

Magnus Sandem Dhelie
Carl Dennis Flåte
Lars Magnus Lie
Erki Sulg

Methods Used in Cyberattacks in the War Between Russia & Ukraine

Bachelor's thesis in Digital Infrastructure and Cybersecurity
Supervisor: Erjon Zoto
May 2023

Magnus Sandem Dhelie
Carl Dennis Flåte
Lars Magnus Lie
Erki Sulg

Methods Used in Cyberattacks in the War Between Russia & Ukraine

Bachelor's thesis in Digital Infrastructure and Cybersecurity
Supervisor: Erjon Zoto
May 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology



Abstract

Title: Methods Used in Cyberattacks in the War Between Russia & Ukraine
Date: 22.05.2023
Authors: Magnus S. Dhelie
Carl D. Flåte
Lars M. Lie
Erki Sulg

Supervisor: Erjon Zoto
Client: Raymond Hagen – Norwegian Digitalisation Agency
Keywords: Cyberattacks, methods, analysis, Russia, Ukraine, war
Pages: 87
Appendix: 5
Availability: Open

Abstract:

In this Bachelor's thesis, the group has examined the methods used for cyberwarfare in the Russo-Ukrainian war, which has been ongoing since February 24th 2022. The scope of the thesis covered one year, from February 1st 2022, to February 1st 2023. The study was conducted in the form of a literature review with the aim of providing an overview and analysis on cyberattacks in modern warfare.

The group used open-source information to investigate registered cyberattacks and their methods used. All of these attacks were then categorised into one of the following methods: cognitive, destructive, disruptive, or reconnaissance.

While it has been difficult to gauge the impact of cyberattacks in this war, they have still played their part. Communications and information channels have been affected by disruptive attacks, and destructive attacks have rendered data useless to their owners. Additionally, we have observed that cognitive operations spread disinformation and confusion, while reconnaissance has been used to gain information on capabilities and weaknesses.

Sammendrag

Tittel:	Methods Used in Cyberattacks in the War Between Russia & Ukraine
Dato:	22.05.2023
Deltakere:	Magnus S. Dhelie Carl D. Flåte Lars M. Lie Erki Sulg
Veileder:	Erjon Zoto
Oppdragsgiver:	Raymond Hagen – Digitaliseringsdirektoratet
Nøkkelord:	Cyberangrep, metoder, analyse, Russland, Ukraina, krig
Antall sider:	87
Antall vedlegg:	5
Tilgjengelighet:	Åpen

Sammendrag:

I denne bachelor-oppgaven har gruppen tatt for seg hvilke metoder som har blitt brukt til cyberkrigføring i Russland-Ukraina krigen som har pågått siden 24. Februar 2022. Omfanget til oppgaven var ett år, fra 1. Februar 2022 til 1. Februar 2023. Oppgaven har vært utført i form av en litteraturstudie med mål om å gi en oversikt og analyse av cyberangrep i moderne krigføring.

Gruppen har brukt offentlig tilgjengelig informasjon til å undersøke registrerte cyberangrep og metoder brukt i disse. Alle disse angrepene ble deretter kategorisert i en av følgende metoder: kognitiv, destruktiv, disruptiv, eller rekognisering.

Selv om det har vært vanskelig å måle virkningen av cyberangrep i denne krigen, har de fortsatt spilt sin rolle. Kommunikasjons- og informasjonskanaler har blitt påvirket av disruptive angrep, og destruktive angrep har gjort data ubrukelige for sine eiere. I tillegg har vi observert at kognitive operasjoner sprer desinformasjon og forvirring, mens rekognosering har blitt brukt for å få informasjon om evner og svakheter.

Preface

This project marks the end of a three year Bachelor's program within Digital Infrastructure and Cybersecurity at NTNU. These past years have provided us with troves of useful and relevant information, that is constantly growing in importance in today's intricately connected society. Working on this thesis has also given us a greater understanding on the current cyberthreat landscape, and the importance of our knowledge in the field of cybersecurity.

We would like to express our thanks towards all who helped us complete our thesis. During this project period we have been presented with a trove of new information and ideas that have helped us form our product.

In addition to all the research that has been done, it would not have been possible to complete this task without the help, and instrumental guidance, from our project supervisor, Erjon Zoto.

Finally, we wish to express our gratitude towards our client, Raymond Hagen at the Norwegian Digitalisation Agency (Digitaliseringsdirektoratet). He has at all times during the project period been available for questions and guidance. Hagen has expressed a positively motivating amount of interest towards our work, and has been instrumental in securing the level of quality we wished for our thesis.

To the reader, we hope that this thesis provides you with useful information and that it can serve as stepping stone towards more in-depth studies in relevant fields.

Magnus Sandem Dhelie, Carl Dennis Flåte, Lars Magnus Lie, Erki Sulg

Gjøvik, spring 2023

Contents

Abstract	iii
Sammendrag	v
Preface	vii
Contents	ix
Figures	xiii
Tables	xv
Acronyms	xvii
Glossary	xix
1 Introduction	1
1.1 Project Background	1
1.2 Problem Definition	2
1.3 Problem Statement	2
1.3.1 Research Questions	2
1.4 Project Goals	3
1.5 Limitations	3
1.6 Target Audience	4
1.7 Task Description	4
1.8 Project Group	5
1.9 Organisation & Framework	6
1.10 Work Method	6
1.11 Thesis Structure	7
2 Background of the Russo-Ukrainian War	9
2.1 Introduction	9
2.2 Historical Background	9
2.2.1 Fall of the Soviet Union	9
2.2.2 Euromaidan	10
2.2.3 Annexation of Crimea	11
2.2.4 Russo-Ukrainian war	11
2.3 Political Background	12
2.3.1 Ukrainian Politics	12
2.3.2 Russian Politics	12
2.3.3 International Politics	13
2.4 Technological Background	14
2.5 Understanding threat actors	16

2.5.1	Advanced Persistent Threats	16
2.5.2	Hackivism and simple threats	18
2.6	Attack Type Categorisation	19
2.6.1	Attack type explanation: Cognitive	19
2.6.2	Attack type explanation: Destructive	20
2.6.3	Attack type explanation: Disruptive	20
2.6.4	Attack type explanation: Reconnaissance	20
2.7	Examining significance of cyberattack methods	21
2.8	NotPetya, Cyberwarfare, and NATO	22
2.9	War in Donbas (2014-2022) Timeline	23
2.9.1	Aftermath	24
3	Method	25
3.1	Introduction	25
3.2	Research Design	25
3.3	Data Collection	26
3.3.1	Web search	26
3.3.2	ChatGPT	27
3.3.3	Social media	28
3.3.4	Lecture	28
3.3.5	Correspondence	28
3.4	Data Analysis	29
3.5	Ethical Considerations	29
3.6	Validity and reliability	29
4	Main Timeline	31
4.1	Full-scale invasion cyber-timeline	32
4.2	Quarterwise overview	34
4.2.1	Quarter 1	34
4.2.2	Quarter 2	35
4.2.3	Quarter 3	36
4.2.4	Quarter 4	36
4.2.5	2023 – Quarter 1	37
5	Analysis of Cyberattacks in the Russo-Ukrainian War	39
5.1	Introduction	39
5.2	Attack overview	40
5.2.1	2022 Q1	40
5.2.2	2022 Q2	43
5.2.3	2022 Q3	44
5.2.4	2022 Q4	47
5.2.5	2023 Q1	49
6	General Findings	51
6.1	Introduction	51
6.2	Methods used in the documented cyberattacks	52
6.2.1	Introduction	52
6.2.2	Cognitive warfare	54

6.2.3	Destructive	55
6.2.4	Disruptive	56
6.2.5	Reconnaissance	57
6.3	Attribution	59
6.4	Impact of cyberattacks	61
6.4.1	Battlefield impact	63
6.5	Discussing the results	64
7	Discussion	65
7.1	Reflection on the thesis	65
7.1.1	Thesis choice	65
7.1.2	Assessment of project strengths and weaknesses	66
7.2	Process and methods	67
7.2.1	Project process	67
7.2.2	Decisions and choices	68
7.3	Interpersonal cooperation	70
7.3.1	Teamwork	70
7.3.2	Collaboration with client	70
7.3.3	Supervision	71
7.4	Outcome	72
7.4.1	Possible improvement	72
7.4.2	Academic contribution of our work	72
7.4.3	Updated Gantt-chart	73
7.4.4	Time analysis	74
7.5	Further work	76
8	Conclusion	77
	Bibliography	79
A	Additional data	89
A.1	Numerical data for graphs	90
A.2	Toggl summary report	91
B	Standard agreement on thesis – NTNU	93
C	Project plan	101
D	Meeting minutes	135

Figures

2.1	Russian Threat Actor Attribution	15
3.1	Example image of ChatGPT use.	27
4.1	Screenshot from the Zelenskyy deepfake [76].	34
6.1	Attacks per month between Feb 2022 - Feb 2023 [45] [78]	53
6.2	Cognitive attacks per month between Feb 2022 - Feb 2023 [78]	54
6.3	Destructive attacks per month between Feb 2022 - Feb 2023 [45] [78]	55
6.4	Disruptive attacks per month between Feb 2022 - Feb 2023 [78]	56
7.1	Updated Gantt-chart	73

Tables

1.1	Project goals	3
2.1	The 7 steps of the Cyber Kill Chain® developed by Lockheed Martin [37]	17
2.2	Attack types	19
5.1	WhisperGate campaign	41
5.2	HermeticWiper campaign	41
5.3	Zelenskyy deepfake	42
5.4	Industroyer2	43
5.5	CaddyWiper	43
5.6	IRIDIUM coordinated hybrid attack	44
5.7	KRYPTON (Turla) Android Malware	45
5.8	EnergoAtom website hack	45
5.9	Anonymous Moscow traffic jam	46
5.10	Prestige ransomware attack	47
5.11	Gamaredon phishing campaign	48
5.12	UNC4166 Trojanised Windows 10 installers	48
6.1	Quarterly attacks by attack type	53
6.2	Known Threat Actor Overview	59
6.3	Known Hactivist Overview	60

Acronyms

APT Advanced Persistent Threat. 14, 36, 63, 64

BBC British Broadcasting Corporation. 29

CISA The United States Cybersecurity and Infrastructure Security Agency. 14, 32

DDoS Distributed Denial-of-Service. 18–21, 56, 61

DIGDIR Norwegian Digitalisation Agency. 5

EU European Union. 12, 13

FSB Federal Security Service of the Russian Federation. 14

GRU Main Directorate of the General Staff of the Armed Forces of the Russian Federation. 14, 22, 23, 58

HUMINT Human Intelligence. 57, 58

IMRaD Introduction – Method – Results – and – Discussion. 6

KGB Committee for State Security of the USSR. 14

MSTIC Microsoft Security Threat Intelligence Center. 41

NATO North Atlantic Treaty Organization. 11, 13, 22

NTNU Norwegian University of Science and Technology. 5, 65, 68, 70, 74

OSINT Open-Source Intelligence. 57, 58

OT Operational Technology. 21, 55

QRA Quick Reaction Alert. 57

SIGINT Signals Intelligence. 57, 58

SSSCIP Ukrainian State Service of Special Communications and Information Protection of Ukraine. 32

SVR Foreign Intelligence Service of the Russian Federation. 14

Glossary

advanced persistent threat "An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives which are typically to establish and extend its presence within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives." [1]. 16

grey literature "Grey literature is any information that is not produced by commercial publishers." [2]. 25

hacktivism A word derived from the combination of 'hack' and 'activism'. Hacktivism is the act of hacking, or breaking into a computer system, for politically or socially motivated purposes.[3]. 18

human intelligence "Human intelligence is derived from human sources. To the public, HUMINT remains synonymous with espionage and clandestine activities; however, most of HUMINT collection is performed by overt collectors such as strategic debriefers and military attaches." [4]. 57

malware "Malware (short for "malicious software") is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants." [5]. 14, 17, 22, 23, 32, 35

open-source intelligence "Open-Source Intelligence is publicly available information appearing in print or electronic form including radio, television, newspapers, journals, the Internet, commercial databases, and videos, graphics, and drawings." [4]. 57

phishing A form of social engineering attack designed to deceive targets into revealing sensitive information or installing malware such as ransomware.[6]. 23

signals intelligence "Signals intelligence is derived from signal intercepts comprising – however transmitted – either individually or in combination: all communications intelligence (COMINT), electronic intelligence (ELINT) and foreign instrumentation signals intelligence (FISINT)." [4]. 57

Chapter 1

Introduction

This chapter provides the necessary background information for the project. It presents the problem definition and statement which we have constructed. We also outline the project goals that we have set for ourselves. Furthermore, we discuss the limitations that we have encountered and the framework we have used to structure the task.

