TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Helena Jäe 221956IVCM

THE EVOLUTION OF CYBER CONFLICT ON THE EXAMPLE OF ESTONIA, GEORGIA AND UKRAINE

Master's Thesis

Supervisor: Kaido Kikkas
PhD

Tallinn 2024

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Helena Jäe 221956IVCM

KÜBERKONFLIKTI EVOLUTSIOON EESTI, GRUUSIA JA UKRAINA NÄITEL

Magistritöö

Juhendaja: Kaido Kikkas
PhD

Tallinn 2024

Author's Declaration of Originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Helena Jäe

12.05.2024

Abstract

The integration of cyber conflict into conventional warfare has become increasingly significant over the past two decades. In 2016, NATO formally recognized the cyber domain as the fourth area of operation, reflecting the growing importance of cyber activities in global conflicts. This study focuses on Russia's activities in Estonia (2007), Georgia (2008), and Ukraine (2014 and 2022), examining the evolution, tactics, and implications of cyber attacks since 2007.

Cyber attacks have evolved into more sophisticated tactics integrated into broader hybrid warfare strategies. Social media has emerged as a crucial tool for propaganda dissemination and information operations, amplifying the impact of cyber attacks.

The interconnectedness between physical and cyber domains in conflict situations is a central theme, emphasizing the importance of understanding the interplay between these realms. Geopolitical awareness and historical context are essential for anticipating and preparing for cyber threats, as minor events can escalate into full-blown cyber conflicts.

Looking ahead, diverse and multifaceted cyber threats are expected to characterize the future of cyber conflict. Adversaries continually evolve tactics, necessitating proactive defense measures and international cooperation to address state-sponsored cyber threats effectively. Attacks on critical infrastructure, such as the NotPetya malware targeting Ukrainian systems, underscore the potential for significant disruption and economic damage.

In conclusion, this study highlights the evolving nature of cyber conflicts and emphasizes the need for comprehensive strategies to mitigate their impact on society. By understanding the evolution, tactics, and implications of cyber attacks, security experts can better prepare for future threats.

The thesis is written in English and is 43 pages long, including 7 chapters and 2 figures.

Annotatsioon

Küberkonflikti evolutsioon Eesti, Gruusia ja Ukraina näitel

Küberkonfliktide integreerimine konventsionaalsesse sõjapidamisse on viimase kahe aastakümne jooksul muutunud järjest olulisemaks. 2016. aastal tunnistas NATO küberdomeeni ametlikult neljandaks operatsioonide valdkonnaks, mis peegeldab kübertegevuse kasvavat tähtsust globaalsetes konfliktides. Kesolev lõputöö keskendub Venemaa tegevusele Eestis (2007), Gruusias (2008) ja Ukrainas (2014 ja 2022), uurides küberrünnakute arengut, taktikat ja tagajärgi alates 2007. aastast.

Küberrünnakud on arenenud keerukamaks, mis on integreeritud laiematesse hübriidsõja strateegiatesse. Sotsiaalmeedia on kujunenud oluliseks vahendiks propaganda levitamisel ja teabeoperatsioonidel, võimendades küberrünnakute mõju.

Füüsilise ja kübervaldkonna vastastikune seotus konfliktiolukordades on keskne teema, mis rõhutab nende valdkondade vastastikuse mõju mõistmise tähtsust. Geopoliitiline teadlikkus ja ajalooline kontekst on küberohtude ennetamiseks ja nendeks valmistumiseks hädavajalikud, sest väiksemad sündmused võivad kasvada täiemahulisteks küberkonfliktiks.

Tulevikku vaadates iseloomustavad küberkonfliktide tulevikku mitmekülgsed ja mitmetahulised küberohud. Vastased arendavad pidevalt taktikat, mistõttu on vaja ennetavaid kaitsemeetmeid ja rahvusvahelist koostööd, et tõhusalt võidelda riigi toetatud küberohtudega. Ründed kriitilisele infrastruktuurile, nagu näiteks Ukraina süsteemidele suunatud NotPetya pahavara, rõhutavad oluliste häirete ja majandusliku kahju võimalikkust.

Kokkuvõttes toob käesolev töö esile küberkonfliktide muutuva olemuse ja rõhutab vajadust terviklike strateegiate järele, et leevendada nende mõju ühiskonnale. Mõistes küberrünnakute arengut, taktikat ja tagajärgi, saavad küberkaitseeksperdid tulevasteks ohtudeks paremini valmistuda.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 43 leheküljel, 7 peatükki ja 2 joonist.

List of Abbreviations and Terms

Cyber warfare	The use of cyber attacks against an enemy state, causing comparable harm to actual warfare and/or disrupting vital computer systems.
DDoS	Distributed Denial-of-Service. A malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
DoS	Denial of Service. A type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning.
Information operations	Activities that governments and military forces undertake to control and exploit the information environment via the use of the information component of national power.
NATO	The North Atlantic Treaty Organization
OSCE	Organization for Security and Cooperation in Europe
Ping floods	A ping flood, also known as an ICMP flood, is a type of distributed denial-of-service (DDoS) attack in which an attacker overwhelms the targeted device or network with continuous request packets (pings)
SQL injections	Attack consists of insertion or "injection" of a SQL query via the input data from the client to the application
State-sponsored	Violence carried out with the active support of national governments provided to violent non-state actors
TDoS	Telephone Denial of Service

Table of Contents

List of Figures

1. Introduction

In the last 18 years, the component of cyber conflict has been added to conventional warfare [1]. In 2016, The North Atlantic Treaty Organization (NATO) added the cyber domain as the fourth area of operation [1]. Manipulation of information and sharing of information favourable to the adversary can begin years before the outbreak of a real military conflict. Subversive activities using cyber attacks have also increased significantly in recent conflicts. These attacks can be on critical infrastructure that paralyzes the functioning of society on a larger scale. They can also restrict services important to ordinary citizens, such as distributed denial-of-service (DDoS) attacks on public transport ticketing systems.

The component of information warfare has been strongly seen in the conflicts in Estonia (2007), Georgia (2008) and Ukraine (2014 and 2022). The main opponent of these conflicts is Russia. Therefore, this work focuses entirely on Russia's subversive activities in these countries. In the theoretical part of the work, the author provides an overview of the literature of the conflicts discussed in this research. The third paragraph gives an overview of the methodology used in this thesis. The fourth chapter of the work contains an overview of the results obtained from the interviews and their analysis. The fifth chapter discusses about the results, and the sixth chapter gives answers to the research questions. The seventh paragraph summarises the thesis.

This work analyses how hybrid warfare has changed by studying Russia's behaviour. This master's thesis opens up the topic by answering the research questions that are defined in 1.2 Research questions paragraph. In addition, the author gives an overview of what methods to use to defend the country that is being cyber-attacked.

The author of this thesis is using the concept of cyber conflict instead of cyber war. This is because war means kinetic conflict, but this thesis focuses on the cyber part of conflicts in Estonia, Georgia and Ukraine.

1.1 Scope and goal

The scope and goal are outlined below. The scope of this study is:

- The scope of this study is on cyber attacks that have occurred in the last 18 years in Estonia, Georgia and Ukraine. This study focuses totally on Russia's attacks in the

previously mentioned countries.

- The narrower scope of this study is on the events that took place in Estonia in 2007, Ukraine in 2014 and 2022, and Georgia in 2008.
- Due to the ongoing conflict in Ukraine, the thesis deals only with events that took place until December 2023.

The limitations of this study are:

- The topic of cyber conflict can be nationally sensitive. Since this research contains a literature review and interviews, not everything may be written in public sources. Therefore, these are excluded from this study.
- Since the cyber attacks in Ukraine are still very recent, not everything has been written about yet. A comparison between 18 years ago and today may remain incomplete.
- The interviewee may not want to discuss everything that has happened in Ukraine, because the topic is still very fresh.

The purpose of this study is to analyse how the conduct of cyber conflict has changed on the example of Estonia, Georgia and Ukraine. The study focuses on investigating which tactics are used and how their scales have changed over the last 18 years. The all focus of the study is on Russia's activities before and during the conflict.

1.2 Research questions

The author has set the following research questions:

1. To what extent have cyber attacks evolved in terms of tactics, scale, and state-sponsored involvement since 2007, with a specific focus on the events in Estonia (2007), Ukraine (2014 & 2022), and Georgia (2008)?
2. What lessons can be drawn from the cyber attacks on Ukraine's infrastructure since 2022?
3. What can we expect from cyber attacks in the future, and how best to prepare for them?

1.3 Novelty

In the context of the ongoing comprehensive military conflict in Ukraine, it is pertinent to elucidate the evolution of cyber conflict and prognosticate potential future developments.

This study focuses on how Russia changed its tactics and behaviour in 2007-2022. In addition, this study looks at the future of cyber conflict and how countries and companies can best protect themselves. In addition, this work has conducted interviews with people who, since 2007, have been very closely connected with the events that the research deals with.

1.4 Outline of the thesis

The thesis has a total of 7 chapters: an introduction, a theoretical background, a methodology, an analysis, a discussion, a results and a summary.

In the introduction and summary chapter, there is a written short summary of the thesis. In the theoretical background, there is a literature review, which gives an overview of the cyber conflict and information operation. There is also an overview of the conflict that took place in 2007 in Estonia, in 2008 in Georgia and in 2014 and 2022 in Ukraine. In the literature review, there is also defined the research gap.

In the methodology chapter, there is defined how the data was collected and analysed. In the following chapter, there is an analysis part, where is the information that has been gained during the interviews and literature review.

