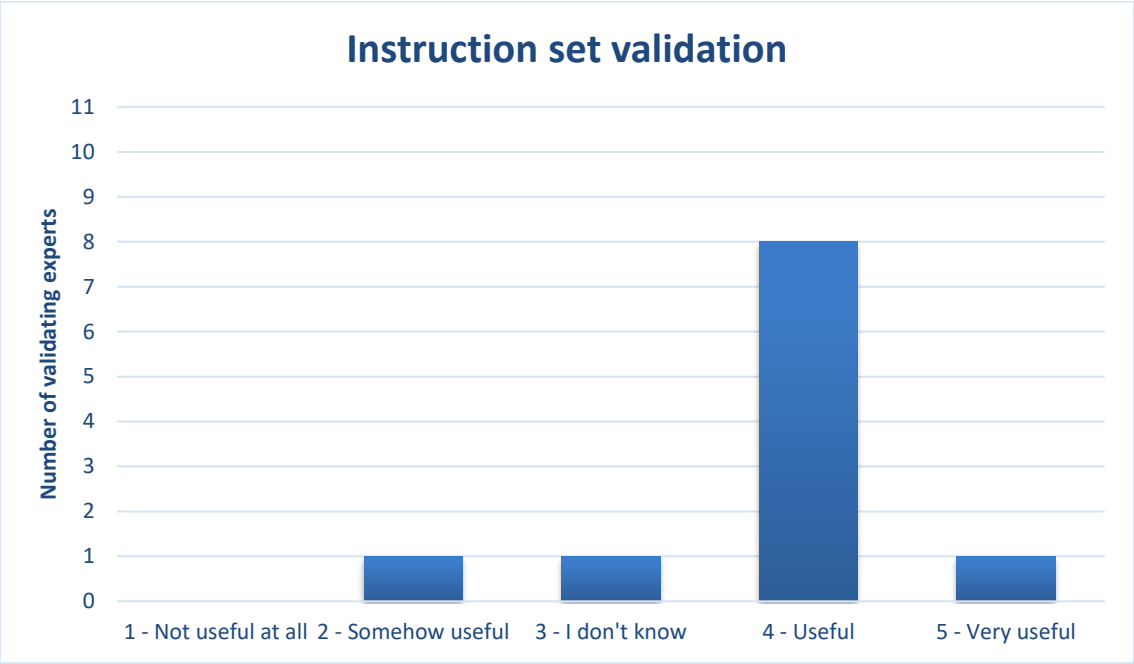

Figure 6. Instruction set validation.

The author of the thesis has received feedback from 11 experts out of 15, which makes ~73% from the overall list. Eight people evaluated the instruction set to be useful, one evaluated it to be very useful, one was unsure and one considered it to be somehow useful. Median is ~3.82, lowest rate is 2 and highest 5.

Additional propositions what could be added into the instruction set are as follows:

- There should be a possibility to disassemble levels during the exercise, if they start to heavily disturb each other (for example, if management incapability is causing technical level to go any further or due to the lack of technical skills, it's not possible to forward essential information to the management etc.)
- Cultural differences should also be considered when planning an exercise.

- When sharing exercise results, some information and suggestions are meant to be public and they shouldn't contain details that would threaten institutions or their systems security. However, the message itself, what was learned and rehearsed, shows the strength, which is positive information to the clients or population.
- Exercise designer should have a practical experience in solving similar scenarios in real life situations.
- Instruction set could be more detailed.

Feedback results on what could have been done differently for achieving the thesis results show that:

- According to specialists, it would have been useful to participate in the designing or conducting of an exercise, but it wouldn't have fit to the master's thesis timeframe. Therefore, interviews made with experts is a good choice.