1.1 Project Background

The Russo-Ukrainian conflict is the first major conflict involving large-scale cyber operations [7]. The previous statement serves as the premises for this project. Additionally, the fact that this conflict is still on-going at the time of writing makes the study more relevant.

For the first time we are able to witness large-scale cyber operations between two nation states. One can also see how cyber operations are carried out in tandem with military operations "on the ground". Furthermore, we have had the opportunity to assess the impact of cyberattacks on a variety of targets.

Russia and Ukraine have had a strained relationship since the fall of the Soviet Union in 1991. Even before those historic events, there were multiple wars fought in the Ukrainian area by the Russian Empire, which sought control of the region. During the 1800s, the Russian Empire sought to perform 'russification' of the people living in this area. [8](3.3.4)

The modern, and weaponized, part of this long-standing conflict began in 2014 with the Russian annexation of the Crimean peninsula [9], and escalated to a full scale invasion of Ukraine in February 2022 [10].

1.2 Problem Definition

The Russo-Ukrainian war has been the first major conflict with active use of cyberwarfare, featuring numerous cyberattacks on all sides. This has in turn highlighted the importance of studying cyberattack methods used in modern cyberwarfare. Threat intelligence has therefore become a critical practice in the cybersecurity field, allowing security experts to stay up-to-date on the latest vulnerabilities, exploits, and threat actors. Without a proper threat intelligence practice every new threat scenario would require starting research from scratch.

This study aims to present an open-source threat intelligence practice for researching information on cyberattacks in a present-day threat scenario. Through collecting and presenting this information in a concise and accurate manner, readers can gain a comprehensive overview of modern cyberattack methods used in this war.

We aim to provide an in-depth understanding of the practices and methods used by nation state-sponsored threat actors and threat actors involved in an active cyberwar. Understanding these practices and methods is important when it comes to developing effective cyber defense strategies and will help in preventing future attacks. Our goal is that this analysis of the cyberattack methods used in the Russo-Ukrainian war can further contribute to the broader literature on cyberwarfare.

1.3 Problem Statement

This Bachelor's thesis will address the following problem statement:

"What methods have been used in cyberattacks between the main actors in the Russo-Ukrainian war?"

1.3.1 Research Questions

In this thesis we will attempt to answer the following research questions.

- What methods have been used in documented cyberattacks in the Russo-Ukrainian war?
- Can any of the documented attacks be attributed to known threat actors? If so, which?
- Has there been any significant impact from any cyberattacks performed in the war? If so, which attacks and why?
 - Additionally, have these attacks made any significant impact on the battlefield, or is the impact solely limited to communications- and other critical-infrastructure?

1.4 Project Goals

The project goals which we have outlined for this project are divided into three categories:

Effect goal	Deliver a completed thesis which can be effectively used by the client for their doctorate research. It should also be of use to other academics and interested parties.
Result goal	Deliver a thesis which will be of great quality.
Learning goals	Gain valuable experience in researching a topic, researching threat intelligence and presenting our findings. We want to better understand the role of cyberattacks in an ongoing war as well as the impact which cyberattacks have on a conflict. We also aim to fulfill the goals described in the Bachelor's thesis course description for our study program.

Table 1.1: Project goals

Our aim is to complete the project goals with our best efforts, as this will provide us with a solid learning outcome from the study program.

1.5 Limitations

Although our task involves a conflict that has been ongoing for many years, we have decided to limit ourselves to a one-year scope. This scope covers the period from the 1st of February 2022 through the 1st of February 2023, (2022-02-01 through 2023-02-01) providing us the possibility of mentioning a variety of incidents. This limitation was chosen since it covers a brief period before the war, and spanning nearly a year after its start. However, this period can have a few exceptions in the case of highly relevant events.

Ensuring the accuracy of our sources has been a high-priority task during our research period. To achieve this, we have only included events which are supported by multiple sources or reliable primary sources. This will minimise the inclusion of non-real events which may have been reported from biased sources attempting to spread misinformation.

As this is an ongoing conflict, we recognise that there is potential for biased reporting from some sources. To counter this, we have attempted to present the events themselves objectively so that we can provide a clear view of the cyberattacks which have been performed. However, we acknowledge that in some cases we have had to rely on assumptions, particularly when discussing attribution, motivation, and effect of the attacks. These assumptions are based on our collective

knowledge of cyberattacks, and may not be completely accurate, but they provide insights into the potential motivation behind attacks and the impact which an attack may have had. The sources are primarily written in either Norwegian or English, but the handful of sources that are written in Ukrainian have been translated before use in this product.

1.6 Target Audience

The client has expressed their intentions to use the results of this project for further research about nation-state funded threat groups. Therefore, it is of significant importance for us to provide easily accessible and understandable referencing for the client in order to avoid any misunderstandings.

As our client has knowledge around cybersecurity and has a technical background, we decided to aim for similar people to be the target group of this report. This means that our main target group consists of people with relevant technical knowledge with an interest in cybersecurity and cyberwarfare. Simultaneously, readers without much familiarity with the topic will, with a sufficient interest in the conflict, also benefit from this study and therefore be included as secondary targets.

1.7 Task Description

Our group has been tasked with researching the cyberdomain of the ongoing war in Ukraine. The research is to focus on the methods used in cyberattacks perpetrated by the major combatants; Russia and Ukraine. The end product is to provide a clear overview of known attacks, complete with methods, consequences and attribution if possible.

The product produced by our group should be well researched, unbiased, and written in a way that the information provided is portrayed clearly and concisely. In addition to that, it is imperative that our end product is of such a quality that it provides itself as useful primarily towards our client, but also towards other researchers and interested parties with an academic interest towards the topic.

At first we have to undertake a period of pure research into the matter at hand. Due to the nature of the conflict, especially with regards to how recent it is, means that there are less sources rooted in academia than for other topics. We need to base our research off of reports from reputable actors in the fields of technology, armed forces and intelligence, technical data, and other open-source information.

When we have accrued satisfactory amounts of information and filtered that for what is truly useful for this project, we have to begin writing our thesis. By piecing together our research we should be able to provide the client with a product that

fulfils their criteria, as well as performing well under scrutiny by the university. Receiving constructive feedback from the client, and our supervisor, on a regular basis should also help towards achieving our goals of a good product.

1.8 Project Group

The project owner is the Norwegian Digitalisation Agency (Digitaliseringsdirektoratet) hereafter referred to as DIGDIR, the Norwegian abbreviation for the agency. Our contact person at DIGDIR is Raymond Hagen, who is referred to as our client in this text. His role is to define our task, answer questions and help us with any requests relating to the project which we might have. Erjon Zoto, university lecturer at the Norwegian University of Science and Technology (NTNU), is the supervisor for this Bachelor's thesis.

The group is on their third and final year of taking a Bachelor's degree in Digital Infrastructure and Cybersecurity at NTNU's campus in Gjøvik. The group consists of Carl Dennis Flåte, Erki Sulg, Lars Magnus Lie and Magnus Sandem Dhelie. Throughout the Bachelor's degree the group members have gained knowledge in several relevant subjects relating to this project. Some relevant experiences for this task are subjects such as Risk Management, Introduction to Incident Response, Malware Analysis, Ethical Hacking, and Cybersecurity & Teamwork. Additionally, Flåte has worked in the Royal Norwegian Navy at the Norwegian Joint Headquarters, and brings valuable military knowledge and experience to the group. Dhelie has also achieved relevant knowledge and skills through his work as a Security Analyst for mnemonic during his studies.

1.9 Organisation & Framework

The report is written in English due to an overwhelming majority of the source material being written in English, and our client has stated that it is their preferred language for the product.

The report is written in Overleaf which is a LaTeX co-writing platform. All of our meetings have been held through Microsoft Teams as long as a physical meeting was not planned. The project shall be completed by the delivery date of 2023-05-22.

As our project is foremost a literary study we have chosen to follow the IMRaD-model. This format suits our needs and allows for a logical, well-structured thesis. The IMRaD-model is also the most prominent format used when doing original research and writing scientific journals [11] which solidifies our choice of model.

1.10 Work Method

The project is divided into two main phases. The first phase is the research phase where we find as many sources as possible related to the project statement and related questions. When this phase is finished we analyse the data we have gathered and start writing the report. The phases are sequential, so the first phase should be completed before work can truly start on the second phase. During each phase the work is done parallel by each group member doing their own research and writing.

1.11 Thesis Structure

- **Chapter 1 - Introduction:** Describes the background of the thesis, description of the task, project goals, scope, limitations, target audience, and information on the group and our work methods.
- **Chapter 2 - Background of the Russo-Ukrainian War:** Describes the historical and political background, from the fall of the Soviet Union to the outbreak of war between the nations, and also explores the various threat actors involved in the cyberwar. The chapter ends with a timeline of the most notable events of the war in Donbas.
- **Chapter 3 - Method:** Describes our methods of research, data collection and data analysis. It also goes describes our ethical considerations and how we validated our research.
- **Chapter 4 - Main Timeline:** Contains the timeline of the most notable events in the Russo-Ukrainian war.
- **Chapter 5 - Analysis of Cyberattacks in the Russo-Ukrainian War:** Describes in detail certain chosen cyberattacks from each quarter.
- **Chapter 6 - General Findings:** Describes the results of our research, shows the usage of each category of cyberattacks, and provides answers to the research questions.
- **Chapter 7 - Discussion:** Describes and discusses our process, decisions and the outcome of the thesis.
- **Chapter 8 - Conclusion:** Describes what we learned from our work and our conclusion.
- **Appendix:** Files and documents relevant to the thesis.

This structure aims to provide a reader with fundamental background information right after the introduction, with the aim of ensuring a minimum level of understanding before being presented with more in-depth information.

Thereafter, our methods are presented to explain how information has been obtained and worked with. Following that are three chapters of findings, with the timeline being shown first to set the perspective, succeeded by the analysis and general findings – including answers to our research questions.

In chapter 7 we discuss our work on the thesis, including an assessment of pros and cons, working process, outcome, and if the original plan was followed.

Finally, we present our conclusion, which covers our findings and delivers our final answer to the thesis problem.

Additionally, we have appended several important files relevant to the project, such as agreements & contracts, and raw data used in statistics.

Chapter 2

Background of the Russo-Ukrainian War

2.1 Introduction

In this chapter, we will take a peek into the origins and progression of the Russo-Ukrainian war, as well as point out some of the underlying historical and political factors that have contributed to the current state of affairs. We will also take a look at Russia's technological background regarding their cyber-operative capabilities and connections to intelligence agencies.

2.2 Historical Background

In this section we will provide important historical background to the war we see today. Even though the conflict between these nations has been an issue for hundreds of years [8], this thesis will focus on the modern side of it. Therefore, this section will touch upon key events, from the collapse of the Soviet Union to the invasion in 2022. Furthermore, the section will take a look at the relationship between the two nations, Russia & Ukraine, and how it has played into the situation at hand.

2.2.1 Fall of the Soviet Union

The fall of the Soviet Union was a pivotal moment in world history that marked the end of the Cold War and the collapse of the socialist state that had existed for nearly 70 years. The fall of the Soviet Union began in the 1980s, a time of economic stagnation and political turmoil, and was driven by a combination of internal and external factors [12].