In the discussion paragraph, there is a deeper analysis of the results gained from the Analysis paragraph. The final paragraph is results, which gives the answer to the research questions.

The thesis has 2 figures and it has total of 48 pages.

There are 2 appendices, one of which is the interview questions that were asked from the interviews.

2. Theoretical background

In the theoretical background, an overview of the nature of cyber conflict, conflicts in Eastern Europe, and the motives of information war. The conflicts that are being investigated are Estonia (2007), Georgia (2008) and Ukraine (2014-2023). The overview of these cyber conflicts is based on a systematic literature review.

2.1 Cyber conflict and information operations

Cyber conflict is a type of war. P. W. Singer and A. Friedman have noted that 'whether it be war on land, at sea, or in the air, or now in cyberspace, war always has a political goal and mode and always has an element of violence' [2, p 121]. Very often, cyber conflict is motivated by political views. An example is the Bronze Night events that took place in Estonia in 2007. Bronze Night was a politically motivated event because the attacks started when Estonia started the removal of the Soviet war memorial from the centre of Tallinn. The cyber attacks in Estonia were the first attacks of their kind aimed at a single country. [3] In June 2007, Aaron Mannes and James Hendler wrote that the era of cyber war has begun [4].

As written in Erik Gartzke's paper, one of the effects of war must be a long-term effect [5, p 56]. In cyberspace, the long-term effect is usually referred to as a loss of confidentiality or integrity of the data. If the information has already been leaked, it is no longer possible to make it completely secret again. This kind of data leak has caused long-term effects to the data owner. [6] In addition to the previously mentioned long-term effects, more attacking methods impact society. For example, DDoS attacks also have a long-term effect, especially regarding people's emotions. [7, p 313] Such attacks can cause people to lose confidence in their government and divide society.

According to the book "Cyber War Will Not Take Place" by Thomas Rid, cyber war is not something that can be classified separately. Rid says that cyber war is something that can be classified under sabotage, subversion and espionage. [8, p 14] This statement may reduce the cyber component in the conflict. As mentioned before, the effects of cyber conflict can also have long-term effects, and cyber activities are not just about sabotage, subversion and espionage. However, it can be said that cyber conflict is not a separate form of kinetic war, but it is one of the ways of warfare. [7, p 303], [9]

The importance of the cyber component in modern warfare can also be shown by NATO (The North Atlantic Treaty Organization). NATO added the cyber domain as the fourth area of operations. It means that NATO must defend itself in this area. Since 2016, the cyber domain has been equivalent to the defence that NATO provides on land, air and sea [1].

Before a full-scale war breaks out, there is often an act of subversion of society. This achieves that riots will be organized in the interest of a foreign power. Hollowing activities can also be political. For example, the parties of the non-incumbent government are supported. Its purpose is to change laws and regulations in a way that suits the foreign power. [10, pp 10-12]

Today, one of the main subversive activities is cyber activities. These activities can be DDoS attacks as well as "troll farms". Strategic subversive activities can weaken societal stability in peacetime. When the society is already sufficiently undermined, it is easier for a foreign power to find the support of the society with its ideas [10, p 15]. Social media can easily be used to blame others. For example, it was very visible when flight MH17 was shot down over Ukraine [10, p 47]. In such cases, it is easy to set any opinion that may be distorted from the truth in motion. However, this kind of activity can lead to divisions in society, and it is easier to achieve the goals you set in a conflict situation.

When it comes to cyber influence, influencing information is also important. If people have been sufficiently influenced and given only one-sided information, ordinary citizens can also be motivated to organize attacks. For example, in the attacks against Estonia, there were different instructions on how to attack Estonia's systems. [11]

2.2 Cyber conflict in Estonia, Georgia and Ukraine

The following three chapters give an overview of the cyber conflict that has been taking place in Estonia, Georgia and Ukraine in the last 17 years. In the subsection 2.2.1, there is an overview of the conflict between Estonia and Russia. The next subsection 2.2.2 overviews the conflict between Georgia and Russia. This paragraph's final subsection 2.2.3 describes the cyber conflict between Ukraine and Russia.

2.2.1 Cyber conflict between Estonia and Russia

In 2007, Estonia was already quite a digitized country. A lot of operations in Estonia could already be done electronically. Only 5% of the banking operations were not done

electronically. In 2007 in Estonia there was already mobile parking, digital signatures, the Internet covers most of the country's and data exchange was done using X-road. [12, p 17] The extensive digitization of Estonia gave the Russians a wide area to attack.

The cyber conflict in Estonia started with a political decision. Estonian government decided to move the Soviet monument to the new place. This monument had a different meaning for Estonians and Russians. For Estonians this monument represented the occupation time Estonia had after the World War II. [11] With today's knowledge, it is difficult to say whether the cyber attacks were planned from very beginning to be involved in the organized riots. Considering that cyber attacks were initially quite rudimentary, it can be said that they were just for testing purposes. And in the second phase they were already more organized [12, p 18].

The Bronze Night did not start with the cyber attacks. Initially, it was only a peaceful demonstration on the city streets. [11] The riots in Estonia started on April 26, 2007. Before that Estonian government announced the relocation of the Bronze Solider. In addition to moving the Bronze Soldier, it was also announced that the preparatory work of excavating war graves and reburying the bodies in the military cemetery would begin. [12, p 16] The riots started a few weeks before the important day for Russians – 9th of May (Victory Day for Russians). [8, p 6] On that day there were big attack wave. Attacks started one hour before the 9th of May. The suggestion is that the attackers were attacking on Moscow time. [11]

The peaceful riots that started on April 26 escalated into a more violent one. Already in the late evening of April 27, cyber attacks on Estonian websites began. These cyber attacks lasted more than three weeks. [12, p 16] The types of attacks that were used were widely known [11]. The Russians mainly used ping floods or denial-of-service (DoS) attacks to attack the Estonian infrastructure. On April 30, the Russians began to carry out more coordinated attacks, and botnets were deployed to increase the impact of the attacks. [8, p 6] This shows that the Russians had familiarized themselves with the systems, and now it was time to launch more massive attacks.

The Bronze Night in Estonia can be called the first cyber war in the world. It was not only an attack on the government but the people's daily activities were also affected. [13, p 61] People could not use the websites of banks, newspapers, political parties, ministries and companies [3]. Some of the banks prohibited network traffic from abroad. It was done because most of the attacking traffic came from outside Estonia. Some areas with few attacker were included to the list. [11]

In addition to the DDoS attacks, the website of the Estonian Reform Party was defaced. Sending spam via e-mail and sending spam in comments can also be considered as a part of the attack that Russia did against Estonia. [8, p 6]

There were many different attacks against Estonian information systems. Therefore, it can be assumed that behind the attack were different individuals, who got instructions from forums. The instructions on how to execute the attack were very simple. People with not-so-technical backgrounds were also able to attack. [11] One example of how the instructions were given is shown on the Figure 1.

Figure 1. Attack instructions that were given during the attacks against Estonian information systems [11].

Attacks against Estonia can be divided into two phases:

1. The first phase (April 27 - 29) – the attacks were quite simple and unorganized.
2. The second phase (April 30 - May 18) – the attacks were professionally coordinated, and on a larger scale, botnets were used. Attacks intensified on important days for Russia [12, p 18].

Major targets, such as government and private sector information channels like banking websites, were significantly affected. Attacks on the national Internet infrastructure and the brief disruption of the emergency number 112 were notable. Cyber attacks targeted Estonian Internet infrastructure institutions, governmental and political entities, private sector services, and personal entities, sparing traditional critical infrastructure like

transportation and energy systems information systems. [12, p 21] It is notable that the targets were chosen so it will have an impact on ordinary citizens' daily lives.

The first phase (April 27 - 29)

The start of the first phase was on the 27th of April evening. The target of these attacks were Estonian information systems and online media news sites [11] [12, p 18]. In this phase, the attacks were simple.

Attacks during the first phase:

- ping commands;
- some .bat files were made public for simple DoS attacks;
- malformed web queries against government and news websites. [12, p 18-19]

Overall the attacks in the first phase were simple and they were not difficult to mitigate. [12, p 19]

The second phase (April 30 - May 18)

The second phase was more coordinated and prepared. Carrying out attacks did not require a lot of special skills and attack instructions in forums were easy to follow. There were four waves during the second phase. [12, p 19]

Attacks during the second phase:

- DDoS attacks on websites;
- attacks against DNS servers and routers;
- DDoS attacks on bank websites and they were down for about 1.5 hours
- defacement of the Estonian Reform Party website;
- mass spam emails. [12, p 19-21]

During the second phase, some websites were inaccessible due to DDoS attacks that caused heavy traffic. Most of the attacks were manageable, but on the 9th of May, up to 58 websites were not accessible at once [12, p 19-20]. The defenders effectively managed the situation, resulting in minimal disruption to people's daily activities. The most notable occurrence during this period was Hansabank's need to suspend its online systems [14] [15]. It can be said that these cyber attacks had little impact on people's activities. In retrospect, it can be said that these attacks were more likely to sow confusion among people.