6. Conclusions and future work

This thesis focuses on mapping best practices and proposing an instruction set for planning multi-level cyber security exercises in Estonia, with the intent to address the problem that national cyber security exercises in Estonia are typically focusing on only one level at a time. Additional aim is to determine shortcomings of cyber exercises. The selected methodology consists of gathering background information though literature review and semi-structured interviews, analyzing the collected data and proposing instructions for planning multi-level exercises based on the analysis. An outcome of the analysis is a set of instructions for designing multi-level cyber exercises.

The background chapter of the thesis concentrates on gathering background information through document analysis methods and defining relevant concepts, such as the current situation on the field and the process of planning cyber exercises. Also, different types of exercises and their similarities are covered.

After completing theoretical research, the author conducted interviews with 13 experts in the field. Most relevant experts' opinions, which help to achieve the thesis goals, were brought out and discussed in Chapter III.

Interview results determined following shortcomings of cyber security exercises:

- There are currently too many exercises;
- Lack of national cyber security exercises strategy;
- Same organizers and participants;
- Small participation rate among vital services providers;
- Exercises objectives' measuring tends to be rather subjective;
- Conclusions made from exercises are rarely taken seriously.

Furthermore, interview results brought out how cyber exercises are planned and conducted in Estonia, which exercises are designed well and which are criticized. Interview results also gave an overview of the advantages of multi-level exercises, what are the designing challenges and how to overcome them. Finally, results covered decision-making levels and decision making in case of cyber crises.

The author analyzed the gathered data from Chapter II (literature review) and Chapter III (interview results) and proposed recommendations for planning multi-level cyber exercises. The recommendation list focuses on topics regarding exercise needs analysis, exercise objectives, target audience, exercise type, scenario, planning cycle, overall planning questions and actions after the exercise. Proposed instruction set helps to overcome issues that rise when designing multi-level exercises, such as time differences and language barriers in different levels. Also, scenario creation, so that levels don't bring other levels off the desired course.

Proposed instruction set for designing multi-level cyber security exercises cover for example following suggestions:

- Different level experts should be involved into scenario creation, because they help to make scenario more realistic, by determining contact points when levels meet during the exercise;
- Advisors should be included into the exercise planning phase, who are able to translate between levels and help to fill language gaps;
- Things should be played through a little bit faster during the exercise than they would actually take in real life, by using time jumps, for example. and/or one level starts earlier than the other;
- Exercise designer should consider, that commands should be sent from upper levels to lower ones during multi-level cyber security exercise, and information should move between levels, but never directly from technical level to strategic and vice versa.

The outcome of the thesis was validated by sending Chapter IV analysis and achieved results overview from Appendix 2 to experts for review and their feedback were collected through questionnaire. Feedback results showed that proposed instruction set by the author is useful when designing multi-level cyber exercise. The achieved results are essential, as it came out from interview results and literature review, there were no recommendations for planning such multi-level cyber exercises before.

As for future work, cyber exercise observation should be planned in order to see, which recommendations from the instruction set are already in use, what is missing and could be added. As a result, proposed instruction set could be used in real life when designing

a multi-level exercise. Moreover, interested counterparties and students, for example, could plan an experimental exercise where proposed recommendations would be used. Although, if exercise is not planned with actual organizers and participants, exercise validity is questionable. Additionally, current work results could be refined due to possible shortcomings rising from testing these instructions in practice. They could be also used as an input for the next academic paper that would concentrate on delving deeper.

References

[1] A. Ogee, R. Gavrila, P. Trimintzios, V. Stravropoulos and A. Zacharis, "The 2015 Report on National and International Cyber Security Exercises," ENISA, 2015. [Online]. Available: https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises. [Accessed 2 March 2017].

[2] I. Odrats, "Information technology in public administration of Estonia. Yearbook 2007," Ministry of Economic Affairs and Communications, 2008. [Online]. Available: http://www.digar.ee/arhiiv/nlib-digar:246421. [Accessed 03 March 2017].

[3] C. Czosseck, A.-M. Talihärm and R. Ottis, "Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," NATO CCD COE, 2011. [Online]. Available: https://ccdcoe.org/articles/2011/Czosseck_Ottis_Taliharm_Estonia_After_the_2007_Cyber_Attacks.PDF. [Accessed 15 February 2017].