Mikhail Gorbachev, who became the Soviet leader in 1985, implemented a series of reforms aimed at modernizing the Soviet economy and political system, in-

cluding glasnost and perestroika, Russian for "openness" and "restructuring" [13]. However, these reforms ultimately led to the unraveling of the Soviet Union, as they gave rise to nationalist movements in the various republics, including Ukraine. These movements sought greater autonomy or even independence from Moscow, leading to tensions between the republics and the central government.

The fall of the Soviet Union culminated in December 1991, when the leaders of Russia, Ukraine, and Belarus signed the Belavezha Accords, which dissolved the Soviet Union and established the Commonwealth of Independent States (CIS) in its place [12].

2.2.2 Euromaidan

The Euromaidan revolution, also known as the Ukrainian Revolution of 2014, was a series of protests and demonstrations that began in November 2013 in response to then-President Viktor Yanukovich's decision to back away from signing an association agreement with the European Union in favor of closer ties with Russia. The protests, which took place in the capital city of Kiev's Independence Square, became increasingly violent and culminated in Yanukovich's ousting in February 2014 [14].

The protests were led by pro-European activists and opposition politicians who believed that Yanukovich's decision to reject the association agreement represented a betrayal of Ukraine's aspirations for closer ties with the West. The protests were met with violent crackdowns by the government, leading to scores of deaths and injuries [14].

The Euromaidan revolution had far-reaching consequences for Ukraine, including the annexation of Crimea by Russia and the ongoing conflict in eastern Ukraine between Ukrainian government forces and Russian-backed separatists [14].

2.2.3 Annexation of Crimea

The annexation of Crimea in 2014 refers to the Russian Federation's takeover of the Crimean Peninsula, which was then part of Ukraine. The annexation followed the Euromaidan revolution in Ukraine, which led to the ousting of then-President Viktor Yanukovich and a shift towards closer ties with the West. Russian President Vladimir Putin claimed that the annexation was necessary to protect Russian interests and ethnic Russians living in Crimea [15].

The annexation was met with widespread international condemnation and sanctions against Russia. The United Nations General Assembly passed a resolution condemning the annexation, with 100 nations voting in favor and 11 against [16]. The European Union and the United States also imposed economic sanctions on Russia in response to the annexation.

The annexation of Crimea has had significant consequences for Ukraine and Russia. The conflict has resulted in thousands of deaths and displacement of civilians [15].

2.2.4 Russo-Ukrainian war

As tensions between the two nations grew, the Russian military was eventually ordered to launch a full-scale invasion into Ukraine on the 24th of February 2022 [10]. The invasion was met with resistance from Ukrainian forces [17], leading to a brutal war that is still ongoing as of May 2023. Throughout the war, Ukraine has received military aid from NATO, including the United States [18] and several European countries [19] in form of supplies such as weapons, ammunition and training for their troops [20]. Despite receiving aid from other countries, the war has taken a heavy toll on the Ukrainian people with thousands being killed and millions being displaced from their homes, especially in the early stages of the war [15].

2.3 Political Background

In this section we aim to provide context to the war by providing political background information, including key players, their motivations and strategies. This section will touch upon the political and economic factors that contributed to the war as we know it, including issues such as identity, nationalism, and sovereignty.

2.3.1 Ukrainian Politics

In November 2013 the sitting president Viktor Yanukovich stopped talks with the European Union (EU), and accepted a bailout deal from Russia. This showed that he was trying to drag Ukraine politically closer to Russia instead of the EU and the West. This event sparked protests in Kiev that was the start of "The Revolution of Dignity". The revolution ended in the Euromaidan victory and severed ties with Russia and brought Ukraine on a path to join the EU [21].

2.3.2 Russian Politics

In president Vladimir Putin's speech given before the Russian invasion, he states that the post-2014, democratically elected Ukrainian government is neo-nazi. He then tries to draw several conclusions to back up these claims [22]. Putin stated that the goal of the Russian "special operation" is to demilitarise and "de-nazify" Ukraine, as well as protect all ethnic Russians inside Ukraine's borders [17]. In his 2021 essay published by the Kremlin, Putin asserts that the Ukrainian and Russian populations are a unified people, and have the same culture and history [23] [24] [25].

2.3.3 International Politics

Negotiations for the association agreement between Ukraine and the EU were launched already in 2007. This agreement is the main tool for bringing Ukraine and the EU, and therefore the West, closer together. The agreement promotes political ties, economic links and common values. The economic part of the agreement is the Deep and Comprehensive Free Trade Area (DCFTA) providing a framework for modernising Ukraine's economy and trade [19].

As previously mentioned, it was the refusal to sign this agreement in 2013 which sparked the Euromaidan revolution, that again led to the ousting of former president Yanukovich. The agreement was signed in 2014. With this agreement the EU and Ukraine have held several association councils reviewing the monitoring & implementation of said agreement [19].

All of this, combined with Russia's increased aggression, led to the EU providing Ukraine candidate status on the 23rd of June 2022 [19], further solidifying Ukraine's migration towards the West and away from Russian influence.

The political shift that Ukraine has experienced the past decades has also led to warmer relations with the United States of America. This has also encouraged increased trade relation between the two nations. The United States have been a leading factor in securing international support for Ukraine after the events of 2014, including supporting enhanced engagement between Ukraine and NATO [18].

The North Atlantic Treaty Organization, on their part, have stated that an independent Ukraine is vital for European stability, and have formally condemned Russia's illegal annexations of Ukrainian territory. They have backed up this statement by providing vital military support in the form of materials, training for Ukrainian troops, and more since 2014. Since 2016, NATO's measures in support of Ukraine have been a part of the Comprehensive Assistance Package (CAP). This package is designed to help Ukraine provide for its own security by employing various NATO standards and other best-practices. Part of this package is the NATO-Ukraine Platform on Countering Hybrid Warfare, which covers activities such as cyber attacks and disinformation campaigns [20].

In a stance mirroring that of the EU, US, and NATO, the United Nations have also condemned Russia's war of aggression in Ukraine. The United Nations sees the invasion as a violation of Ukraine's territorial integrity and sovereignty. Additionally, they have opened investigations towards reported human rights violations and war crimes in the region, while continuously calling for a peaceful resolution, though Russia's vetoing power has made this difficult [26].

2.4 Technological Background

Russia is known to have some of the world's most proficient cyber threat actors due to the investment of the Russian government into this field [27]. Many of these threat actors are nation-state sponsored providing them with access to both physical equipment and economic resources. Access to these resources allow the threat actors to act with increased efficiency and effectiveness.

The notorious 2014 *BlackEnergy* malware, which caused blackouts in several Ukrainian regions, has been attributed to Russian state-sponsored actors [28]. Similarly, the 2017 *NotPetya* ransomware attacks are also attributed to Russian actors, with sources attributing the attacks to the Sandworm group [29][30], who are believed to be associated with the Russian GRU [30].

Russian state-sponsored threat actors are all subject to at least one of the three operative intelligence agencies of the Russian Federation, where all but the GRU are successor agencies to the USSR's KGB. These three agencies operate in different areas and domains, often without cooperating, and sometimes unaware of each other's operations and goals [31].

Domestic operations are, in most cases, handled by the FSB who are responsible for counterintelligence, anti-terrorism, and surveillance of the Russian armed forces. Though primarily operating on Russian soil and against domestic targets, the FSB does at times conduct intelligence activities abroad together with the SVR [32] and has seen an increase in international operations during Putin's presidency [31].

As the FSB operates domestically, so does the SVR internationally by being tasked with intelligence and espionage activities outside of Russia. The SVR is active in perpetrating offensive APT-activity towards other nations, and continuously seek intelligence through cyber exploitation. CISA states that the SVR primarily focuses on "government networks, think tank and policy analysis organisations, and information technology companies" [33].

Unlike the FSB and SVR, the GRU does not fall under direct jurisdiction of the President of Russia, but is instead subject to Russian Military Command. The GRU is tasked with responsibility for all levels of military intelligence, from tactical to strategic [34]. The GRU routinely conducts cyberoperations towards international targets, including reconnaissance, disinformation & propaganda, and full-on attacks. These operations are often of a bold and aggressive nature, leading to the agency and its threat actors being attributed to attacks such as *NotPetya* in 2017 [34].

The advanced threat actors we see in play in this war all have ties to these intelligence agencies. Their participation in large scale cyberoperations can be due to these agencies perceiving any detriment to the West being a gain for Russia [31]. In their eagerness to advance Russian interests, these agencies will deploy all their capabilities to their full capacity.

The following figure 2.1 presents known threat actors and their alleged affiliation to Russian intelligence agencies.

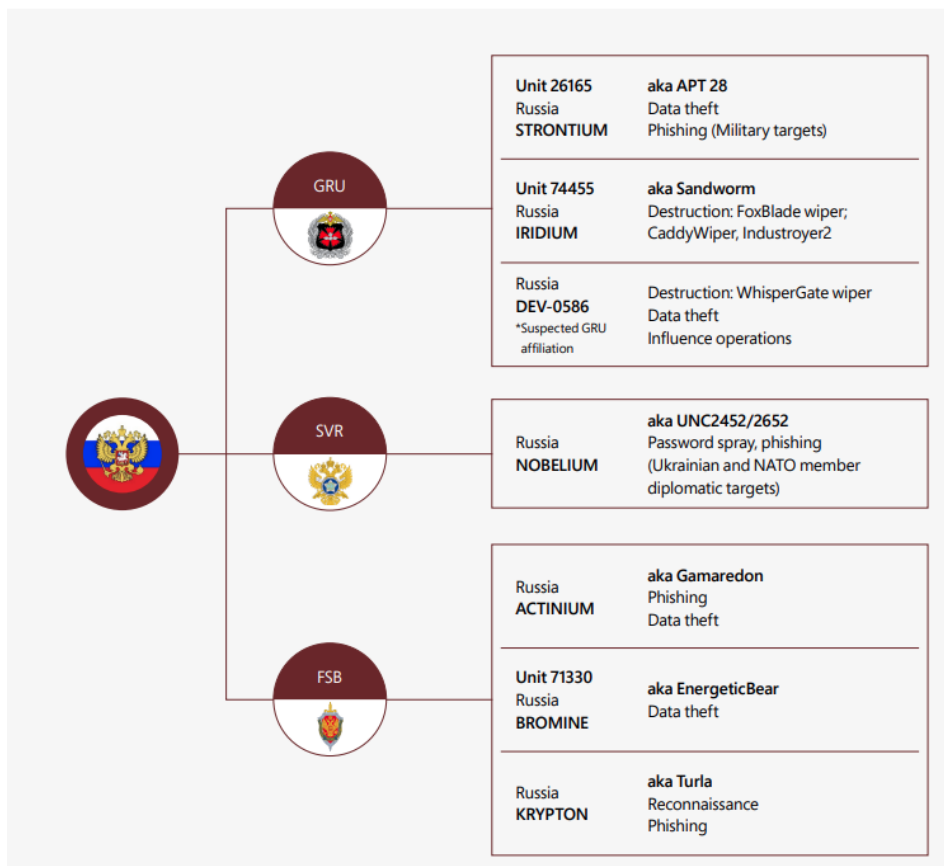


Figure 2.1: Russian Threat Actor Attribution
Source: Microsoft "Special Report: Ukraine" [35]

Across the border, Ukraine has been a target for Russian threat actors since the conflict arose in late 2013. The constant pressure of being the primary target has led to Ukraine significantly increasing their defensive capabilities to prevent incoming attacks. However, they are not impervious and Ukraine has been experiencing a drastic increase in attacks leading up to the commencement of the invasion and during the war itself [36].

Due to the pressure and resource demanding nature of defending against cyberattacks, one might presume that it is the leading reason for the low amount of organised offensive cyberoperations from Ukraine's side.

2.5 Understanding threat actors

2.5.1 Advanced Persistent Threats

Performing a serious, impactful, cyberattack requires significant planning. First, an attacker must decide on a specific target, which could be anyone or anything. However, state-sponsored attackers often have a particular mission that requires them to target specific companies or sectors in a specified country. A relevant example is pro-Russian attackers which are currently targeting companies and organisations in Ukraine as part of the war effort.