2.2.2 Cyber conflict between Georgia and Russia

The second conflict with the cyber attacks occurred a year later in South Ossetia in 2008. This conflict started between Georgia and Russia in August of 2008 [8, p 7]. South Ossetia is *de facto* independent from Georgia. The beginning of the war is considered to be when the Russian troops entered Georgia through the Roki tunnel on the 8th of August. Two months before that, military exercises were taking place in both, Russia and Georgia. [16, p 7]

Before the separatist provocations in August 2008, there started a conflict between OSCE (Organization for Security and Cooperation in Europe) troops. The coordination among these troops proved inadequate, resulting in a steady rise in tensions between Georgia and predominantly separatist groups backed by Russia. The first kinetic attack in this conflict was on the 7th of August in 2008 by Georgian forces. This attack was against the separatist forces. On the next day, the Russian Federation started military operations. Russian Forces first were in the South Ossetian region and then moved on to the Georgian region. On the 9th of August, Georgia announced the state of war. [12, p 67 - 68] At the beginning of the war, Russia provided a list of Georgian websites to attack. On the website stopgeorgia.ru, there were instructions how to attack Georgian websites. [14]

Before the war went kinetic, there were cyber attacks on Georgian cyber infrastructure [17]. Russian military incursions into South Ossetia coincided with a series of DDoS attacks that incapacitated Georgia's networks, severing government communications and defacing official websites. One of the defaced websites can be seen on the Figure 2. As it was in Estonia a year earlier, the Georgian banks and telecommunications providers were attacked [14]. When the kinetic war ended on the 12th of August 2008, the cyber attacks continued until the end of August [12, p 68].

The Estonia's and Russia's conflict had the political reason to start the attack. Georgia and Russia had many factors to start the war: geopolitical, legal, economic and cultural. In addition to the many reasons why Russia attacked Georgia, Russia also attacked Georgia on many fronts. Land, air, and sea were used as new methods of attack, and the cyber domain was involved in the war. Russia's cyber attacks on Georgian infrastructure were the first time when cyber attacks were planned to be coordinated with kinetic warfare. [17, p 17]

During the cyber conflict in Georgia, various websites were inaccessible to ordinary citizens. While the war was already ongoing in Georgia, a few hours later, the first DDoS attacks on Gorgia's websites started. During the attacks, more than 50 websites were

inaccessible to ordinary users. The botnet network used against Georgia had the same IP addresses used a year earlier (2007) in cyber attacks against Estonia. [18]

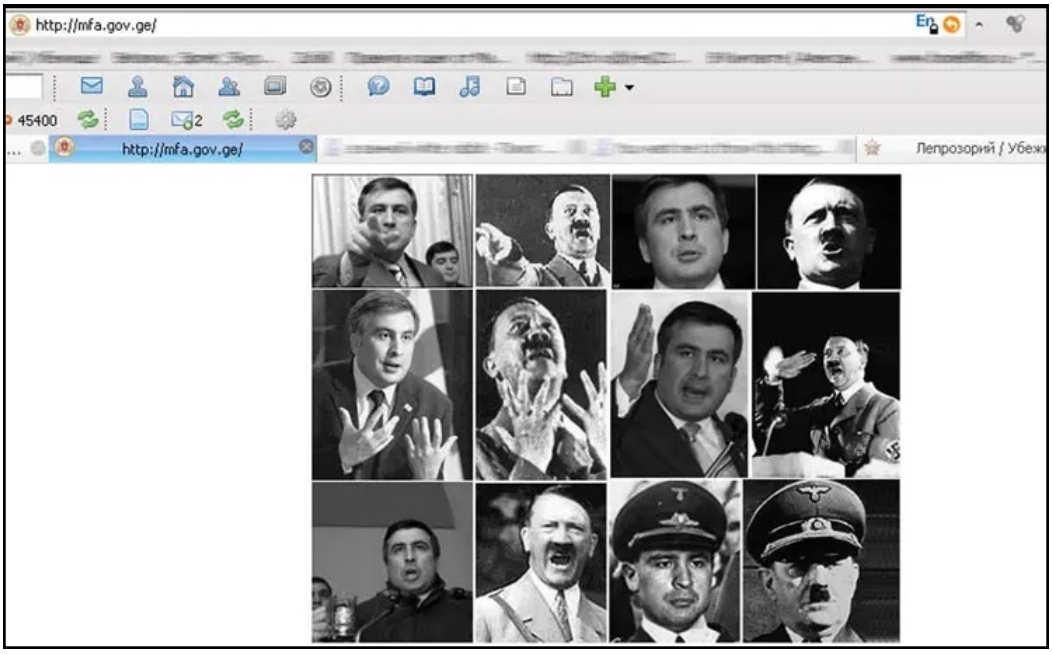

Figure 2. Defaced Georgian Parliament website [19].

During the second DDoS attack, the main targets were the websites of financial institutions, businesses and educational institutions. According to the investigation done by U.S. Cyber Consequences Unit, the cyber attacks were carried out by Russian civilians who had no direct connection with Russian authorities. Those Russian civilians who needed help were supported by Russian organised crime. [20]

Compared to the cyber attack against Estonia a year earlier, many more civilians were involved at that time [20]. As during the cyber attacks against Estonia, there were instructions on how to attack the websites. There were also instructions on how to attack Georgian websites. [14] The number of computers used for attacks was much smaller in the Georgia attack than in the attack against Estonia. [20]

Attack methods used during cyber conflict between Georgia and Russia:

- DDoS attack;
- SQL injections;
- defaced websites. [14, p 18], [16, p 10]

Although the cyber attacks in 2008 had minimal overall impact due to Georgia's limited IT infrastructure at the time, the Georgian government managed to reroute most of its traffic through servers in other countries, including the United States, Estonia, and Poland.

Nonetheless, it marked the first known instance of wide-scale offensive cyber operations being conducted alongside conventional military actions. [14, p 18]

2.2.3 Cyber conflict between Ukraine and Russia

The third conflict is between Ukraine and Russia. The conflict started in 2014 and escalated again in 2022 when Russia started a full-scale war in Ukraine. Although the armed military situation had calmed down in the meantime, cyber attacks still took place between 2014 and 2022. [21, p 23]

Just as in the case of cyber conflicts in Estonia and Georgia, the cyber conflict in Ukraine is also led by political reasons. In November 2013, then-President Viktor Yanukovych wanted to make Ukraine politically more like Russia. [21, p 12]

The cyber conflict in Ukraine is completely different from how it was in Estonia (2007) and Georgia (2008). Both Ukraine and Russia have done small DDoS attacks against each other. But there haven't been cyber attacks as big as against Estonia or Georgia. In a book published in 2015, Martin Libicki wrote that most of the war was taking place on social media. There was propaganda and information war on social media, mainly from the Russian side. He wrote that there weren't yet cyber attacks against critical infrastructure or defence systems at that time. [22] Before the end of 2015, Russia was gradually compromising the Ukrainian government and military systems. At the end of the 2015 Russia started to show their willingness to use cyber attacks to to achieve their results in kinetic warfare. [14]

In 2014, Ukraine got hit by *BlackEnergy* malware. It caused blackouts in several Ukrainian regions. [23] In 2017, another attack on Ukraine took place. *NotPetya* malware used Ukrainian accounting software to launch it. [24] *NotPetya* malware caused more than $10 billion in damage [25]. This cyber attack affected more than 220 000 Ukrainians. This was the biggest attack against Ukraine at that time. It was seen that this attack took a lot of time and preparation to deliver it. [14, p 20]

Before a full-scale kinetic conflict against Ukraine in 2022, there were several phishing campaigns [21]. Before and at the beginning of the full-scale kinetic conflict in Ukraine in 2022, Ukrainian banks and government websites were affected by the DDoS attack [21, p. 32].

Attack methods used during cyber conflict between Ukraine and Russia:

- phishing;
- malware;
- telephone denial of Service (TDoS);
- DDoS attack;
- SQL injections;
- defaced websites. [14, p 18] [16, p 10]

2.3 Research gap

While research has been conducted on cyber conflicts in Estonia, Georgia and Ukraine, some areas need further investigation. Firstly, the evolution of cyber attacks since 2007 requires analysis, focusing on events in Estonia, Ukraine, and Georgia. Understanding the motives behind these attacks.

Secondly, lessons from cyber attacks on Ukraine's infrastructure since 2022. Research should delve into the specific tactics used and strategies for mitigation and response. Moreover, examining the role of international cooperation in bolstering cyber resilience is essential.

Thirdly, there is need to anticipate and prepare for future cyber attacks. This requires a deeper understanding of emerging cyber threats, potential attack vectors, and best practices for enhancing cyber security and resilience.

Therefore, further research is necessary to comprehensively address these gaps, providing insights into the evolving nature of cyber warfare and informing strategies for mitigating cyber threats in the future. Such research is important for enhancing cyber security, protecting critical infrastructure, and preserving stability in an increasingly complex cyber threat landscape.

3. Methodology

The research was conducted using qualitative research. This research was done using the interviewing method. The interviews were conducted as individual interviews. This method was chosen so the interviewee could answer the questions at his/her own pace. The interviews were semi-structured, i.e. in addition to preparatory questions, the interviewer had the opportunity to ask clarifying questions.

During the thesis writing, 5 interviews were conducted with experts in Estonia. These experts have knowledge and experience of cyber conflicts, which are discussed in the thesis - Estonia, Georgia and Ukraine. The interviews were conducted individually, except for one interview in which two interviewees participated in the same interview.

The author of the thesis prepared the interview questions according to the research questions. The interview questions can be found in Appendix 1.2.

The interviews were analysed through listening them again and writing out important parts of the interviews. The results gained by the interviews are validated by other interviewers since the answers to the questions were similar. Extra validation for the thesis is not needed.