[4] L. Marinos, "ENISA Threat Landscape 2014, Overview of current and emerging cyber-threats," ENISA, 2014. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2014. [Accessed 3 April 2017].

[5] M. Hosenball, "Experts say Iran has "neutralized" Stuxnet virus," Reuters, 14 February 2012. [Online]. Available: http://www.reuters.com/article/us-iran-usa-stuxnet-idUSTRE81D24Q20120214. [Accessed 13 January 2017].

[6] D. E. Sanger and S. Erlanger, "Suspicion Falls on Russia as ‘Snake’ Cyberattacks Target Ukraine’s Government," The New York Times, 8 March 2014. [Online]. Available: https://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html?_r=0. [Accessed 12 January 2017].

[7] P. Trimintzios, R. Holfeldt, M. Koraeus, B. Uckan, R. Gavrila and G. Makrodimitris, "Report on Cyber Crisis Cooperation and Management," ENISA, 2014. [Online]. Available: https://www.enisa.europa.eu/publications/ccc-study. [Accessed 16 January 2017].

[8] Estonian Information System Authority, "Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2015. aasta kokkuvõte," Estonian Information System Authority, 2016. [Online]. Available: https://www.ria.ee/public/Kuberturvalisus/RIA_kuberturbe_aruanne_2015.pdf. [Accessed 20 February 2017].

[9] Ministry of the Interior, "Conex 2015," Ministry of the Interior, [Online]. Available:

https://www.siseministeerium.ee/et/tegevusvaldkonnad/kriisireguleerimine/oppused. [Accessed 8 February 2017].

[10] ENISA, "Cyber Europe 2014," ENISA, [Online]. Available: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/ce2014. [Accessed 16 Febrary 2017].

[11] ENISA, "Cyber Europe 2016," ENISA, [Online]. Available: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/ce-2016. [Accessed 15 February 2017].

[12] Estonian Defense Forces, "Largest NATO cyber defence exercise concludes in Estonia," Estonian Defense Forces, 2 December 2016. [Online]. Available: http://www.mil.ee/en/news/9515/largest-nato-cyber-defence-exercise-concludes-in-estonia. [Accessed 18 February 2017].

[13] N. Wilhelmson and T. Svensson, "Handbook for planning, running and evaluating information technology and cyber security exercises," The Swedish National Defence College, 2014. [Online]. Available: https://www.fhs.se/Documents/Externwebben/forskning/centrumbildningar/CATS/publikationer/Handbook%20for%20planning,%20running%20and%20evaluating%20information%20technology%20and%20cyber%20security%20exercises.pdf. [Accessed 23 February 2017].

[14] J. Kick , "Cyber Exercise Playbook," The MITRE Corporation, 2014. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf. [Accessed 22 February 2017].

[15] E. Ouzounis, P. Trimintzios and P. Saragiotis, "Good Practice Guide on National Exercises," ENISA, 2009. [Online]. Available: https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide. [Accessed 16 March 2017].

[16] M. M. Jalil , "Practical Guidelines for Conducting Research - Summarising Good Research Practice in Line with the DCED Standard," Donor Committee for Enterprise Development, 2013. [Online]. Available: https://ssrn.com/abstract=2591803. [Accessed 21 February 2017].

[17] M. C. Harrell and M. A. Bradley, "Data Collection Methods: Semi-Structured Interviews and Focus Groups," RAND corporation, 2009. [Online]. Available: http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR718.pdf. [Accessed 19 February 2017].

[18] ISO/TC 223, "ISO 22398:2013, Societal security — Guidelines for exercises," ISO, September 2013. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:22398:ed-1:v1:en:fig:1. [Accessed 27 February 2017].