Before analysing the methods used in a cyberattack, it is essential to understand the process from the attacker's point of view. A common model used to describe the steps which an attacker must take is the "cyber kill chain". One widely used cyber kill chain model is Lockheed Martin's Cyber Kill Chain® [37]. For a more comprehensive model, the Unified Kill Chain model [38] can be referenced.

The purpose of the cyber kill chain is to defend against cyberattacks carried out by advanced persistent threats. The model allows for organisations to implement defenses and solutions with the intent to "break" the kill chain and stopping the attack.

The following page contains an overview and explanation of the steps in the kill chain.

1. Reconnaissance	This step sees the attacker selecting a target and performing reconnaissance to gather information about the target. This information is used to identify vulnerabilities in the target network.
2. Weaponisation	The attacker creates a malware which exploits the identified vulnerabilities. This malware is often a virus or a worm depending on their purpose.
3. Delivery	The attacker has to deliver the weapon to the target. This can be done in multiple ways such as digitally through email-attachments or malicious software bundles. The attacker can also choose to physically deliver the malware through a device such as a USB drive.
4. Exploitation	The malware triggers and the vulnerability is exploited on the target network. This may be the first step where the attack is detected in the network. Software and hardware may cease functions and the network experiences disruptions.
5. Installation	The attacker attempts to gain access to the network remotely. This step is accomplished through the installation of a "backdoor", an access point into the network which the attacker can use.
6. Command and Control (C2)	The attacker has hands-on access to the target network. The attacker is able to gain persistent access to the target network.
7. Actions on Objective	This step is where the attacker has access to the network and is taking actions to achieve the goals they set out to accomplish with the attack. This may be data exfiltration, data destruction or encryption.

Table 2.1: The 7 steps of the Cyber Kill Chain® developed by Lockheed Martin [37]

2.5.2 Hactivism and simple threats

On the other side of cyber actors, there are the simpler threats and hactivism. Check Point describes hactivism as "[...]the act of hacking, or breaking into a computer system, for politically or socially motivated purposes." [3]. These threat actors perform less sophisticated attacks and are often unorganized, small groups. They claim responsibility for disruptive attacks, such as Distributed Denial-of-Service attacks. Furthermore, they are also active in the spread of misinformation on social media platforms [39].

However, these threats should not be underestimated as they are described to "currently create the highest 'noise' in the cyberspace around the conflict, but not always the highest damage" [39]. The reason for this is that in today's world, social media pressure is constantly present which enables certain groups to rapidly and efficiently disseminate their own agenda, or make claims and statements that may be difficult to confirm.

2.6 Attack Type Categorisation

All documented attacks which we have researched have been divided into types based on their main characteristic or purpose.

The attack types were determined to enhance simplicity in the research. These 4 categories have allowed us to categorise all the performed attacks based on their main purpose.

Attacks are categorized into the following types listed in the table below. Following the table are further explanations on the different attack types.

Cognitive	An attack of this type is designed to cognitively influence the target. An example of this attack can be a disinformation campaign. Data leaks are also included in this category.
Destructive	An attack of this type is designed to damage or destroy data. The data which is attacked may be specifically targeted or may be random.
Disruptive	An attack of this type is performed with the intent to disrupt services and cause outages. Typical disruptive attacks are Distributed Denial-of-Service (DDoS) attacks.
Reconnaissance	An attack of this type is performed with intent to gather information.

Table 2.2: Attack types

2.6.1 Attack type explanation: Cognitive

Cognitive warfare exploits the human mind as its battlefield. Here the attacker tries to influence and change how people think and act. If successful it can change how a group behaves in favour of the aggressor. Cognitive attacks can have both short and long term goals [40].

2.6.2 Attack type explanation: Destructive

Destructive attacks aim to take down or damage the targeted system or network. At times these can look like ransomware attacks, but instead of encrypting the files they will overwrite the data and make it inaccessible.

The Danish Center for Cyber Security [41] describes destructive attacks like this: "Destructive cyber attacks are attacks that could result in:

- Death or personal injury.
- Significant physical damage.
- Destruction or manipulation of information, data or software, rendering them unfit for use unless extensive restoration is undertaken."

The best example of a physically destructive cyberattack is the one that hit the Iranian uranium enrichment centrifuges, and was named *Stuxnet* [42].

2.6.3 Attack type explanation: Disruptive

As the name implies, disruptive attacks aim to disrupt the target's operations or services.

During the course of this war, observations show that this is usually performed by launching a DDoS attack. DDoS derives from the term DoS which stands for *Denial of Service*, where the first 'D' stands for *Distributed*. These attacks attempt to flood the targeted system with false requests, thus overloading it and rendering the system inoperable.

2.6.4 Attack type explanation: Reconnaissance

In a reconnaissance attack, the attacker tries to gain information about the target system or network. This information is then used to identify vulnerabilities to be used in upcoming attacks [43].

Reconnaissance is a crucial part of any modern conflict or war. It is used to gather information about an adversary's strengths and weaknesses. Reconnaissance can be both active and passive, and has six primary disciplines.

More on reconnaissance and how it has been utilised in this war can be found in section 6.2.5.

2.7 Examining significance of cyberattack methods

A clear pattern arises when examining the cyberattacks which have been performed in the Russo-Ukrainian war. Early in the war, there was a prevalence of destructive attacks that were aimed against Operational Technology (OT) which controls critical infrastructure and government operational systems [35].

Paired alongside physical attacks, such as targeted missiles and ground forces, these cyberattacks have a goal to damage as many targets as possible. After the first couple of weeks, these attack methods had all but been exhausted. The defensive efforts which Ukraine and its allies had responded with proved to be worth the effort. As the war persisted for more than two months, all the initially planned cyberattacks were expended.

The next step of cyberattack methods comes in the form of a combination of disruptive attacks as well as cognitive attacks [44]. Disrupting online systems has become a quick and relatively easy method of performing an attack. However, the effect these attacks have are often no more than a temporary issue and have no lasting effects. Most disruptive attacks are seen in the form of DDoS attacks, where the goal is to create a temporary disruption in a provided online service. On the other hand, for any organisation which relies heavily on having a stable online presence, a DDoS attack may be an effective attack method which very often achieves its goal of temporary disruption.

Acting in conjunction with the disruptive attacks, a significant amount of cognitive attack methods were employed [45]. Cognitive attacks make use of modern globalisation and quick spread of information through online media. The methods employed here vary, but are most often seen as disinformation and misinformation campaigns.

The aim of these campaigns is to cognitively influence either a certain target group or as many people as possible through online media. In this war, Russia's cognitive attacks aim to create a false narrative which in turn bolsters their own reputation or weakens Ukraine's [45].

2.8 NotPetya, Cyberwarfare, and NATO

NotPetya was a major cyberattack, launched on June 27th 2017 which affected companies in countries across the world. Ukrainian organisations were the first to report being victims of the attack [46]. Kaspersky Labs reported that around 90% of the attacks were located in Ukraine (60%) and Russia (30%). The remaining 10% of attacks were mostly located in Poland, Italy and Germany [47].

The malware was first identified as ransomware, requiring the victims to pay a ransom to unencrypt the data which had been encrypted. However, analysis performed by Kaspersky Labs a day after the attack revealed that the malware was a wiper and the encrypted data could not be decrypted [48].

The *NotPetya* cyberattack was attributed to the GRU, specifically the Sandworm group [49]. In other words, Russian state sponsored actors could be attributed to being the perpetrators of the attack.

The reactions to the *NotPetya* attack indicated that a cyberattack of this caliber could be a catalyst for escalation or an act of war. NATO chief Jens Stoltenberg made a remark that the *NotPetya* ransomware could "trigger collective defense" based on NATO's Article 5 [50]. NATO researcher Tomáš Minárik also said that the *NotPetya* attacks could warrant retaliation if the attack was deemed to be state-sponsored [51].¹

These remarks show that NATO is aware of the impending threat of Russian state-sponsored threat actors, as well as the intentions of the Kremlin. NATO was aware that Russia would likely start a war by invasion, but they were unsure of who the target would be among the countries around the Black Sea and former members of the Soviet Union [52].

¹The attacks were attributed to the GRU in 2020. The attribution was however not done by NATO, but rather the American Department of Justice [46].

2.9 War in Donbas (2014-2022) Timeline

18.-23. Feb 2014	•	Revolution of Dignity ensues resulting in a Euromaidan victory[21].
Feb-Mar 2014	•	Pro-Russian unrest in southern[53] and eastern Ukraine[54].
18. Mar 2014	•	Russia annexes the Crimean peninsula[9]
2014-2015	•	BlackEnergy malware causes blackouts in the Ivano-Frankivsk region.[28]
Jun 2017	•	Ukrainian organisations fall victim to NotPetya ransomware.[46]
Apr 2021	•	FROZENVISTA phishing campaigns target Ukraine[55]
Sep-Oct 2022	•	FROZENLAKE phishing campaign sends over 14000 emails to targets worldwide[55]
(2022 Q1) 11. Jan 2022	•	Joint Cyber Security Advisory on Russian State-sponsored cyber-threats released by USA authorities.[56]
Jan 2022	•	FROZENVISTA phishing campaign targeting Ukraine for the second time.[55]
13. Jan 2022	•	WhisperGate wiper deployed to Ukrainian government and IT systems. [35]
14. Feb 2022	•	Odessa-based critical infrastructure compromised by Russian actors. [35]
15-16. Feb 2022	•	GRU DDoS attacks against Ukrainian financial institutions. [35]
17. Feb 2022	•	Suspected Russian actors detected in critical infrastructure in Sumy.[35]
23. Feb 2022	•	IRIDIUM deploys FoxBlade wiper in hundreds of systems across multiple organizations linked to Ukrainian government, IT, energy and financial sectors. [35]
23. Feb 2022	•	HermeticWiper detection revealed by ESET [57]

2.9.1 Aftermath

The pre-war timeline shows that Russian actors have been steadily preparing cyberattacks for a while prior to the full onset of the war. The cyberattacks which have been observed are destructive wiper attacks and disruptive DDoS attacks. Both of these types of attacks were used with the intention of creating service disruptions throughout Ukrainian organisations leading up to the war.

There was also a large amount of phishing activity, specifically targeting organisations in Ukraine with the *FROZENLAKE* and *FROZENVISTA* phishing campaigns. These campaigns were likely the initial access methods for some of the attacks which were executed directly after the war began [55].

Chapter 3

Method

3.1 Introduction

In this chapter, we have detailed the activities that were undertaken to answer the research questions presented in section 1.3.1. We have provided a thorough description of the research, data analysis, and other activities used in our study. We will justify why each method was chosen and how it contributes to answering the research questions. Our aim is to provide a road-map for the activities undertaken to answer the research questions and to ensure that the research is conducted in a systematic and robust manner. In the following sections, we will describe each method used and provide detailed explanations for our choices.

3.2 Research Design

For the research process we have conducted qualitative research by searching for online news articles, blogs, and reports which contain information about cyber-attacks which have been conducted and reported in the current Russo-Ukrainian war.

Our project is performed as a literature review where we review previously published information on this topic. This has allowed us to gain important insight into the timeline of cyberattacks in the war as well as understand which threat actors are active in the cyberdomain. This process also involves being critical of the sources we encounter so as to not present false, inaccurate, or biased information.

For our sources we have used a combination of grey literature and news publications. This way we have been able to find news about events as well as reports from security organisations detailing specific attacks and periods. It has also allowed us to make specific claims about threat actors and their affiliations.

3.3 Data Collection

Data collection has been a crucial part of our research and we have therefore used various methods to collect data. Among these methods were strategic web searches, the use of ChatGPT, social media, and communication with relevant people and organisations.

Strategic web searches allowed us to efficiently find relevant information and identify useful sources of data. The use of ChatGPT provided us with helpful insights and answers that traditional web searches may have missed. We also used social media platforms, mainly Telegram to collect quantitative data from public opinions and discussions. Finally, communication with relevant individuals and organisations through interviews and written correspondence has provided us with first-hand insights and data that has been beneficial to our research.

By using a combination of these methods we have been able to gather diverse and high-quality data that has allowed us to provide valuable insights and findings in our research.