Interviews were conducted with the following people and for the sake of clarity of the analysis, the interviewees have been numbered and referred to accordingly:

- The interviewee 1 - Toomas Lepik
- The interviewee 2 - Rain Ottis
- The interviewee 3 - Paavo Kuiv
- The interviewee 4 - Hillar Aarelaid
- The interviewee 5 - Hillar Põldmaa

The first interviewee, Toomas Lepik, is a Cyber Security Analyst at the Centre for Digital Forensics and Cyber Security at Tallinn University of Technology [26]. He was chosen to be one of the interviewees because he has studied conflicts in Estonia and Georgia. [27]

The second interviewee, Rain Ottis, is a Tenured Associate Professor and Head of the Centre for Digital Forensics and Cyber Security [26]. Rain Ottis was chosen as one of the

interviewees because he thoroughly studied the conflict in Estonia in 2007. [28]

The third interviewee, Paavo Kuiv, is a specialist at CERT-EE and he knows about the events that took place in 2007 in Estonia, in 2008 in Georgia and starting in 2014 in Ukraine.

The fourth interviewee, Hillar Aarelaid, was chosen to get the interview because he was the head of CERT-EE when the cyber conflict occurred in 2007. [29]

The fifth interviewee, Hillar Põldmaa, is an information and cyber security lecturer at the University of Tallinn. [30]

All interviewees have been permitted to publish their names in the thesis.

In this thesis, Grammarly is a valuable tool for ensuring the accuracy and coherence of the written content. Its functionality encompasses spell-checking and the enhancement of sentence structure.

4. Analysis

In the following sections, there are interviews results.

4.1 Cyber conflict comparison

The first research question was:

[RQ1] To what extent have cyber attacks evolved in terms of tactics, scale, and state-sponsored involvement since 2007, with a specific focus on the events in Estonia (2007), Ukraine (2014 & 2022), and Georgia (2008)?

Based on the responses provided by the interviewees, we can analyze how cyber conflicts have evolved. The involvement is focusing on the events in Estonia (2007), Ukraine (2014 & 2022), and Georgia (2008).

4.1.1 Beginning of the cyber conflict

Interviewee 1 pointed out that social signs often precede cyber conflicts, such as political decisions leading to societal dissatisfaction. For instance, in the case of Ukraine's conflict in 2022 that has impacted Estonia. DDoS attacks followed the decision to remove a tank monument near Narva City in Estonia. These social tensions can empower individuals or groups with technical capabilities to organize attacks independently or acquire them from external sources.

Furthermore, Interviewee 1 highlighted a preparation phase in which attackers familiarize themselves with the target infrastructure, including listening to communication channels and conducting test attacks. This phase is followed by port scanning, indicating an advancing stage of cyber conflict where adversaries demonstrate an interest in the target environment. Political motivations often underpin such attacks.

Interviewee 2 compared the cyber attacks on Estonia in 2007 and Georgia in 2008, noting their similarity in tactics: primarily DDoS attacks, botnets, and spam attacks, suggesting possible involvement of hacktivists. However, these attacks lacked complexity and coordinated countermeasures from the targeted countries.

In contrast, Interviewee 2 highlighted Ukraine's experiences, where cyber attacks since 2014 have demonstrated a higher level of sophistication and coordination. Notable incidents include the NotPetya attack and targeted strikes on critical infrastructure like the electric grid. This suggests a shift towards more state-sponsored involvement and strategic planning.

Moreover, Interviewee 3 emphasized the importance of mapping out target infrastructure as a precursor to cyber conflict. This involves planning phishing campaigns and identifying vulnerabilities to exploit.

Interviewee 4 stressed the significance of having adequate sensors and capacity to detect and respond to cyber threats, indicating the importance of technological preparedness in mitigating cyber conflicts.

Lastly, Interviewee 5 highlighted the initial stages of cyber conflict, which often involve mapping out targets through activities like pinging or network scanning, serving as early warning signs.

In conclusion, cyber conflicts have evolved significantly since 2007, marked by a transition from unsophisticated and sporadic attacks to more complex, coordinated, and impactful campaigns. State-sponsored involvement has become more pronounced, reflecting geopolitical tensions and strategic interests. Understanding the signs of cyber conflict initiation, evolving tactics, and state-sponsored involvement is crucial for effective cybersecurity measures in today's interconnected world.

4.1.2 First weeks of the cyber conflict

Several notable changes emerge when comparing Estonian and Ukrainian cyber conflicts in the first weeks before the conflict began in 2007 and 2022.

Interviewee 1 highlights a shift in the visibility of port scanning activities. While scans were more pronounced in 2007, they have become more widespread yet less conspicuous in 2022, indicating a refinement in attackers' tactics to evade detection.

Interviewee 2 draws attention to the geopolitical context surrounding cyber conflicts. In 2007, the attacks on Estonia lacked a military dimension. This might be due to Estonia's membership in the EU and NATO. These acted as protective factors against escalation into kinetic conflict. However, in Ukraine in 2022, the primary dimension is kinetic conflict, with cyber operations playing a secondary role. This suggests that the strategic importance

of cyber operations may vary depending on the overall military and political context of the conflict.

Interviewee 3 provides insights into the response strategies of targeted nations. In 2007, Estonia's response to cyber attacks included wide publication of the attacks, indicating a more transparent approach to handling cyber incidents. However, in 2022, the response in Ukraine was less effective, with plans going awry and confusion ensuing, potentially due to misjudgments or miscalculations in response strategies.

Interviewee 4 offers a retrospective analysis of the attacks in 2007 in Estonia, noting the meticulous planning involved and the unforeseen challenges faced by the attackers. The importance of understanding the target's defence capabilities and adapting attack strategies accordingly is underscored, highlighting the complexity of cyber conflicts.

Interviewee 5 emphasizes the increasing severity and impact of cyber attacks over time. While attacks in 2007 primarily targeted websites through DDoS attacks, those in 2022 have expanded to disrupt critical services such as satellite phone connections, electric grids, and water supplies. This escalation in the scope and impact of cyber attacks underscores the evolving nature of cyber warfare tactics.

Overall, the responses from the interviewees provide valuable insights into how cyber attacks have evolved since 2007. These answers demonstrate changes in tactics, responses, and the strategic significance of cyber operations within the context of geopolitical conflicts.

4.1.3 Cyber conflict turning into kinetic war

The responses provided by the interviewees offer various perspectives. They focus on how to recognize the potential transition of a cyber conflict into a kinetic conflict or war. This aligns with the research question about the evolution of cyber attacks. It also addresses their potential escalation into broader conflicts.

Interviewee 1 highlights the importance of considering broader contextual factors beyond cyber operations alone. They emphasize that military activities, such as troop movements and military training, can serve as indicators of potential escalation. For instance, he mentions the presence of military camps near the Ukraine border before the full-scale war in 2022, indicating heightened tensions that could lead to kinetic conflict.

Interviewee 2 suggests that highly targeted cyber attacks against critical military infrastructure may signal the potential for escalation to kinetic conflict. Examples include radar

systems or air defence capabilities. They note that previous kinetic wars did not directly start from cyber attacks. However, they highlight the importance of monitoring attacks targeting military-used systems. These attacks could indicate strategic efforts to disrupt essential defence capabilities.

Interviewee 3 asserts that cyber and kinetic conflicts are interconnected, with one potentially supporting the other. While not providing specific indicators, this perspective underscores the complexity of modern conflicts. In these conflicts, cyber operations can be part of broader military strategies or serve as precursors to kinetic engagement.

Interviewee 4 suggested that cyber and kinetic conflicts may not necessarily be directly related or occur simultaneously. He argues that the effects of cyber attacks can persist beyond their initial occurrence, making it challenging to assess their direct impact on the escalation to kinetic conflict.

Interviewee 5 focuses on the role of strategic communication, including disinformation operations, as potential indicators of the escalation of conflicts. They highlight similarities between conflicts in Georgia (2008) and Ukraine (2022), where the presence of disinformation campaigns preceded broader kinetic engagements.

Overall, these perspectives offer insights into the complexities of recognizing the potential transition from cyber to kinetic conflict. Considering military activities, targeted cyber attacks on critical infrastructure, the interplay between cyber and kinetic operations, and the role of strategic communication helps stakeholders. It enables them to better understand and anticipate the escalation of conflicts into broader engagements.

4.1.4 Differences and similarities between Estonia 2007 and Georgia 2008 cyber conflict

The analysis focus on the main differences and similarities between the cyber attacks on Estonia in 2007 and Georgia in 2008. This analysis sheds light on the evolution of cyber attacks and their impact on different contexts.

Main differences between Estonia (2007) and Georgia (2008):

1. **Impact and Infrastructure**: Interviewee 1 highlights that the impact of the attacks differed due to variations in infrastructure and online services. Estonia, being more technologically advanced with widespread online services, experienced a bigger

impact compared to Georgia, which had fewer active media and internet users. Additionally, the communication mast being taken down in Georgia indicates a more direct physical impact compared to Estonia, where the impact was more on street riots and media coverage.

2. **Preparedness and Response**: Interviewee 2 notes that Estonia was relatively more prepared due to its e-governance initiatives, such as E-Estonia, which strengthened its resilience against cyber attacks. On the other hand, Georgia had to deal with additional challenges like concerns about kinetic attacks, which diverted attention and resources from cybersecurity measures.
3. **Infrastructure and Software Usage**: Interviewee 3 points out differences in the usage of IT infrastructure and software. Georgia's reliance on pirated Windows software and @mail.ru email addresses for official purposes contrasts with Estonia's use of licensed software and official email addresses, indicating variations in cybersecurity practices and standards.
4. **Adaptation and Learning**: Interviewee 4 mentions that while the attackers' plan in Estonia was disrupted, they adapted and learned from how to better the attack in Georgia. This suggests that attackers may refine their tactics based on previous experiences, highlighting the dynamic nature of cyber warfare.