[19] U.S. Department of Homeland Security, "Homeland Security Exercise and Evaluation Program (HSEEP), Volume 1: HSEEP Overview and Exercise Program," U.S. Department of Homeland Security, 2006. [Online]. Available: http://www.michigan.gov/documents/deq/deq-wb-wws-HSEEP_Vol_I_271850_7.pdf. [Accessed 13 February 2017].

[20] U.S. Department of Homeland Security, "Homeland Security Exercise and Evaluation Program (HSEEP)," U.S. Department of Homeland Security, 2013. [Online]. Available: https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf. [Accessed 16 February 2017].

[21] U.S. Joint Chiefs of Staff, "Joint Publication 1, Doctrine for the Armed Forces," U.S. Joint Chiefs of Staff, 2013. [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp1.pdf. [Accessed 12 February 2017].

[22] Estonian Defence League, "Kõikehõlmava riigikaitse sõjaline doktriin," Estonian Defence League, [Online]. Available: http://www.kaitseliit.ee/files/kaitseliit/img/files/Koikeholmava_riigikaitse_sojaline_doktriin(1).pdf. [Accessed 25 February 2017].

[23] A. Laneman, "Strateegiline sõdur ja taktikaline kindral," Delfi, 6 June 2006. [Online]. Available: http://epl.delfi.ee/news/eesti/strateegiline-sodur-ja-taktikaline-kindral?id=51042567. [Accessed 24 February 2017].

[24] U.S. Department of the Army, "ADRP 6-0, Mission Command," U.S. Department of the Army, 2012. [Online]. Available: https://fas.org/irp/doddir/army/adrp6_0.pdf. [Accessed 13 February 2017].

[25] R. Gavrila, A. Ogée, P. Trimintzios and A. Zacharis, "ENISA CE2014 After Action Report," ENISA, 2015. [Online]. Available: https://www.enisa.europa.eu/publications/ce2014-after-action-report. [Accessed 3 February 2017].

[26] ENISA, "Cyber Cooperation and Exercises," ENISA, March 2015. [Online]. Available: https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/march-2015/presentations/exercises-presentation-nlomeeting-march-2015.pdf/view. [Accessed 14 February 2017].

[27] T. Svensson, *Cyber Defense Exercises A way of building Trust,* 2015.

[28] ENISA, "Cyber Europe," ENISA, [Online]. Available: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme. [Accessed 23 January 2017].

[29] NATO CCD COE, "Crossed Swords Exercise," NATO CCD COE, [Online]. Available: https://ccdcoe.org/crossed-swords-exercise.html. [Accessed 2 February 2017].

[30] NATO CCD COE, "Cyber Defence Exercise Focuses on Vulnerability Testing," NATO CCD COE, 2016. [Online]. Available: https://ccdcoe.org/cyber-defence-exercise-focuses-vulnerability-testing.html. [Accessed 16 January 2017].

[31] NATO CCD COE, "Locked Shields 2016," NATO CCD COE, [Online]. Available: https://ccdcoe.org/locked-shields-2016.html. [Accessed 3 February 2017].

[32] The Baltic Times, "The largest international technical cyber defence exercise in the world takes place next week," The Baltic Times, 20 April 2017. [Online]. Available: http://www.baltictimes.com/the_largest_international_technical_cyber_defence_exercise_in_the_world_takes_place_next_week/. [Accessed 22 April 2017].

[33] North Atlantic Treaty Organization, "NATO holds annual cyber exercise in Estonia," NATO, 27 February 2017. [Online]. Available: http://www.nato.int/cps/en/natohq/news_138674.htm?selectedLocale=en. [Accessed 13 January 2017].

[34] T. Grance, T. Nolan, K. Burke, R. Dudley, G. White and T. Good, "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities," NIST, 2006. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf. [Accessed 15 January 2017].

[35] T. Männiste, Sõjalise väljaõppe metoodika, Estonian National Defence College, 2013.