3.3.1 Web search

Conducting research by searching on the internet was our main method of discovering relevant pieces of information. This was done by looking for articles using several search engines and by inserting related keywords to narrow down our searches. An important reason behind utilising multiple search engines was to expand our searches in order to detect a greater variety of sources, or just to look for specific data. Aside from regular search engines such as Google etc. we also used Google Scholar to specifically find academic works, and as mentioned earlier, ChatGPT to locate articles that might have taken unnecessary time to locate.

Due to the research being heavily reliant on searching for open-source information, we had to resort to including related keywords that narrowed down our search to what we were looking for. In addition to being used on their own, the keywords were also used along with other keywords to be even more specific in some cases. Some of the more important keywords were:

- Cyberattack
- Russo-Ukrainian war
- Cyberwarfare
- Cybersecurity
- Timeline
- Analysis

3.3.2 ChatGPT

To assist us in finding sources, we also made use of the ChatGPT artificial intelligence and its capabilities of returning the information we were looking for. Due to the inconsistencies in some details, especially referencing, our main use of ChatGPT was to use it as a search engine to discover further pieces of information. After finding relevant data to answer the research questions, we continued by going back to the web search method to ensure validity and reliability that ChatGPT on its own would likely not provide.

This method was also recommended by our client.

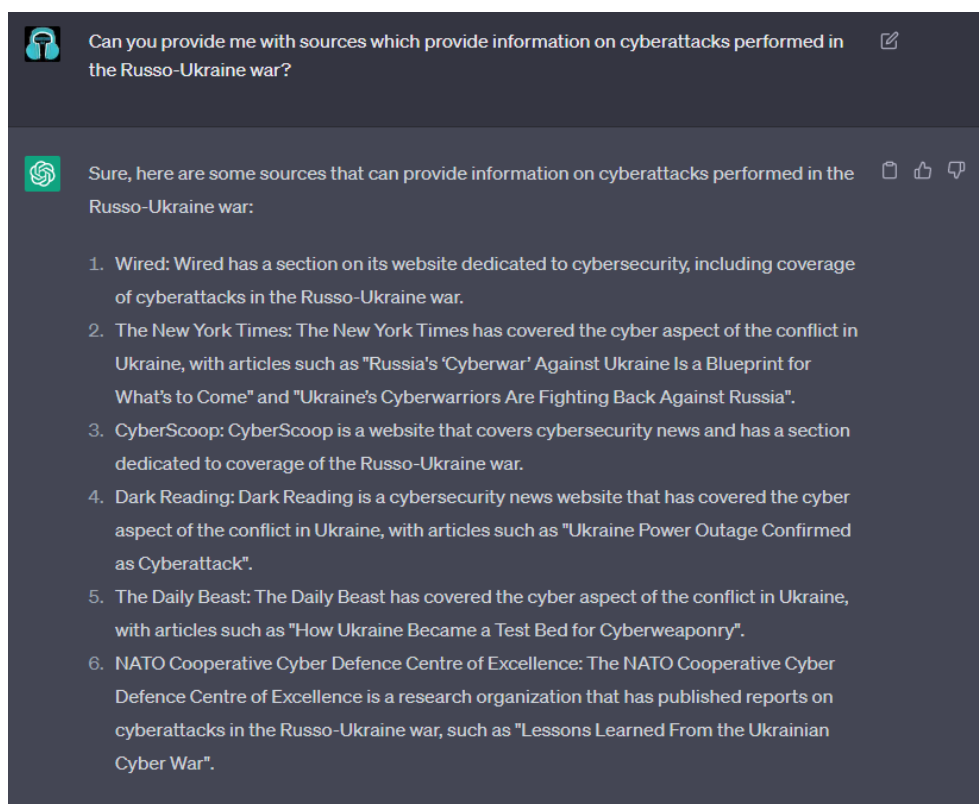


Figure 3.1: Example image of ChatGPT use.

3.3.3 Social media

To find more obscure information, we also decided to use social media, mainly by joining various Telegram channels related to news about the war. As our client also recommended this method, he provided us with a few Telegram channels that could possibly be useful. In addition to Telegram, some information and graphics have been found on Twitter, as the platform is still popular with several actors in fields relevant to this study.

Due to the obscurity of the information posted to social media, it is naturally also less reliable due to having fewer available sources to back it up, along with displaying possible biases and agendas.

3.3.4 Lecture

Our client gave us the opportunity to have a history professor present the history behind Russian and Ukrainian relations. This seemed like an effective way of gaining information about the historical context of the conflict itself and the relations between the two nations.

The lecture provided us with interesting background information to the ongoing conflict, but due to the time-frame that was focused on (< 1945), we were unable to relevantly include much of the gained information from the lecture in this report.¹

3.3.5 Correspondence

In order to gather information that was not as easily available, or published at all, we also chose to reach out to several Norwegian cybersecurity companies and -agencies by e-mail. Since this thesis is supposed to be available to the public, we also mentioned that we were only looking for information that could be published. We used this method to gather information that may not have been found as easily online, and was done in an attempt to provide insight about the more unknown sides of the conflict.

From a total of eight e-mails sent, we received three answers. The replies confirmed that we were on the right track, as the replies only contained information and published reports which we had already tracked down on our own.

¹Notes from this lecture can be found in Appendix D

3.4 Data Analysis

As our research was heavily dependent on other sources of information, we opted to using analysis methods that involved using additional data in order to fit our research. One of the major preparations we made for data analysis was converting our findings into descriptive statistics in the form of charts. These would help us explain and visualise the results that we gathered from our research. When analysing more specific data, we would naturally make use of methods such as meta-analysis and literature review, meaning that a considerable amount of our analysis was based on the results of other scientific research and the contents of other published information, such as news or other types of articles.

3.5 Ethical Considerations

When using any amount of material from external sources, we made sure to properly provide appropriate citing or crediting to avoid falsely claiming the work as our own. To maintain proper authenticity within our thesis, we recognised that avoiding data manipulation and bias from our own side was absolutely necessary. This involved not altering any results in order to fit them to answer our research questions, while also documenting both sides of the war to avoid possible biases from our side.

3.6 Validity and reliability

Since we used various sources while researching, with some being less reliable than others, we took into action measures to validate our findings. When referring to sources that may not be known for their reliability, we also checked for other sources that state the same details to ensure that the articles are not entirely made up. An important reason to why we resorted to this method was that most of the articles that we found were relatively new, and availability of expert analysis about the incidents was scarce. Using this method was also recommended by the client. When it came to more reliable sources such as Microsoft or BBC, using this method was not as necessary, and would only be used to gather more details about the same events.

Chapter 4

Main Timeline


The following page contains a timeline over important events and cyberattacks performed in the Russo-Ukrainian war from February 23rd 2022 through February 1st 2023.

As our scope ranges from February 1st 2022 through February 1st 2023, attacks performed from February 1st 2022 to February 22nd 2022 are located in the War in Donbas timeline (section 2.9). This way they are sorted correctly, as that specific time is categorised as pre full-scale invasion.

The timeline is sorted in a chronologically ascending order. Each event has dates on the left side of the line and a short description of the event along with a source citation on the right. Additionally, the timeline also contains markers indicating the quarters of the year.

4.1 Full-scale invasion cyber-timeline

(2022 Q1)	23. Feb 2022	HermeticWiper attacks mark the first destructive attacks which are attributed to the war effort. (Section 5.2) [57]
	24. Feb 2022	Russia invades Ukraine [10].
	24. Feb 2022	Russian government websites were taken down [58].
	28. Feb 2022	Denial of Service attack against Viasat[59].
	28. Feb 2022	Kyiv based media-companies are victims of destructive attacks [35].
	2. Mar 2022	Microsoft document lateral movement of threat actor in Ukrainian nuclear power network [35].
	4. Mar 2022	STRONTIUM (Fancy Bear/APT28) compromise Vinnytsia government network [35].
	16. Mar 2022	Zelenskyy deepfake is spread across social media[60] [61].
(2022 Q2)	1.-12. Apr 2022	Industroyer2 and CaddyWiper attacks revealed by CERT-UA and ESET [62][63].
	19. Apr 2022	IRIDIUM performs destructive attack against Lviv-based logistics provider [44].
	29. Apr 2022	Microsoft reveal IRIDIUM (Sandworm) to be behind reconnaissance attacks on Lviv transportation sector network [44].
	5. May 2022	Odessa City council hit by cyberattack [60].
	May-Jun 2022	Continued global phishing attempts from SEABORGIUM (ColdRiver) [45].
(2022 Q3)	19. Jul 2022	Google TAG reveals KRYPTON (Turla) distributing Android malware targeting the Ukrainian IT Army [64].
	27. Jul 2022	CISA and SSSCIP sign cooperation agreement [65].
	30. Jul 2022	SSSCIP release report stating a total of 203 attacks on local Ukrainian authorities and financial institutions in July [66].
	16. Aug 2022	Ukrainian nuclear power operator, EnergoAtom, website attacked by Russian hackers [67].
	22. Aug 2022	Ukraine and Poland sign memorandum on cyber security cooperation [68][69].
	1. Sep 2022	Anonymous cause massive traffic jam in Moscow after hacking Yandex Taxi app [70].

- 
- (2022 Q4) 11. Oct 2022 • "Prestige" ransomware attacks organisations in Ukraine & Poland [71].
 - 7. Nov 2022 • CERT-UA identify Gamaredon phishing campaign intended to spread malware [72].
 - 3. Dec 2022 • Microsoft reports recent trends in Russian cyberattacks could indicate a shift to attacks towards organisations outside Ukraine [73].
 - 15. Dec 2022 • UNC4166 targeting Ukrainian organisations with trojanised Windows 10 installers [74].
 - (2023 Q1) 21. Jan 2023 • Rasmus Paludan performs Quran burning outside Turkish embassy in Sweden. Organised by Pro-Kremlin journalist [75].
 - 1. Feb 2023 • **End of scope**

4.2 Quarterwise overview

4.2.1 Quarter 1

Quarter 1 of 2022 is the time period ranging from January towards the end of March. This period contains the pre-war documentation and advisories released as the US authorities and NATO were preparing for a likely invasion by the Russian Federation.

The commencement of the war took place on February 24th 2022, with the entire world viewing a modern war politically disguised by the term "special operation".

One special attack of note is the spread of the Zelenskyy deepfake [61]. This was a type of cognitive attack aimed towards the citizens who use social media and watch local news. The video in question shows a fake video of Ukrainian president Volodymyr Zelenskyy telling Ukrainian soldiers to lay down their weapons and go home. This video spread like wildfire in social media after being released on a compromised Ukrainian news website.

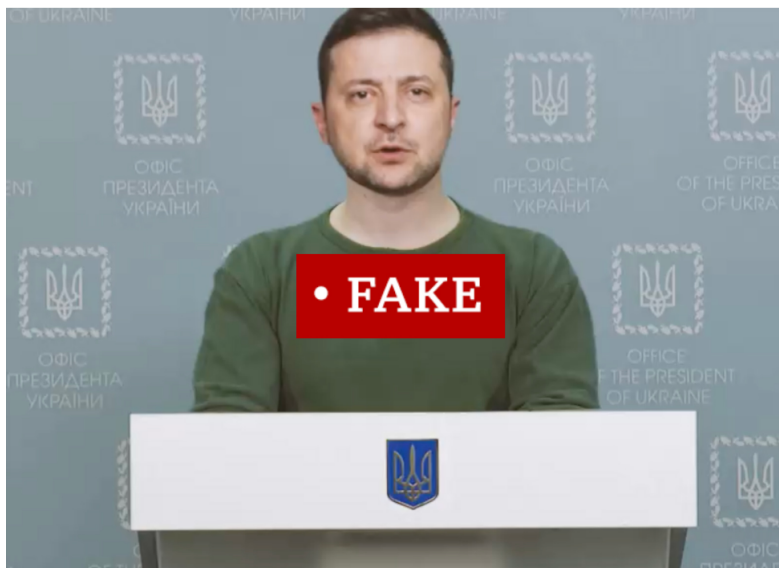


Figure 4.1: Screenshot from the Zelenskyy deepfake [76].