Main Similarities:

1. **Attack Methods**: Despite the contextual differences, Interviewee 1 notes that both Estonia and Georgia experienced similar attack methods, including defacement and DDoS attacks on government websites and official news channels. This indicates a commonality in the tactics employed by the attackers across both incidents.
2. **Use of Botnets and Primitive Methods**: Interviewee 2 observes that both attacks utilized botnets and primitive methods, suggesting that the attackers relied on relatively basic tools and techniques to achieve their objectives. This similarity underscores the simplicity and accessibility of cyber attack methods during that time.
3. **Targeting of Government Systems**: Interviewee 5 emphasizes that both Estonia and Georgia were targeted at the level of government websites and official news channels. This indicates a shared focus on disrupting governmental operations and communication channels.

In conclusion, notable differences existed in the impact, preparedness, infrastructure, and response strategies between the cyber attacks on Estonia and Georgia. However, significant similarities existed in the attack methods employed and the targets selected. These insights contribute to understanding how cyber attacks have evolved.

4.1.5 Differences and similarities between Estonia 2007 and Ukraine 2022 cyber conflict

Analyzing the interviewees' responses offers valuable insights. They focus on the main differences and similarities between the cyber attacks on Estonia in 2007 and Ukraine in 2022. This analysis provides valuable insights into the evolution of cyber attacks and their impact over time.

Main Differences:

1. **Scope and Impact**: Interviewee 1 highlights that the cyber attacks in Ukraine in 2022 targeted the energy sector and communication channels, with repercussions extending to kinetic warfare. This suggests a broader and more severe impact compared to the cyber attacks in Estonia in 2007. Those attacks primarily involved rioting and disruption of communication channels. However, they did not escalate to kinetic conflict.
2. **Response and International Assistance**: Interviewee 2 notes that Ukraine received significant assistance from other countries in response to the cyber attacks. In contrast, Estonia primarily relied on its own resources. It requested external help to combat botnets. This difference underscores the shift towards greater international cooperation and support in responding to cyber attacks over time.
3. **Technological Advancements and Time**: Interviewees 3 and 4 emphasize the role of technological advancements and the passage of time as significant differences between the cyber attacks on Estonia and Ukraine. Improved technology has influenced both attackers and defenders, leading to more sophisticated tactics and defences in the latter case.

Main Similarities:

1. **Propaganda and Information Warfare**: Interviewee 5 points out that both Estonia and Ukraine experienced significant propaganda efforts alongside the cyber attacks. This similarity suggests a common strategy employed by aggressors to manipulate public opinion and sow discord in targeted countries.
2. **Cyber Attacks as Part of Hybrid Warfare**: Despite differences in scope and impact, both Estonia and Ukraine experienced cyber attacks. These attacks were part of broader hybrid warfare strategies, combining conventional military tactics with cyber operations and propaganda efforts. This indicates a commonality in the strategic approach adopted by aggressors in both cases.

In conclusion, there are notable differences in the scope, response, and technological context of the cyber attacks on Estonia in 2007 and Ukraine in 2022. However, there are also significant similarities regarding the propaganda efforts and the integration of cyber attacks into broader hybrid warfare strategies.

4.1.6 Social media in these conflicts

Analyzing the responses provided by the interviewees sheds light on the role of social media in cyber conflicts. It also reveals how this role has evolved since 2007. This aligns with the research question concerning the evolution of cyber attacks.

Role of Social Media:

1. **Shift in Usage and Accessibility:** Interviewee 1 highlights the significant shift in the accessibility and widespread use of social media platforms over time. In 2007, social media was not as prevalent, but by 2022, nearly everyone had access to social media accounts, demonstrating a substantial increase in social media usage across populations.
2. **Evolution of Communication Channels:** Interviewee 2 points out the evolution of communication channels from forums in 2007 to various social media apps in later years. This shift indicates changes in the platforms used for disseminating information and coordinating activities, with forums being replaced by platforms like Telegram channels.
3. **Impact of AI and Information Operations:** Interviewee 2 also highlights the impact of AI on social media, including deepfakes, false news, and bot-driven misinformation campaigns. These developments amplify the role of social media in information operations, indicating a more sophisticated approach to manipulating public opinion and spreading propaganda.
4. **Targeted Social Media Channels:** Interviewee 3 mentions the emergence of targeted social media channels during conflicts, such as those seen in the war in Donbass in 2014. This demonstrates the use of social media as a tool for targeted messaging and propaganda dissemination, reflecting its role in shaping narratives during conflicts.
5. **Adaptation and Utilization:** Interviewee 4 discusses how Georgians adapted to social media as a means of communication when traditional channels were compromised. This adaptation underscores the importance of social media as an alternative information dissemination platform during times of crisis.
6. **Propagation of Information and Propaganda:** Interviewee 5 emphasizes the proliferation of social media channels for spreading propaganda and sharing tactical

information. This highlights the role of social media not only in communication but also in facilitating strategic and tactical coordination among actors involved in conflicts.

In conclusion, the analysis of the interview responses illustrates the evolving role of social media in cyber conflicts since 2007. Social media has become a pivotal element in contemporary cyber conflicts. It transitioned from limited use and impact in the early 2000s to widespread adoption and instrumental role in information operations and propaganda dissemination today. These insights contribute to our understanding of how cyber conflicts have evolved. They shed light on tactics, scale, and state-sponsored involvement. This aligns with the research question's focus on the evolution of cyber attacks.

4.2 Cyber conflict in Ukraine

The second research question was:

[RQ2] What lessons can be drawn from the cyber attacks on Ukraine's infrastructure since 2022?

Signs that cyber attacks may start on Ukrainian infrastructure:

1. **Kinetic Attacks Preceding Cyber Attacks:** Interviewee 1 highlights that in 2022, the war started with physical attacks on Ukraine, which were supported by taking down communication channels. This suggests a coordinated approach where cyber attacks were used in conjunction with traditional warfare tactics.
2. **Recognition of Russian Intentions:** Interviewee 2 mentions the "green little man" and indicates that it would be naive to disregard Russia's intentions regarding Crimea and potential invasion plans. While not directly related to cyber attacks, this recognition of geopolitical tensions and intentions could be seen as a precursor to cyber aggression.
3. **Historical Context and Prior Incidents:** Interviewee 3 emphasizes the importance of considering events over the past two decades, mentioning significant cyber incidents like BlackEnergy and NotPetya in 2014. This underscores the need to analyze cyber attacks within a broader historical context to understand their evolution.
4. **Constant Pressure and Lack of Specificity:** Interviewee 4 notes the constant pressure on Ukraine without highlighting any specific cyber-related markers. This suggests a continuous state of vulnerability rather than isolated incidents.
5. **Connection Between Real-World Events and Cyber Attacks:** Interviewee 5 provides insights into the connection between real-world events and cyber attacks,

citing the gathering of Russian troops in Yelnya in 2020/2021 as a signal of potential conflict. This highlights the interplay between geopolitical tensions and cyber activities, indicating that cyber attacks are often linked to broader strategic objectives.

Overall, the responses from the interviewees demonstrate the complex relationship between geopolitical events, traditional warfare tactics, and cyber attacks. They emphasize the importance of considering historical context, recognizing signs of potential aggression, and understanding the interconnectedness between physical and cyber domains in conflict situations.

The following list will give some ideas of what Ukraine could have done better before the cyber attacks started on its infrastructure.

1. **Limited Focus on Cyber Operations Pre-War:** Interviewee 1 suggests that in 2014, the focus was primarily on political signs and physical actions rather than cyber operations. This indicates a shift in tactics over time, where cyber attacks may have played a supporting rather than a primary role in the conflict.
2. **Emphasis on Foundational Cybersecurity:** Interviewee 2 acknowledges that determining specific actions Ukraine could have taken to prevent the attack is challenging. They emphasize the importance of having a strong cybersecurity foundation. This foundation should encompass people, technology, procedures, and an uncorrupted environment. This underscores the evolution of cyber attacks, highlighting the need for robust defences to mitigate their impact.
3. **Underutilization of Resources:** Interviewee 3 highlights that Ukraine had significant resources after the collapse of the Soviet Union but failed to utilize them effectively. This suggests a lack of strategic foresight and investment in cybersecurity measures, potentially contributing to vulnerability in the face of cyber attacks.
4. **Historical Context and Beliefs:** Interviewee 4 mentions Ukraine's historical context and disbelief that they would be targeted for attack. This indicates a failure to recognize the evolving threat landscape and adapt defences accordingly, emphasizing the need for increased awareness and preparedness for cyber threats over time.
5. **Speculation and Social Problems:** Interviewee 5 mentions speculation about Ukraine being a remnant of the Soviet Union and alludes to social problems within the country. While not directly addressing cyber attacks, this suggests broader systemic issues that may have hindered Ukraine's ability to effectively defend against cyber threats.

Overall, the responses highlight the multifaceted nature of cyber attacks and the challenges countries like Ukraine face in adapting to evolving threats. They underscore the importance

of proactive cybersecurity measures, strategic foresight, and investment in resilience to mitigate the impact of cyber attacks on critical infrastructure.

Overall, the responses provide insights into the evolving nature of cyber conflict preparation. They highlight the importance of comprehensive response strategies, risk prioritization, technical solutions, continuous learning, and maintaining public trust and confidence. These factors contribute to understanding how cyber attacks have evolved. They shed light on tactics, scale, and state-sponsored involvement since 2007, particularly through the lens of events in Estonia, Ukraine, and Georgia.