[36] C. May and J. Hammerstein , "The CERT® Approach to Cybersecurity Workforce Development," Software Engineering Institute - CMU, 2010. [Online]. Available: http://www.sei.cmu.edu/reports/10tr045.pdf. [Accessed 19 February 2017].

[37] NATO/EAPC, "Guidelines for Planning, Conduct and Assessment of International EAPC Exercises," NATO/EAPC, 2009. [Online]. Available: http://msb.gov.ba/PDF/docEN30102015.pdf. [Accessed 16 February 2017].

[38] G. Longo, "Designing Cyber Exercises," Software Engineering Institute - CMU, 2014. [Online]. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA613366. [Accessed 23 February 2017].

[39] U.S. Department of Homeland Security, "Communications-Specific Tabletop Exercise Methodology," U.S. Department of Homeland Security, 2011. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/CommunicationsSpecificTabletopExerciseMethodology.pdf. [Accessed 18 January 2017].

[40] North Atlantic Treaty Organisation, "BI-SC COLLECTIVE TRAINING AND EXERCISE DIRECTIVE (CT&ED) 075-003," NATO, 2013. [Online].

Available: http://www.act.nato.int/images/stories/structure/jft/bi-sc-75-3_final.pdf. [Accessed 4 February 2017].

[41] U.S. Department of Homeland Security, "Homeland Security Exercise and Evaluation Program (HSEEP), Volume III: Exercise Evaluation and Improvement planning," U.S. Department of Homeland Security, 2006. [Online]. Available: http://www.michigan.gov/documents/deq/deq-wb-wws-HSEEP_Vol_III_271853_7.pdf. [Accessed 17 February 2017].

Appendix 1 – Interview questions template

Intervjuu viiakse läbi Tallinna Tehnikaülikooli küberkaitse eriala tudengi Katrin Kuke koostatava magistritöö raames, mille eesmärk on pakkuda lahendusi mitmetasandiliste (tehnilise- ja operatiivtasandi) küberõppuste korraldamiseks. Ekspertintervjuude tulemusi kasutatakse sisendina magistritöös püstitatud eesmärkide saavutamisel.

Vajadusel ei seosta magistritöö autor intervjuu käigus esitatud ekspertide seisukohti nimedega, vaid kasutab umbisikulist vormi. Lõputöö ei käsitle riigisaladusi ega AK-materjale. Intervjueeritud ekspertide nimekiri kuulub magistritöö lisadesse, kuid helisalvestised ning transkriptsioonidokumendid mitte. Enne magistritöö avalikustamist saadab magistritöö autor valminud töö ka intervjueeritavatele, et olla veendunud intervjueeritavatega tehtud kokkulepete kinnipidamises.

Kas Te olete nõus, et Teie nimi kajastub intervjueeritavate nimekirjas?

Kas Teie ütlusi võib tsiteerida ja nimeliselt viidata või on vajalik vastuste anonümiseerimine?

- Palun kirjeldage oma rolli Eesti Vabariigi küberkaitses ja milline on seotus küberõppustega.
- Milliste küberõppustega Te olete kokku puutunud?
- Milliste küberõppustega Te olete lisaks eelmises küsimuses nimetatuile veel kokku puutunud ja millist rolli nende raames omanud?
- Kas Teil on kokkupuudet olnud ka näiteks mõne järgeva küberõppusega: KüberSiil, Conex, Cyber Europe, Locked Shiels, Crossed Swords, Cyber Coalition?

Kui 3nda küsimuse vastus oli jah, siis küsida ka alamküsimused:

- Mis Te arvate nende küberõppuste korralduslikust poolest ja õppustele seatud eesmärkidest?
- Millised on nende õppuste kitsaskohad ja kas on midagi, mida saaks Teie arvates paremini teha?
- Kas on veel mõnda Teie jaoks olulist küberõppust, mida ma hetk tagasi ei nimetanud?

- Kuidas hetkel küberõppuste korraldamisel veendutakse, et kogu oluline sihtgrupp saaks kaetud?