Head of security policy at Meta, Nathaniel Gleicher, issued a statement on Twitter in which he said that this video was reviewed and removed from their platform as it violated their policy for "misleading manipulated media" [77].

This quarter contains a large amount of destructive attacks aimed towards Ukrainian critical infrastructure networks as well as governmental institutions. The pur-

pose of these destructive attacks was to cripple infrastructure in Ukraine alongside the invasion from Russian ground forces.

4.2.2 Quarter 2

Quarter 2 of 2022, which spans from April to June, marks a shift from destructive cyber attacks to a more cognitive attack focus. This shift in methods is likely caused by a failure to predict a prolonged war.

As destructive attacks require a considerable amount of time to plan and execute, it is possible that the Russian cyber-threats had exhausted their capabilities in deploying such attacks at this point. Notably, the deployment of *Industroyer2* marked the last novel malware attack before the deployment of *Prestige* in October 2022.

Despite the decrease in destructive attacks, there was a significant increase in propaganda, disinformation, and efforts to undermine Ukraine's foreign support [45].

4.2.3 Quarter 3

Quarter 3 of 2022, which spans from July to September features no destructive attacks. On the other hand, August is the month which has the largest amount of disruptive attacks. These attacks are almost entirely performed by hacktivists in the form of DDoS attacks, originating from both sides of the war. From the Russian side, the most active hacktivist group is the People's CyberArmy [78].

On the Ukrainian side the most active hacktivist group is the IT Army of Ukraine [78]. With the rise of hacktivism we also see an interesting attack performed by the threat actor KRYPTON (Turla). This threat actor targeted the IT Army of Ukraine with Android malware [64].

This high amount of disruptive attacks continues into September as well.

This period also features Ukraine's counteroffensives in Kherson (late August) and Kharkiv (early September). In the cyberdomain, APTs likely used this period to prepare future destructive cyberattacks for Quarter 4.

4.2.4 Quarter 4

Quarter 4 of 2022 rounds out the year spanning from October through December and features a prominent cyberattack in the form of the *Prestige* ransomware [71]. This attack was a ransomware campaign launched on October 11th. It targeted transportation and logistics organisations in both Ukraine and Poland. The attack was attributed to the Russian APT IRIDIUM, aka Sandworm [71].

In December, Microsoft reports a likely shift in Russian cyberattack targets [73]. Seeing as *Prestige* hit Poland, it was likely that Russian cyber operations could be aiming to target countries and organisations who were providing Ukraine with vital aid.

4.2.5 2023 – Quarter 1

Due to the scope of our project, 2023 includes only the period of January through February 1st. February 24th marked 1 year of war between Russia and Ukraine, with no end to be seen in the foreseeable future.

The most important event of this month is the psychological operation (PsyOp) performed through the burning of a Quran outside the Turkish embassy in Sweden by the Danish politician Rasmus Paludan. This event was organised and financed by a pro-Russian journalist, Chang Frick [75].

The importance of this event lies in the fact that it was spread swiftly through social media and news channels. This could in turn influence people cognitively and create political discourse.

We cannot say with certainty whether this was planned by Russian state actors. However, the sources state that the man who organised the event is a pro-Russian journalist who is likely attempting to spread a pro-Russian agenda.

Chapter 5

Analysis of Cyberattacks in the Russo-Ukrainian War

5.1 Introduction

This chapter will cover subjects that are crucial for this thesis, as they are central for our discussion and results. Areas covered in this chapter include attacks, their types, their sources, attribution of attacks while simultaneously providing a cyberattack overview for the full invasion timeline.

The chapter contains an overview of notable cyberattacks from the first quarter of 2022 through the beginning of 2023. The contents of this chapter are organised chronologically with the oldest events at the beginning and the most recent events towards the end.

The attacks we have deemed to be notable are the ones which have had a more significant impact in the war. The notable attacks also contribute to explaining the most relevant attack methods per quarter. Analysing these attacks will show how the war has been unfolding over the past year. The events also show which threat actors are most active in the war and how certain threat actors are more experienced with launching attacks with specific attack methods. Additionally, each event contains notes describing details relating to the event and its significance.

For attack type explanations, refer to section 2.6.

5.2 Attack overview

5.2.1 2022 Q1

Quarter 1 of 2022 includes the month-and-a-half preceding the declaration of the war as well as the month-and-a-half after the outbreak of the war.

As such, the attacks which take place in this period are grouped into pre-war and during the war. However, this does not mean that the attacks preceding the war are any less important, but rather that they are part of a "wave" signaling an imminent invasion.

The following page contains notable events in quarter 1 of 2022.

Notable events in Q1:

Name	WhisperGate
Date	2022-01-13
Type	Destructive
Attribution	DEV-0586 ¹
Source	<i>Special Report: Ukraine</i> by Microsoft Security Threat Intelligence Center [35]
Notes	WhisperGate is the earliest wiper attack in 2022 leading up to the start of the war. The malware was specifically targeted towards Ukrainian government and IT sector systems. This destructive attack is likely a direct result of failed de-escalation attempts through diplomatic efforts.

Table 5.1: WhisperGate campaign

Name	HermeticWiper, IsaacWiper and HermeticWizard
Date	2022-02-23
Type	Destructive
Attribution	pro-Russian actor
Source	WeLiveSecurity by ESET Research [57]
Notes	This attack is one of the earliest offensive cyberattacks which can be attributed directly to the war effort. The attack precedes the invasion of Ukraine by only a few hours, but artifacts analysed suggest that the attack had been planned for months.

Table 5.2: HermeticWiper campaign

¹"Microsoft uses DEV-#### designations as a temporary name given to an unknown, emerging, or a developing cluster of threat activity, allowing Microsoft Threat Intelligence Center (MSTIC) to track it as a unique set of information until we reach a high confidence about the origin or identity of the actor behind the activity." [79]

Name	Zelenskyy deepfake
Date	2022-03-16
Type	Cognitive
Attribution	Unattributed
Source	Wakefield, Jane for BBC News [61]
Notes	<p>This video was spread to multiple social media sites. In the video, an obviously fake Volodymyr Zelenskyy appears to tell his soldiers to lay down their arms and surrender the fight against Russia.</p> <p>Zelenskyy himself was quick to post a video to his official Instagram refuting the claims made in the fake video [76].</p>

Table 5.3: Zelenskyy deepfake

5.2.2 2022 Q2

Quarter 2 of 2022 spans from April through June. This period is predominantly frontloaded with destructive attacks performed by IRIDIUM in April and May. This period of time starting in June is relatively quiet, featuring only a couple disruptive attacks alongside some data leaks categorised as cognitive attacks.

Notable events in Q2:

Name	Industroyer2
Date	2022-04-08
Type	Destructive
Attribution	IRIDIUM (Sandworm)
Source	WeLiveSecurity by ESET Research [63]
Notes	This cyberattack, performed by the Sandworm group, shows intent to destroy critical infrastructure in Ukraine. According to Portable Executable (PE) file analysis the attack had been planned for more than two weeks. Acting in coordination these two pieces of malware are used to take control of the ICS of the power stations which were targeted, and then wipe any trace of the malware from the system to cover their tracks, as well as hampering recovery processes.

Table 5.4: Industroyer2

Name	CaddyWiper
Date	2022-04-12
Type	Destructive
Attribution	IRIDIUM (Sandworm)
Source	CERT-UA [62]
Notes	CaddyWiper is an attack performed alongside Industroyer2 towards critical energy infrastructure in Ukraine.

Table 5.5: CaddyWiper

Name	IRIDIUM coordinated attacks towards Lviv
Date	2022-04-19 through 2022-05-03
Type	Destructive
Attribution	IRIDIUM (Sandworm)
Source	Microsoft: <i>Defending Ukraine: Early lessons from the Cyber War</i> [44]
Notes	<p>This specific coordinated cyber- and physical attack timeline is important in the sense that it reveals how a cyberattack is performed in conjunction with a kinetic missile strike.</p> <p>On April 19th 2022, the threat actor IRIDIUM is attributed with performing a destructive attack against an Lviv-based logistics provider.</p> <p>On April 29th 2022, IRIDIUM conducts reconnaissance against a transportation sector network in Lviv.</p> <p>On May 3rd 2022 Russian missiles strike multiple railway substations disrupting the transportation service in Lviv.</p> <p>This entire sequence of events, conducted only over 14 days, shows the role of cyberattacks combined with kinetic strikes.</p>

Table 5.6: IRIDIUM coordinated hybrid attack

5.2.3 2022 Q3

Quarter 3 of 2022 shows the rise of hacktivism in the Russo-Ukrainian war. August had the highest amount of disruptive attacks seen so far, and most of them were attributed to hacktivist groups on both sides of the war [78].

This quarter also features the Ukrainian counteroffensives in the Kherson and Kharkiv areas. It could be assumed that the significant increase in hacktivist activity was a form of power projection while the Russians were focused on the offensive ground war.

Notable events in Q3:

Name	KRYPTON Android malware targeting IT Army of Ukraine
Date	2022-07-19
Type	Disruptive
Attribution	KRYPTON (Turla)
Source	Google Threat Analysis Group [64]
Notes	<p>This attack is located in the beginning of the rise in hacktivist activity for Quarter 3. It is specifically targeted against the hacktivist group named the IT Army of Ukraine.</p> <p>The Android apps were hosted on a domain spoofing the Ukrainian Azov Regiment, which was disseminated across social media channels. The apps were claimed to perform DDoS attacks against Russian sites, but did not do this and were instead infected with malware.</p> <p>Google assessed there to be little to no damage, and installs were minimal.</p>

Table 5.7: KRYPTON (Turla) Android Malware

Name	EnergoAtom DDoS attack
Date	2022-08-16
Type	Disruptive
Attribution	People's CyberArmy
Source	EnergoAtom official source [67]
Notes	<p>EnergoAtom is a Ukrainian nuclear energy provider. The official media channels of EnergoAtom published that they had been targeted in a large DDoS attack by the People's CyberArmy.</p> <p>EnergoAtom did however ensure that this did not significantly impact their work in any way.</p> <p>This attack is part of the massive wave of disruptive attacks from both sides and shows that hacktivist groups are clearly very active in attempting disruptive operations against important targets.</p>

Table 5.8: EnergoAtom website hack

Name	Anonymous cause Moscow taxi traffic jam
Date	2022-09-01
Type	Disruptive
Attribution	Anonymous
Source	HackRead and @YourAnonTV [70]
Notes	This is another attack performed by hacktivist activity. The Anonymous collective performed a hack of the Yandex Taxi service in Moscow. The hack allowed them to order all available taxis to one location. This caused a traffic jam in central Moscow which lasted for three hours.

Table 5.9: Anonymous Moscow traffic jam

5.2.4 2022 Q4

Quarter 4 of 2022 features the *Prestige* ransomware attack targeting transportation organisations in both Ukraine and Poland. This could indicate a shift in threat actor activity towards targeting countries other than just Ukraine.

Simultaneously, there are also continued phishing attempts, primarily from the Gamaredon threat actor. These phishing campaigns towards Ukrainian targets are likely used as initial access methods which can later be used in more destructive attacks.

Quarter 4 is likely the start of a second wave of cyberattacks in the war. Threat actors have had time to develop more destructive malware and have gained initial access through consistent phishing attempts throughout Quarters 2 and 3.