4.3 Future cyber attacks

The third research question was:

[RQ3] What can we expect from cyber attacks in the future, and how best to prepare for them?

This list gives an overview of what can be expected from the cyber conflict in Ukraine.

1. **Diverse Cyber Threats:** Interviewee 1 highlights the multifaceted nature of cyber threats, including infrastructure attacks and information breaches. This suggests an evolution in cyber attack tactics, encompassing various methods beyond traditional breaches.
2. **Secondary Role of Cyberattacks:** Interviewee 2 suggests that cyberattacks will play a secondary role in the conflict, with primary focus on the front lines and attacks against countries and companies supporting Ukraine. This reflects a shift in scale and state-sponsored involvement, indicating potential attacks against the supply chain and allies of Ukraine.
3. **Sophistication of Cyber Tactics:** Interviewee 3 discusses the sophistication of Russian cyber tactics, including DDoS attacks and phishing, highlighting the evolving nature of cyber attacks in terms of tactics and state-sponsored involvement. The emphasis on reconnaissance and obtaining information for future attacks indicates a strategic evolution in cyber warfare.
4. **Integration of Cyber and Kinetic Warfare:** Interviewee 4 mentions the integration of cyber elements into kinetic warfare, suggesting a convergence of traditional and cyber tactics. This indicates an evolution in the scale and tactics of cyber attacks, with cyber elements being used to support physical operations.
5. **Targeting Critical Infrastructure:** Interviewee 5 emphasizes the continued targeting of critical infrastructure by Russia, both physically and cybernetically, to weaken

resistance. This aligns with the research question's focus on understanding the scale and impact of cyber attacks on critical infrastructure since 2007.

Overall, the responses provide insights into the evolving nature of cyber conflict, highlighting the diversification, sophistication, and integration of cyber tactics with traditional warfare.

This list gives an overview of cyber attacks against ordinary citizens.

1. **Impact on Ordinary Citizens:** Interviewee 1 points out that cyber attacks are designed to impact ordinary citizens, whether through attacks on critical infrastructure or other means. This suggests an evolution in tactics, with adversaries aiming to cause suffering and damage morale among the targeted population.
2. **Targeting Civilian Infrastructure:** Interviewee 2 highlights the targeting of civilian infrastructure by adversaries, such as communication channels used by civil society. This reflects a shift in tactics, with attackers exploiting vulnerabilities in systems used by ordinary citizens as potential targets.
3. **Exploitation of Vulnerabilities:** Interviewee 3 mentions the exploitation of vulnerabilities in call center hosting in Ukraine before the full-scale war. This indicates a tactic of targeting civilian infrastructure and services, further illustrating the evolving landscape of cyber attacks on ordinary citizens.
4. **Social Engineering and Scams:** Interviewee 4 discusses the use of social engineering tactics, such as phone scams targeting soldiers' families in Ukraine. This demonstrates an adaptation in tactics, with attackers exploiting personal connections and emotions to achieve their goals.
5. **Impact on Morale:** Interviewee 5 emphasizes the importance of targeting vital services to bring down people's morale. This aligns with the research question's focus on understanding the scale and impact of cyber attacks on ordinary citizens, indicating a strategic objective of undermining societal resilience and morale.

Overall, the responses provide insights into the evolving nature of cyber conflicts, highlighting a shift towards targeting ordinary citizens and civilian infrastructure as part of state-sponsored cyber operations. These factors contribute to understanding how cyber attacks have evolved in terms of tactics, scale, and state-sponsored involvement since 2007, particularly through the lens of events in Estonia, Ukraine, and Georgia.

The following list gives an overview of how great media and other channel coverage about cyber will affect future cyber attacks.

1. **Shift towards Targeting Ordinary Citizens:** Interviewee 1 suggests that increased discussion about cyber attacks may lead to a higher frequency of attacks directed at ordinary citizens, with a focus on perpetrating various frauds. This aligns with the evolving tactics of cyber attacks, indicating a potential escalation in targeting civilian populations to weaken the resistance of the attacked country.
2. **Exploitation of AI and Deepfakes:** Interviewee 2 highlights the evolving tactics of cyber attacks, particularly through the use of AI and deepfakes. Increased discussion of cyber issues could lead to more sophisticated attacks where adversaries use AI chatbots to trick people. This reflects a shift in tactics and scale, with attackers exploiting advancements in technology to carry out more effective attacks.
3. **Impact of Media Reporting:** Interviewee 3 discusses a tacit agreement with media houses. They propose limiting reporting on DDoS attacks. This suggestion implies increased media discussion about cyber attacks might inadvertently empower attackers. It illustrates the potential consequences of public discourse on cyber attacks. Such discourse can influence the tactics and scale of these attacks.
4. **Knowledge Gap in Public Discourse:** Interviewee 4 points out a potential downside of increased cyber attack discussion. They note that despite the growing conversation, there may be a lack of understanding among individuals discussing the topic. This highlights the importance of informed discourse and education in addressing cyber threats effectively.
5. **Focus on Real-world Impact:** Interviewee 5 emphasizes the importance of considering the real-world impact of increased discussion about cyber attacks. While discussion itself may not directly affect the frequency or sophistication of attacks, it may influence the effectiveness of the influence achieved by such attacks in the real world. This suggests a broader perspective on the relationship between discourse and cyber attacks, beyond just tactics and scale.

Overall, the responses provide insights into the potential implications of increased discussion about cyber attacks, highlighting shifts in tactics, scale, and state-sponsored involvement since 2007.

This final list will give an overview of what role will state-sponsored attacks play in future cyber conflict.

1. **Assurance of State-Sponsored Attacks:** Interviewee 1 straightforwardly acknowledges the presence of state-sponsored attacks in future cyber conflicts. This indicates a continuation of state involvement in cyber warfare, aligning with the research question's focus on state-sponsored involvement since 2007.
2. **Comparison with Physical Attacks:** Interviewee 2 compares state-sponsored cyber

attacks with physical attacks, suggesting that physical attacks may have a more significant impact economically or on public health. This perspective highlights the interplay between cyber and physical warfare tactics, indicating an evolution in the scale and tactics of state-sponsored involvement in cyber conflicts since 2007.

3. **Ethical Considerations:** Interviewee 3 raises ethical considerations regarding individuals who participate in cyber warfare, particularly in the context of forming a Ukrainian IT army. This suggests a broader discussion on the implications of state-sponsored attacks and the ethical responsibilities of individuals involved, reflecting on the evolving dynamics of cyber conflicts.
4. **Post-War Activities:** Interviewee 4 discusses the potential actions of individuals involved in cyber attacks post-war, such as Ukrainian call centers scamming Russians. This raises questions about the long-term implications of state-sponsored cyber attacks and the potential for such activities to continue or shift focus after conflicts end.
5. **Outsourcing of Cyber Operations:** Interviewee 5 highlights the outsourcing of cyber operations by Russia to different organizations and knowledgeable individuals, indicating a complex landscape of state-sponsored cyber activities. This suggests an evolution in the tactics and scale of state-sponsored involvement in cyber conflicts, with states leveraging external expertise and resources to conduct cyber operations.

Overall, the responses provide insights into the evolving role of state-sponsored attacks in future cyber conflicts, highlighting shifts in tactics, scale, and ethical considerations since 2007. These factors contribute to understanding the evolving nature of cyber attacks and state-sponsored involvement in cyber warfare, particularly in the context of events in Estonia, Ukraine, and Georgia.

5. Discussion

In this chapter there is a discussion about the finding that has been found in the analysis part.

5.1 Evolution of Cyber Attacks

The literature review provides a comprehensive overview of the evolution of cyber attacks in Eastern Europe, tracing their development from rudimentary tactics to sophisticated state-sponsored operations. Initially, cyber conflicts were characterized by politically motivated actions, such as DDoS attacks and website defacements. For example, the Bronze Night events in Estonia in 2007 and the conflict in Georgia in 2008 primarily involved such basic tactics. However, as highlighted by P.W. Singer and A. Friedman [2], cyber warfare has evolved alongside traditional forms of warfare, with an increasing emphasis on achieving political goals through violence, albeit in cyberspace. This evolution is evident in the shift towards more coordinated and impactful campaigns targeting critical infrastructure, as seen in Ukraine since 2014.

The interview results support this narrative, indicating that cyber attacks have become more sophisticated over time. Notably, the use of advanced malware like NotPetya in Ukraine demonstrates a higher level of complexity and strategic planning. This shift towards state-sponsored involvement and the use of sophisticated tactics underscores the growing importance of cyber warfare as a strategic tool in geopolitical conflicts.

5.2 Geopolitical Context and Motivations

The conflicts in Estonia, Georgia, and Ukraine are deeply rooted in geopolitical tensions and territorial disputes. Political decisions or actions often serve as triggers for cyber aggression. For instance, the decision to relocate a war memorial in Estonia led to the Bronze Night cyber attacks, while the conflict between Georgia and Russia in 2008 was preceded by military tensions in the South Ossetia region. Similarly, the ongoing conflict in Ukraine has been fueled by political unrest and attempts by various actors to exert influence over the country's territory.

The interview results provide further insight into the motivations behind these conflicts. The war Ukraine, for example, has impacted the Estonia, when Estonian government

decided to remove a tank monument near Narva City sparked cyber aggression from Russia. This illustrates how events can escalate influence to use cyber attacks when viewed through a geopolitical lens. Moreover, the interconnectedness between real-world events and cyber activities underscores the complex nature of modern warfare, where cyber attacks are used as tools to achieve strategic objectives.