Küsida neilt, kes ise korraldanud või korraldavad:

- Kuidas toimub Teie puhul küberõppuste ajaline planeerimine?
- Millised tegevused toimuvad enne ja pärast küberõppust?
- Kuidas kaasatakse küberõppusele osapooli?
- Kuidas pannakse paika küberõppuse eesmärgid?

- Millised erinevad juhtimistasandid Teie valdkonnas kasutusel on, kuidas need jaotuvad ning kuidas neid kirjeldaksite (nt. mis on taktikaline/tehniline tasand, operatiivtasand ja strateegiline tasand)?
- Mida tähendab Teie jaoks väljend mitmetasandiline küberõppus?
- Kas Te olete mõne küberõppuse raames kogenud mitme tasandi koos harjutamist? Nt. ühel küberõppusel on samaaegselt harjutatud nii tehnilist kui ka operatiivtasandit?

Kui 7nda küsimuse vastus oli jah, siis küsida ka alamküsimused:

- Kuidas need küberõppused õnnestusid? Kas Te oskate välja tuua, mis nende õppuste puhul toimis ja mis mitte.
- Kas need küberõppused vajasid planeerimise mõistes ka mingisugust erikohtlemist?
- Palun kirjeldage eeliseid, miks oleks mitmetasandiliste küberõppuste korraldamine hea?

Kui 7nda küsimuse vastus oli ei, siis küsida ka alamküsimus:

- Palun kirjeldage eeliseid, miks oleks mitmetasandiliste küberõppuste korraldamine hea?
- Palun kirjeldage väljakutseid, mis kerkivad esile mitmetasandiliste küberõppuste korraldamisel?
- Millist lahendust näeksite ise mitmetasandiliste küberõppuste korraldamiseks ja erinevate keerukustega toimetulemiseks?

- Kas Teie arvates on mitmetasandilistel küberõppustel erinevatel tasanditel erinev ajaskaala?
- Kas Teie arvates on mõnda moodust, kuidas saaks siduda mitmetasandilistel küberõppustel selle ajalise faktori?

- Kuidas tehakse praegu küberkriisi olukorras otsuseid?
- Millisel tasandil oleks tarvis teha otsuseid?
- Milliste teemade osas on kübervaldkonnas otsustuspädevus ja see, kellel on mandaat otsuseid vastu võtta, kirjas?
- Kas otsused peaks olema tehtud mitme kollektiivi või indiviidi poolt? Kas need peaks olema kompromisside või käsuõiguse tulem? Tuua näiteid.

- Kujutage ette tehnilise tasandi küberõppust, millele on lisatud ka operatiivpool, suhtlevad tehnilise tasandi osalejad teiste riikide ISP-dega ilma operatiivpoolt kaasamata. Kuna see erineb tavapärasest kriisiolukorras kasutatavast käsuliinist, kas selline alternatiivne lähenemine oleks Teie arvates probleem?

Küsida neilt, kes ise korraldanud või korraldavad:

- Kas on veel midagi, mis muudab mitmetasandiliste küberõppuste korraldamise keeruliseks?
- Kas Te kirjeldaksite juhendmaterjale, millest ise küberõppuste korraldamisel lähtute? Kas neid oleks võimalik ka minuga jagada?
- Kas Te oskate veel midagi nimetada, mis vajaks küberõppuste korraldamisel parandamist?
- Kas Teil on soovitusi, keda võiksin veel intervjueerida?

Appendix 2 – Instruction set for designing multi-level exercises

Exercise needs analysis (Chapter 4.1):

- Exercise planning phase should start with needs analysis.

Exercise objectives (Chapter 4.1.1):

- Objectives should be set according to the rule of SMART (specific, measurable, achievable, relevant, time-bound);
- Exercises' organizers should limit the number of objectives set to the exercise in order to sustain exercise manageability.

Target audience (Chapter 4.1.2):

- Target audience should be chosen based on the exercise objectives, but participants should be divided between different years;
- Main exercise participants should be the ones, who should be also solving incidents in real life situation.