Notable events in Q4:

Name	Prestige ransomware attack
Date	2022-10-11
Type	Destructive
Attribution	IRIDIUM (Sandworm)
Source	Microsoft Threat Intelligence Center[71]
Notes	<p>The Prestige ransomware is an important attack in Quarter 4. It is the first novel ransomware (used in the war) since Industroyer2 in April 2022.</p> <p>Prestige was mainly targeted toward the transportation sector in Ukraine, but also had victims in Poland.</p> <p>As Prestige was the first destructive attack in many months, it could signal that Russian threat actors were ready to launch another wave of sophisticated attacks in the war effort.</p> <p>The fact that Prestige also had victims in Poland was significant in that it may indicate a shift in Russian threat actor tactics where they target more European countries.</p> <p>The Prestige ransomware was also likely a test for the "Sullivan" variants released in the same campaign, by IRIDIUM as well.</p>

Table 5.10: Prestige ransomware attack

Name	Gamaredon malware campaign
Date	2022-11-07
Type	Destructive
Attribution	ACTINIUM (Gamaredon)
Source	CERT-UA [72]
Notes	<p>Gamaredon is an active threat actor in the Russo-Ukrainian war but has mostly focused on phishing campaigns and spreading malware.</p> <p>The aim of these campaigns is to load destructive malware on Ukrainian organisations systems.</p> <p>CERT-UA explains that Gamaredon has been consistently performing phishing attacks against Ukrainian organisations. This is likely also a method of initial access in attempts to perform more destructive attacks and identify vulnerabilities in systems.</p>

Table 5.11: Gamaredon phishing campaign

Name	UNC4166 targeting Ukrainian government with trojanised Windows 10 installers
Date	2022-12-15
Type	Destructive (Reconnaissance)
Attribution	UNC4166 ²
Source	Mandiant Intelligence [74]
Notes	<p>Mandiant identified UNC4166 to be targeting Ukrainian officials and government organisations with trojanised Windows 10 installers. These versions of Windows 10 are spread through torrent sites as a supply chain attack.</p> <p>These infected versions of Windows 10 are designed to exfiltrate data from the systems where they are installed. Mandiant cannot attribute UNC4166 to any previously tracked group, but they do provide an analysis which shows an overlap of targets related to GRU clusters.</p>

Table 5.12: UNC4166 Trojanised Windows 10 installers

²UNC-#### is a categorisation assigned by Mandiant to Uncategorized Threat Groups. This means that there is not enough information on the group or the attacks performed to correlate them with an existing group.

5.2.5 2023 Q1

Quarter 1 of 2023 contains only the month of January until February 1st 2023 as mentioned by our choice of scope. This month of January does however contain one provocative event: The burning of a Quran outside the Turkish embassy in Sweden [80].

This was not a regular cyberattack in the sense that there was no digital involvement, however an argument could be made that this is a strong cognitive attack meant to influence people through media exposure.

Though the demonstration was performed by a Danish far-right politician, Rasmus Paludan, it was a pro-Kremlin journalist named Chang Frick that had paid the administrative fee to organise the inflammatory protest [75].

It is unknown whether this organisation was done on a mission from the Kremlin or if it was Frick's own initiative. Despite this, the essence of the protest remains the same; a pro-Russian ideologist organised an extremist demonstration to sour the relations between Sweden and Turkey.

The reason for this demonstration at this time is likely due to the upcoming 2023 Turkish general election where President Recep Tayyip Erdoğan is attempting to get reelected. Turkish-Swedish relations have recently been tense and as Sweden attempts to join NATO, Turkey must ratify the Swedish NATO application. Russia is likely attempting to destabilise the relations so that Turkey decides to not accept the Swedish application. Erdoğan has even said "*Those who allow such blasphemy in front of our embassy can no longer expect our support for their NATO membership[...]*" [81].

This shows how a cognitive attack using media exposure can be seen as a relevant attempt at using the cyber domain to influence political relations and public opinion.

Chapter 6

General Findings

6.1 Introduction

This chapter contains the thesis' general findings, providing an overview of our research and results. These findings were the results of research conducted by following the methods presented in the method chapter. The main topic of the chapter is an overview of registered attacks divided by category. Each section aims to answer the research questions presented in 1.3.1.

The purpose of documenting the methods used in these cyberattacks is to provide an overview of how modern cyberwarfare is being conducted.

Due to the nature of this conflict being ongoing at the time of writing, all numbers might not represent the actual amount of attacks.

6.2 Methods used in the documented cyberattacks

6.2.1 Introduction

The Russo-Ukrainian war is the first modern, large scale conflict where cyberwarfare has shown what it can and can not do. Hundreds of attacks have been reported on both sides during our chosen scope as seen in figure 6.1. The war is still ongoing as of May 2023 [78].

This section will address the problem statement presented in section 1.3 "*What methods have been used in cyberattacks between the main actors in the Russo-Ukrainian war?*".

Also answered in this section is the research question: "*What methods have been used in documented cyberattacks in the Russo-Ukrainian war?*".

The main research question, and the name of the task, was to survey the methods in which cyberattacks are being used in the Russo-Ukrainian war. By finding sources on as many attacks as possible we were able to map the usage of the different method categories. The results of our research can be seen later in this chapter.

Our primary sources for the attack numbers are the CyberPeace Institute [78], and Microsoft's March 2023 report [45]. The numbers from these sources were then sorted into monthly categories and then added to the graphs in this section. If a cyberattack lasted over multiple days crossing between months, the start date is what was counted.

We have only included attacks of the categories: cognitive, destructive, disruptive, and reconnaissance. These four categories make up the majority of attacks and simplifies the categorisation process. If an attack was outside these categories (ex. phishing) it has not been counted. There are a total of 21 attacks categorised as "Other/Unknown" in our sources which we have not included, this includes phishing campaigns. We have taken the decision to categorise phishing as an entry vector and not a cyberattack. All numbers in this section are what we could find as of 01.04.2023 and may not be representative of the actual amount of cyberattacks.

Figure 6.1 shows the general trend in cyberattacks from both sides during the conflict. As the graph clearly shows, there was a lot of activity in the beginning which then fell off during late spring/early summer. Later in this chapter we will further explain each category’s details and their numbers. Due to no reported attacks being explicitly defined as reconnaissance, it is not included in this graph.

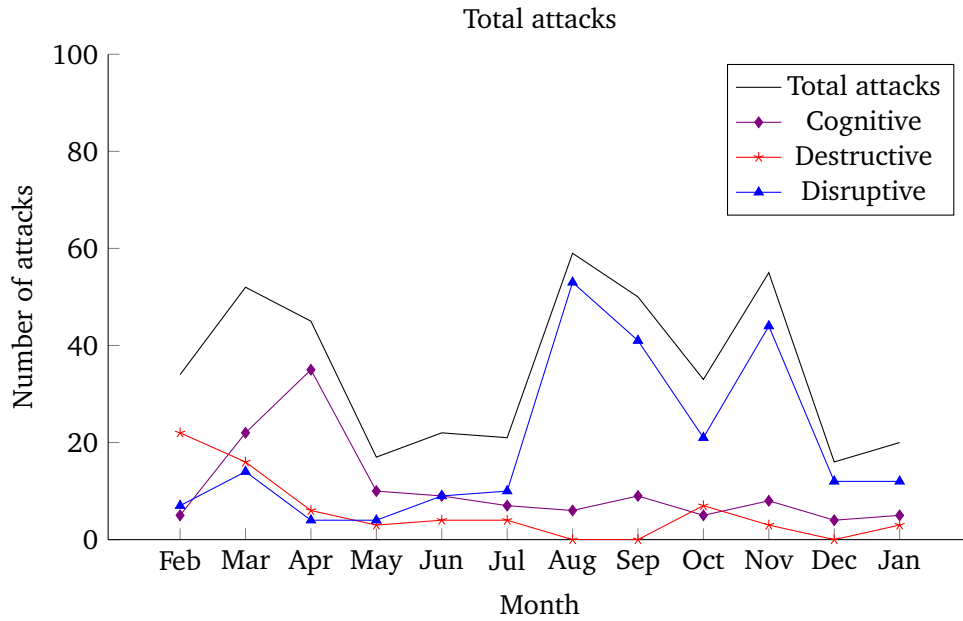


Figure 6.1: Attacks per month between Feb 2022 - Feb 2023 [45] [78]

Our results show that both parties in the conflict have used cognitive, destructive and disruptive cyberattacks in the conflict. We assume that both sides have performed reconnaissance attacks, both before and during the conflict. The table below contains the total number of attacks grouped by quarter and attack type.¹

Attack Type	Q1	Q2	Q3	Q4	Jan 2023	Total
Cognitive	27	54	22	17	5	125
Destructive	38	13	4	10	3	68
Disruptive	21	17	104	77	12	231
Reconnaissance	0	0	0	0	0	0

Table 6.1: Quarterly attacks by attack type

¹Refer to Appendix A.1 for raw numerical data

6.2.2 Cognitive warfare

A certain attack of note is the deepfake in March 2022 of Ukrainian president Volodymyr Zelenskyy telling the Ukrainian people to lay down their weapons and surrender (mentioned in table 5.3). This video was uploaded to a hacked Ukrainian news site [61]. Most likely, this operation had the goal of making Ukrainian defence forces surrender and thus advance Russian territorial gains.

Figure 6.2 shows the number of cognitive cyberattacks against both sides during the conflict. "Hacks and leaks" are included, because they can have a cognitive effect depending on what was leaked (e.g documents which smear influential people). This in turn means that many of the attacks we see against Russia here are leaked documents from state institutes and organisations.

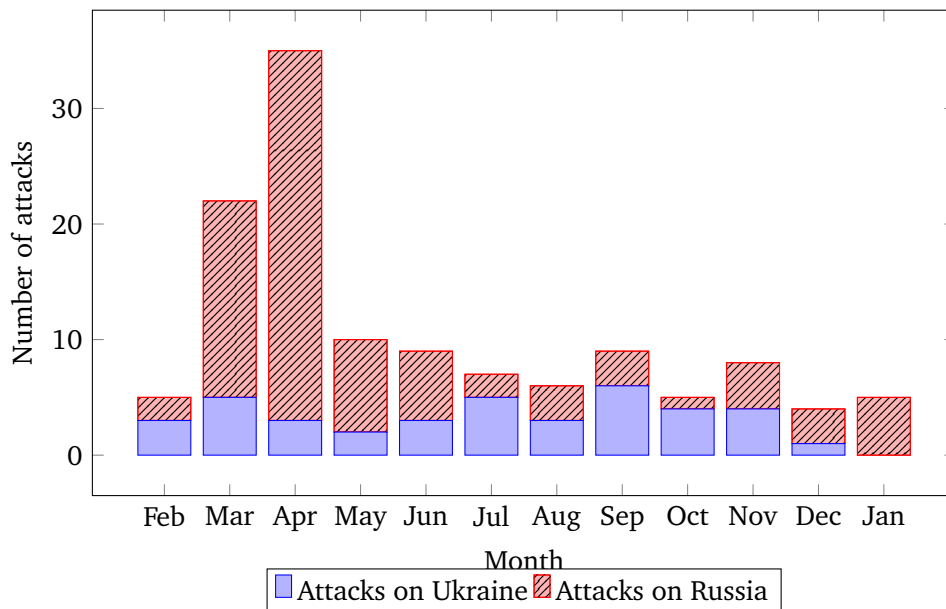


Figure 6.2: Cognitive attacks per month between Feb 2022 - Feb 2023 [78]

6.2.3 Destructive

Figure 6.3 shows the division of destructive attacks per side. The graph shows a massive amount of attacks during the outbreak of the war.

We could not locate any sources of any physical harm to either people or Operational Technology (OT) by destructive cyberattacks in Ukraine.

Our results show that there are very few destructive attacks against Russia, and none at all from July of 2022 through January of 2023.