5.3 Tactics and State-Sponsored Involvement

The tactics employed in cyber conflicts have evolved significantly over time, from simple DDoS attacks to more complex and coordinated campaigns. The literature review outlines how early conflicts primarily involved basic methods like DDoS attacks and website defacements, often carried out by non-state actors. However, as seen in the conflicts in Georgia and Ukraine, state-sponsored involvement has become increasingly prevalent, with attackers using sophisticated malware and targeting critical infrastructure.

The interview results provide additional evidence of state-sponsored involvement in cyber conflicts. For example, the use of advanced malware like NotPetya in Ukraine suggests a level of sophistication that is typically associated with state actors. This indicates a shift towards more strategic planning and coordination, with cyber attacks being used as part of broader geopolitical strategies.

5.4 Role of Social Media and Information Warfare

Social media has played a significant role in shaping the narrative and dissemination of information during cyber conflicts. It has become a key battleground for propaganda dissemination and information warfare, amplifying the impact of cyber attacks. The emergence of targeted social media channels and the use of AI to spread misinformation underscore the complexity of modern cyber conflicts.

The interview results further emphasize the importance of social media in cyber conflicts, with propaganda efforts and misinformation campaigns playing a central role in shaping public opinion and influencing the outcome of conflicts. For example, in Ukraine, social media was used as a platform for spreading propaganda and disinformation, further fueling tensions and exacerbating the conflict. This highlights the need for greater awareness and resilience against information warfare tactics in cyberspace.

5.5 Interconnectedness of Physical and Cyber Domains

The interconnectedness between physical and cyber domains is a central theme in modern cyber conflicts. Both the literature review and interview results underscore the coordinated approach where cyber attacks are used alongside traditional warfare tactics. For instance, in the conflicts in Georgia and Ukraine, cyber attacks were preceded by physical actions, such as military incursions or territorial disputes.

This interconnectedness highlights the need for a holistic approach to defense that addresses both physical and digital threats. Moreover, the integration of cyber elements into kinetic warfare indicates a convergence of traditional and cyber tactics, further blurring the lines between physical and cyber domains. This underscores the importance of considering both aspects in conflict preparation and defense strategies.

5.6 How to best prepare for the cyber attacks

The following points will give an overview about how to best prepare for the cyber attacks.

1. **Importance of Preparedness and Reaction:** Interviewee 1 emphasizes the need for not only preventing cyber attacks but also knowing how to react to them effectively. This highlights the evolving nature of cyber threats and the necessity for comprehensive response strategies.
2. **Asset Protection and Risk Prioritization:** Interviewee 2 suggests that it's crucial to identify and protect key assets before an attack occurs, as it's impossible to prevent all attacks entirely. This aligns with the research question's focus on understanding how cyber attacks have evolved in terms of tactics and scale. It indicates a shift towards prioritizing protection based on risk assessment.
3. **Technical Solutions and Early Preparation:** Interviewee 3 mentions the importance of technical solutions like DDoS attack protection and emphasizes the need for early preparation and well-negotiated contracts. This reflects the evolving sophistication of cyber attacks and the importance of proactive defence measures.
4. **Continuous Learning and Awareness:** Interviewee 4 underscores the importance of staying informed through continuous learning and reading news, highlighting the dynamic nature of cyber threats and the need for ongoing adaptation and education.
5. **Focus on Critical Infrastructure and Trust:** Interviewee 5 emphasizes the importance of keeping critical infrastructure operational and maintaining public confidence in the country's governance and institutions. This aligns with the research question's focus on state-sponsored involvement and indicates a recognition of the intercon-

nectedness between cyber attacks and broader societal trust and stability.

5.7 Lessons Learned and Future Threats

The conflicts in Estonia, Georgia, and Ukraine offer valuable lessons for understanding the nature of cyber warfare and preparing for future threats. Understanding the coordinated nature of cyber attacks, geopolitical awareness, and historical context are crucial. Looking ahead, future threats are expected to be diverse and multifaceted, with attackers employing sophisticated techniques to target critical infrastructure and disrupt essential services. This underscores the need for proactive defense measures, international cooperation, and a comprehensive approach to cybersecurity. Additionally, the increasing interconnectedness of physical and cyber domains necessitates a holistic approach to defense that addresses both aspects effectively.

6. Results

The following chapter will give the results to the research questions.

6.1 First research question results

[RQ1] To what extent have cyber attacks evolved in terms of tactics, scale, and state-sponsored involvement since 2007, with a specific focus on the events in Estonia (2007), Ukraine (2014 & 2022), and Georgia (2008)?

Based on the analysis of the intervieews, cyber attacks have evolved significantly since 2007, both in tactics and state-sponsored involvement. Initially, cyber conflicts often stemmed from social tensions and political decisions. For example, when the Ukraine's conflict began in 2022 Estonia made the decision to remove te tank monument near Narva city. It was triggering the Russian hackers to start DDoS and spam attacks against Estonian infrastructure. They also had limited coordination and countermeasures.

However, over time, cyber attacks have become more sophisticated, coordinated, and impactful, particularly evident in Ukraine since 2014. Attacks such as NotPetya and targeted strikes on critical infrastructure demonstrate a higher level of sophistication. They also show state-sponsored involvement. This indicates a shift towards strategic planning. Geopolitical tensions play a significant role in this shift.

Furthermore, differences and similarities between cyber conflicts in Estonia, Georgia, and Ukraine highlight the evolution of tactics and responses. While attacks on Estonia and Georgia in the late 2000s primarily employed basic methods like DDoS attacks and targeted government systems, cyber attacks on Ukraine in 2022 targeted critical infrastructure. The repercussions extended to kinetic warfare. However, propaganda efforts and integrating cyber attacks into broader hybrid warfare strategies remain common in these conflicts.

The role of social media has also evolved significantly, from limited usage in the early 2000s to widespread adoption and instrumental involvement in information operations and propaganda dissemination today. The emergence of targeted social media channels underscores the evolving nature of cyber conflicts. The impact of AI on spreading mis-information also highlights this evolution. Understanding these dynamics is crucial for effective cybersecurity measures.

In conclusion, cyber attacks have evolved markedly since 2007. There has been a transition from unsophisticated and sporadic attacks to more complex, coordinated, and impactful campaigns. Increased state-sponsored involvement and the evolving role of social media play pivotal roles in contemporary cyber conflicts.

6.2 Second research question results

[RQ2] What lessons can be drawn from the cyber attacks on Ukraine's infrastructure since 2022?

The cyber attacks on Ukraine's infrastructure were preceded by physical attacks, suggesting a coordinated approach where cyber attacks were used alongside traditional warfare tactics. This underscores the importance of recognizing the interconnectedness between physical and cyber domains in conflict situations.

Recognition of geopolitical tensions and intentions, such as Russia's actions in Crimea, is crucial. Understanding these intentions can serve as a precursor to cyber aggression, highlighting the importance of geopolitical awareness in anticipating and preparing for cyber attacks.

Analyzing cyber attacks within a broader historical context, including prior incidents like BlackEnergy and NotPetya in 2014, is essential. This historical perspective helps in understanding the evolution of cyber threats and preparing better for future attacks.

The constant pressure on Ukraine without specific cyber-related markers indicates a continuous state of vulnerability rather than isolated incidents. This suggests the importance of maintaining a state of readiness and resilience against cyber threats.

The connection between real-world events, such as the gathering of Russian troops, and cyber attacks highlights the interplay between geopolitical tensions and cyber activities. Cyber attacks are often linked to broader strategic objectives, emphasizing the need to consider both physical and cyber aspects in conflict preparation.

In summary, the lessons learned include the importance of understanding the coordinated nature of cyber attacks. Geopolitical awareness and historical context are also crucial. Continuous vulnerability and recognizing the interplay between real-world events and cyber activities are essential. These lessons can inform future strategies for enhancing cybersecurity and resilience against cyber threats to critical infrastructure.

6.3 Third research question results

[RQ3] What can we expect from cyber attacks in the future, and how best to prepare for them?

In the evolving cyber conflict landscape, the future of attacks seems characterized by diverse threats. Cyber adversaries are expected to employ various methods beyond traditional breaches, including attacks on critical infrastructure and information. This indicates a shift towards more sophisticated tactics aimed at disrupting essential services and compromising data.

While cyberattacks may not always take center stage in conflicts, they are increasingly playing a significant role. There's a growing trend of targeting countries and companies that support adversaries' targets, suggesting potential attacks against supply chains and allies. This highlights the interconnected nature of cyber warfare and the importance of defending not only one's own infrastructure but also the broader network of partners.

Cyber attackers continually evolve tactics, utilizing techniques such as DDoS attacks, phishing, and reconnaissance. This evolution underscores the need for proactive defence measures that can adapt to emerging threats in real-time. Moreover, the integration of cyber elements into kinetic warfare indicates a convergence of traditional and cyber tactics, emphasizing the importance of a holistic approach to defence that addresses physical and digital threats.

Critical infrastructure remains a prime target for cyber adversaries, with attacks aimed at weakening resistance both physically and cybernetically. This underscores the strategic objective of undermining societal resilience and morale. To prepare for future cyber threats, it's imperative to enhance cybersecurity measures across critical infrastructure by investing in robust defence mechanisms and fostering international cooperation to address state-sponsored cyber threats effectively.