Exercise type (Chapter 4.1.3):

- Exercise type should be chosen based on the exercise objectives and mixed from different single level exercises elements.

Scenario (Chapter 4.1.4):

- Scenario should be realistic;
- Scenario should allow flexibility to add injects during the exercise to avoid deflect from the desired course;
- Scenario should limit a number of incidents to sustain exercise manageability;
- When multiple entities are involved in the exercise, there should be at least one person per institute to participate in the planning phase;
- Different level experts should be involved into scenario creation, because they help to make scenario more realistic, by determining contact points when levels meet during the exercise.

Planning cycle (Chapter 4.2):

- 9 months should be considered for designing national multi-level cyber exercise and 12 months for exercise, where all the levels would be included;
- Exercises should use exercise planning conferences system, where:
  Initial Planning Conference (IPC) should be conducted 8-9 months before the exercise;
  Main Planning Conference (MPC) 5-6 months before the exercise;
  Final Planning Conference (FPC) 2-3 months before the exercise.

Overall planning questions (Chapter 4.2.1)

- Resource planning should be precise. People involved in the planning should have full overview of their tasks, planning timeframes and milestones;
- Timeframe and milestones should be divided into smaller pieces;
- Advisors should be included into the multi-level cyber security exercise planning phase, who are able to translate between levels and help to fill language gaps;
- Things should be played through a little bit faster during the multi-level cyber exercise than they would actually take in real life, by using time jumps, for example, and/or one level starts earlier than the other;
- Exercise planning should allow people from different levels to start solving their exercise tasks from the location where they are currently located;
- Exercise planning should allow putting strategic and technical levels together during the exercise for approximately an hour, to increase situational awareness in upper management;
- Exercise designer should consider, that commands should be sent from upper levels to lower ones during multi-level cyber security exercise, and information should move between levels, but never directly from technical level to strategic and vice versa.

Increasing motivation to participate (Chapter 4.2.2)

- Different methods for increasing motivation to participate (bonuses, such as getting a day off from work or offering food and/or social elements during the exercise. In worst-case scenario, assign repercussions if people decide to ditch the exercise without a valid reason) should be considered when planning an exercise.

After the exercise (Chapter 4.2.3):

- Measurement between entities should be comprehensive and constructive, so they could see their weaknesses in compared to other institutions and know their improvement areas;
- After-Action Report (AAR) should be created after every exercise, which would also include improvements areas and list;
- Improvement tasks should be divided between multiple people, who keep an eye on the tasks and ask feedback from time to time and see if there is any progress.

Appendix 3 – Thesis results validating e-mail

Tere!

Minu magistritöö valmimine on jõudnud lõpusirgele ning jäänud on veel lõputöö käigus valminud mitmetasandiliste küberõppuste korraldamise soovituste nimekirja valideerimine. Palun Teilt, et leiaksite 15-20 minutit soovituste nimekirja kasulikkuse hindamiseks 5 palli süsteemis, kus 1 - Pole kasulik, 2 - Mingil määral kasulik, 3 - Ei tea, 4 - Kasulik, 5 - Väga kasulik. Soovituste nimekirja võiks hinnata õppuse korraldaja pilgu läbi, eriti olukorras, kus korraldaja pole varem mitmetasandiliste õppuste planeerimisega kokku puutunud. Lisaks palun Teilt ka võimaluse korral kommentaare küsimustele:

1) Kas on midagi, mida võiks soovituste nimekirja veel lisada?

2) Kas lõputöö autor oleks võinud tulemuste saamiseks kasutada mõnda teist moodust peale ekspertintervjuude ning olemasolevate erinevate valdkondade õppuste juhendimaterjalide analüüsimise?

Lisan kirjale soovituste nimekirja ning igaks juhuks ka peatüki magistritööst, mille põhjal sai soovituste nimekiri kokkupandud.

Parimate soovidega

Katrin Kukk