Additionally, educating the public about cybersecurity risks and promoting responsible media reporting can help mitigate the impact of cyber attacks on ordinary citizens and civilian infrastructure. Ethical considerations surrounding state-sponsored cyber warfare and the outsourcing of cyber operations emphasize the need for a comprehensive approach addressing both technical and ethical/legal aspects of cyber defence and deterrence. By adopting a proactive and multifaceted strategy, nations can better prepare for the evolving nature of cyber conflict and mitigate its potential impact on society.

7. Summary

The thesis results offer significant insights into the evolution, tactics, and implications of cyber attacks since 2007, particularly focusing on events in Estonia, Georgia, and Ukraine. The analysis reveals several key trends and lessons that shape our understanding of modern cyber warfare.

Firstly, the evolution of cyber attacks from sporadic and unsophisticated actions to more complex, coordinated campaigns demonstrates the growing strategic importance of cyber warfare. The initial conflicts, such as the Bronze Night events in Estonia and the conflict in Georgia in 2008, primarily involved basic methods like DDoS attacks and website defacements. However, since then, there has been a notable shift towards more sophisticated tactics, often with state-sponsored involvement. The integration of cyber attacks into broader hybrid warfare strategies, as seen in Ukraine since 2014, underscores the evolving nature of cyber conflicts. Moreover, the emergence of social media as a pivotal tool for propaganda dissemination and information operations has further amplified the impact of cyber attacks.

Secondly, the interconnectedness between physical and cyber domains in conflict situations is a key theme that emerges from the analysis. Cyber attacks often complement traditional warfare tactics, highlighting the importance of understanding the interplay between these domains. Geopolitical awareness and historical context are deemed essential for anticipating and preparing for cyber threats. Events such as the decision to relocate a tank monument in Estonia and the conflict in South Ossetia in 2008 illustrate how events can escalate into full-blown cyber conflicts.

Lastly, the future of cyber attacks is expected to be characterized by diverse and multifaceted threats. Adversaries continually evolve tactics, necessitating proactive defense measures and international cooperation to address state-sponsored cyber threats effectively. Attacks on critical infrastructure, such as the NotPetya malware targeting Ukrainian systems, highlight the potential for significant disruption and economic damage. Moreover, the increasing interconnectedness of physical and cyber domains emphasizes the need for comprehensive strategies that address both aspects of warfare.

In summary, the thesis highlights the evolving nature of cyber conflicts and emphasizes the need for comprehensive strategies to mitigate their impact on society. By understanding the

evolution, tactics, and implications of cyber attacks, policymakers and defense experts can better prepare for future threats and safeguard critical infrastructure and national security.

References

[1] *Warsaw Summit Communiqué*. Accessed: October 25, 2023. 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[2] P.W. Singer and A. Friedman. *Cybersecurity and Cyberwar*. What Everyone Needs To Know. OUP USA, 2014. ISBN: 9780199918119.

[3] Ian Traynor. *Russia accused of unleashing cyberwar to disable Estonia*. Accessed: October 24, 2023. 2007. URL: https://www.theguardian.com/world/2007/may/17/topstories3.russia.

[4] Aaron Mannes and James Hendler. *Net Attack*. Accessed: October 20, 2023. 2007. URL: https://www.wsj.com/articles/SB118099627980924270.

[5] Erik Gartzke. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth". In: *International Security* 38.2 (2013), pp. 41–73. ISSN: 01622889, 15314804. URL: http://www.jstor.org/stable/24480930.

[6] Rain Ottis. *Routledge Handbook of the Future of Warfare*. Routledge, 2023. Chap. Conflict in Cyberspace. ISBN: 9781003299011. URL: https://www.taylorfrancis.com/chapters/edit/10.4324/9781003299011-43/conflict-cyberspace-rain-ottis?context=ubx&refId=eeadc055-6035-49bf-83e5-738d1087910a.

[7] Ryan C. Maness and Brandon Valeriano. "The Impact of Cyber Conflict on International Interactions". In: *Armed Forces Society* 42.2 (2016), pp. 301–323. ISSN: 0095327X, 15560848. URL: https://www.jstor.org/stable/48670248 (visited on 05/04/2024).

[8] Thomas Rid. *Cyber War Will Not Take Place*. USA: Oxford University Press, Inc., 2013. ISBN: 0199330638.

[9] Martin C Libicki. *Conquest in cyberspace: national security and information warfare*. Cambridge University Press, 2007.

[10] Thomas Elkjer Nissen. *# TheWeaponizationOfSocialMedia:@ Characteristics_of_-Contemporary_Conflicts*. Royal Danish Defence College, 2015.

[11] Rain Ottis. "Analysis of the 2007 cyber attacks against estonia from the information warfare perspective". In: 2008, pp. 163–168. URL: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

[12] Kadri Kaska Eneken Tikk and Liis Vihu. "International Cyber Incidents". In: (2010).

[13] Välisministeerium. *Pilk peeglisse 2007*. Accessed: October 25, 2023. 2007. URL: https://vm.ee/sites/default/files/content-editors/web-static/115/cyber_attacks.pdf.

[14] Michael Connell and Sarah Vogler. *Russia's approach to cyber warfare*. CNA Arlington, VA, 2017.

[15] Mark Landler and John Markoff. "Digital fears emerge after data siege in Estonia". In: *The New York Times* 29 (2007), p. 2007.

[16] Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata. "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war". In: *Security Dialogue* 43.1 (2012), pp. 3–24. ISSN: 09670106, 14603640. URL: http://www.jstor.org/stable/26301960 (visited on 03/05/2024).

[17] David Hollis. "Cyberwar case study: Georgia 2008". In: (2011).

[18] Cameran Ashraf. "A preliminary engagement with the spatiality of power in cyberwar". In: *GeoJourna* 88.5 (2023), pp. 5555–5573. ISSN: 03432521. URL: https://doi.org/10.1007/s10708-023-10929-z.

[19] John Markoff. "Before the gunfire, cyberattacks". In: *New York Times* 12 (2008), pp. 27–28.

[20] John Bumgarner and Scott Borg. "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008". In: *US-CCU Special Report* (2009).

[21] Magnus Sandem Dhelie et al. "Methods Used in Cyberattacks in the War Between Russia & Ukraine". B.S. thesis. NTNU, 2023.

[22] Martin Libicki. *Cyber War in Perspective: Russian Aggression against Ukraine*. CCDCOE, 2015. Chap. The Cyber War That Wasn't. ISBN: 978-9949-9544-5-2. URL: https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf.

[23] Kim Zetter. *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*. Accessed: October 14, 2023. 2016. URL: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[24] Kristen E. Eichensehr. "Ukraine, Cyberattacks, and the Lessons for International Law". In: *AJIL Unbound* 116 (2022), pp. 145–149. DOI: 10.1017/aju.2022.20.

[25] Aandy Greenberg. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History". In: *Wired* (2018).

[26] *CENTRE FOR DIGITAL FORENSICS AND CYBER SECURITY*. Accessed: April 20, 2024. 2024. URL: https://taltech.ee/en/centre-for-digital-forensics-cyber-security/people.

[27] Toomas Lepik. CV at the Estonian Research Information System. Accessed: April 20, 2024. 2024. URL: https://www.etis.ee/CV/Toomas_Lepik_001/est/.

[28] Rain Ottis. CV at the Estonian Research Information System. Accessed: April 20, 2024. 2024. URL: https://www.etis.ee/CV/Rain_Ottis/eng/.

[29] *CERT-EE Wayback Machine*. Accessed: April 20, 2024. 2007. URL: https://web.archive.org/web/20070105145302/http://www.cert.ee/.

[30] Personal Profile at LinkedIn.com. Accessed: April 20, 2024. URL: https://www.linkedin.com/in/hillarpoldmaa/?originalSubdomain=ee.

Appendix 1 – Non-Exclusive License for Reproduction and Publication of a Graduation Thesis[1]

I Helena Jäe

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "The evolution of cyber conflict on the example of Estonia, Georgia and Ukraine", supervised by Kaido Kikkas
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

12.05.2024

[1]The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 - Interview questions

[RQ1] To what extent have cyber attacks evolved in terms of tactics, scale, and state-sponsored involvement since 2007, with a specific focus on the events in Estonia (2007), Ukraine (2014 & 2022), and Georgia (2008)?

1. What are the signs (if any) that a cyber conflict may begin?
2. If we compare 2007 and 2022, how have the first weeks before the cyber conflict changed?
3. How to recognise that a cyber conflict may further turn into a kinetic conflict/war?
4. What are the main differences when comparing Estonia 2007 and Georgia 2008? What about the similarities?
5. If you look at Estonia 2007 and Ukraine 2022, what are the main differences? Similarities?
6. What role does social media play in these conflicts?

[RQ2] What lessons can be drawn from the cyber attacks on Ukraine's infrastructure since 2022?

1. What were the signs before/when the cyber attacks on Ukrainian infrastructure started?
2. What could Ukraine have done better in its cyber operations before the war in 2014 to minimise the impact on its infrastructure?
3. How to best prepare for the cyber conflict? What are the key takeaways? On example of Ukraine

[RQ3] What can we expect from cyber attacks in the future, and how best to prepare for them?

1. What can be expected from the current Ukrainian 2022 cyber conflict? What other cyber attacks could Ukraine experience?
2. As we see that the attacks have increased towards ordinary citizens, will future cyber conflicts have ordinary citizens as a priority target? (For example, hospital attacks in Ukraine)
3. As cyber becomes more and more discussed, how might this affect cyber attacks?
4. What will be the role of state-sponsored attacks in future cyber conflict?