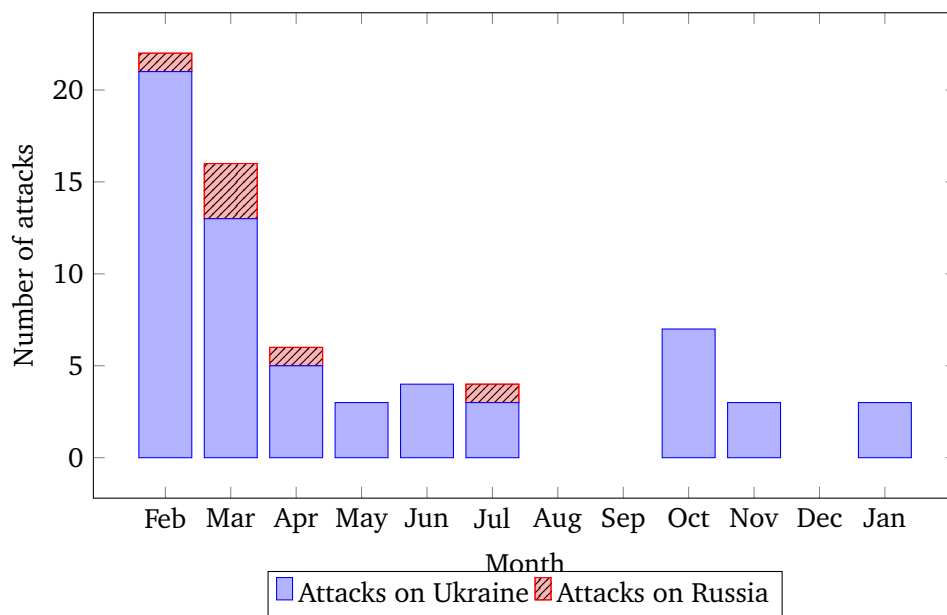


Figure 6.3: Destructive attacks per month between Feb 2022 - Feb 2023 [45]
[78]

6.2.4 Disruptive

Disruptive attacks aim to disrupt the target's operations.

During the course of this conflict, observations show that this is usually performed by launching a DDoS attack. These attacks attempt to flood the targeted system with false requests, thus overloading it and rendering the system inoperable.

In the following figure 6.4, one can observe the full amount of registered disruptive attacks. From this data, one can see that the amount of attacks experienced a sharp increase during the summer of 2022, and then another spike in November, before falling to levels observed earlier in the conflict. From figure 6.1 one can see that the majority of attacks from the beginning of the large-scale conflict, to the end of our set scope, are of a disruptive nature.

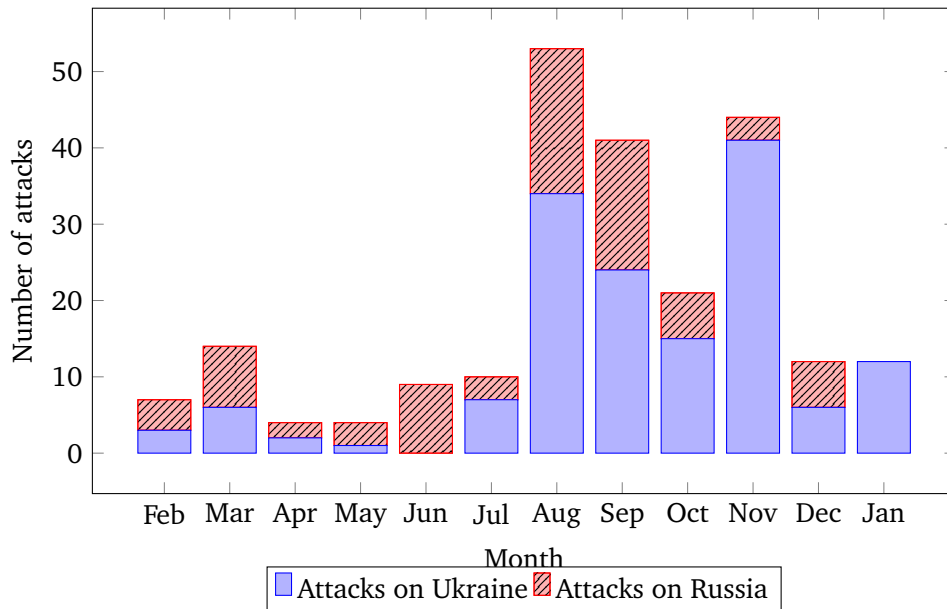


Figure 6.4: Disruptive attacks per month between Feb 2022 - Feb 2023 [78]

6.2.5 Reconnaissance

In this section we are going to explore some of the reconnaissance methods used in the war.

The group was unable to find any reported reconnaissance cyberattacks during our research. This is most likely due to the secrecy surrounding intelligence gathering. Therefore this chapter will not contain any numbers on attacks, but rather be a discussion on what cyberattacks can be seen as possible reconnaissance attacks.

Below are some of the disciplines of reconnaissance which are used in warfare.

- signals intelligence (SIGINT) is the action of intercepting and analysing electronic signals and communication. This may give insight into the enemy's intentions and location. This information may be gathered from: radar, foreign communications and other electronic systems [82].
- open-source intelligence (OSINT) is defined as intelligence gained by collecting, evaluating and analyzing publicly available information. Sources for such information might be from sources such as: news media, public records, social media platforms and more [83].
- human intelligence (HUMINT) is gathering intelligence from human sources, rather than technical means. This is usually provided by covert agents and informants. HUMINT usually gathers political, scientific, or technical intelligence [84] [4].

One type of reconnaissance Russia is known to do is testing neighboring countries' military responses and response times. One way that this is done is by flying military aircraft along NATO airspace. By doing this they trigger the NATO Quick Reaction Alert (QRA), and measure the time and the force of the response [85] [86].

If one looks at the aforementioned reconnaissance method in cyberspace, earlier attacks could be used to gain intelligence on Ukrainian responses and remediation time. With this knowledge an attacker can estimate the capabilities and estimated response times of their target. Cyberattacks also have the possibility of revealing other weaknesses that an attacker can use in a later operation.

The following major cyberattacks can be characterised as reconnaissance:

- **BlackEnergy:** Was a malware attack on the Ukrainian power grid, resulting in power outages in December 2015. The attackers used the malware to infiltrate the Ukrainian systems to gather information and take control. This attack has been attributed to Russian backed hackers [28] [87].
- **NotPetya:** In June 2017 the world was struck by the *NotPetya* malware. While the primary target for *NotPetya* was Ukraine, which was hit hard, it also spread across the world. While looking like typical ransomware, *NotPetya* reportedly had no way of decryption, making it a purely destructive malware; aka a *wiper* [46] [88].
- **WhisperGate:** In January 2022, Ukrainian government systems were the target of the *WhisperGate* wiper. The malware deleted selected file extensions, and manipulated the Master Boot Record to render systems inoperable [35].

All the aforementioned attacks have been attributed to Russian linked threat actors. Both *BlackEnergy* and *NotPetya* are attributed to Unit 74455 of the GRU. This group is also known as Sandworm, and has been reported as active since at least 2009 [89][35].

As in most conflicts, reconnaissance has been an important aspect of the Russo-Ukrainian war. Both sides use a wide variety of methods to gather information on their adversaries, be it OSINT, HUMINT, SIGINT or other methods not covered in this thesis. While not explicitly confirmed, NATO has stated that they are providing Ukraine with non-lethal military assistance. We assume that this is assistance in reconnaissance in both physical forms and in cyberspace [20].

The lessons learned from the Russo-Ukrainian war will influence future defence strategies both on the physical- and the digital-plane. Experience gained from how Russian threat actors have mapped out systems, often years before an attack, could lead to actors in the field of cybersecurity being more alert for activity that might be reconnaissance for future offensive operations.

6.3 Attribution

This section aims to answer the research question:

"Can any of the documented attacks be attributed to known threat actors? If so, which?"

We can see that many known threat actors are active in the Russo-Ukrainian war. Below is a table containing an overview of the active threat actors and known examples of attributed attacks.

Name	Prominent attack method	Russian state affiliation	Known attacks
IRIDIUM (Sandworm)	Destructive wiper attacks	GRU	-FoxBlade -Industroyer2(5.4) -CaddyWiper(5.5) -Prestige(5.10)
DEV-0586	Destructive wiper attacks	Unknown	-WhisperGate(5.1)
KRYPTON (Turla)	Disruptive malware distribution	FSB	-Hactivist Android malware (5.7)
ACTINIUM (Gamaredon)	Phishing & Malware	FSB	-Malware and phishing campaigns(5.11)
STRONTIUM (APT28/Fancy Bear)	Destructive	GRU	-Vinnitsia government compromise(2.9)
UNC4166	Destructive (Reconnaissance)	Unknown	-Trojanised Windows 10 installers(5.12)

Table 6.2: Known Threat Actor Overview

We also want to show the active hacktivist groups. The table below presents the known hacktivist groups which have performed a significant amount of registered disruptive attacks.

Name	Prominent attack method	Affiliation
IT Army of Ukraine	Disruptive DDoS attacks	Ukrainian
Anonymous	Disruptive hacking	pro-Ukrainian
CyberPalyanitsa	Disruptive DDoS attacks	Ukrainian
People's CyberArmy	Disruptive DDoS attacks	Russian
NoName057(16)	Disruptive DDoS attacks	pro-Russian
Anonymous Russia	Disruptive DDoS attacks	pro-Russian
Killnet	Disruptive DDoS attacks	pro-Russian

Table 6.3: Known Hacktivist Overview

There are other small, active hacktivist groups. However, these groups are attributed to very few attacks and are therefore left out of the table. Almost all of these attacks are DDoS attacks towards organisation's websites.

Notably, we also see that there has been a split in Anonymous, with the pro-Russian Anonymous members having split into Anonymous Russia.

6.4 Impact of cyberattacks

This section aims to answer the research question:

"Has there been any significant impact from any cyberattacks performed in the war? If so, which attacks and why?"

It is difficult to gauge the impact of cyberattacks in this war. Disruptive DDoS attacks, which make up the majority of the documented cyberattacks, are generally low-impact attacks. They serve little to no purpose other than to disrupt an organisation's website or service. However, we could make the claim that these attacks send a political message, demonstrating that the targeted organisations are important to the ongoing war. Additionally, these disruptions prevent people from getting vital information from these channels.

On the other hand, we see more significant consequences from the destructive wiper attacks performed by more sophisticated threat actors. These attacks target computer- & network systems and critical infrastructure, which prompts a response from the affected organisations. If these systems are left unrestored, it could lead to disruptions in crucial communication and command systems, and critical services such as energy suppliers, internet services & communications channels, and credible national news channels. Ukrainian organisations targeted by such attacks have to perform restoration on the targeted systems in order to prevent such disruptions.

The attacks which have created significant impact in the war are:

- WhisperGate
- FoxBlade
- HermeticWiper/CaddyWiper
- Industroyer2
- Prestige

One also has to take note of the impact from cognitive attacks. These attacks are purposely designed and performed to be spread in and by the media, and to play a cognitive effect on the population. One such major attack which we could state that has had an impact is the Zelenskyy deepfake as shown in section 5.2.1.

The intended effect of such an operation, the spreading of disinformation through online media, would likely be to influence both Ukrainian and Russian citizens who came across it. However, the Zelenskyy deepfake was very quickly refuted by government officials, even by Zelenskyy himself [76], before it was able to sow any significant confusion and disruption in the populace. One may argue that this could mean that the impact was minimal or negligible all things considered. However, the refutation and correction from Ukrainian officials might not have been

spread as well as the deepfake by some media, thus perhaps still leading to moderate success and propaganda value for the perpetrators.

It is also important to address the political and psychosocial effect of the Rasmus Paludan Quran burning. This event is not a regular cyberattack, however it utilised online media and by extent the cyberdomain to create the intended effect. The intended effect was to cause discourse in online media and create political tension between Sweden and Turkey, and thus disrupt both Sweden and Finland's NATO membership application ratification. The protest was organised by a pro-Russian journalist, Chang Frick, thus the reason we are classifying this influence operation as a Russian cyberoperation.

At the same time, multiple hacktivist groups are conducting massive amounts of disruptive attacks throughout the war, as discussed in section 6.3. However, we do recognise that these attacks are significantly less impactful than the destructive and cognitive attacks.

This is due to the simple reason that there are no lasting effects from a service disruption. A public-facing website which is disrupted for some hours does not have a significant impact on the war. An organisation who has been the target of a disruptive attack will notify the public of their service disruption and then quickly resolve the issue.

6.4.1 Battlefield impact

This subsection will answer the research question:

"Have these attacks made any significant impact on the battlefield, or is the impact solely limited to communications- and other critical-infrastructure?"

We believe the best use of cyberattacks in a modern conflict is in combination with other types of offensive operations; whether it be electronic warfare, precision-guided weapons or disinformation campaigns. The goal of cyberattacks in this approach should be to degrade the adversary's informational advantage and communication systems. Cyberattacks can also be used to create turmoil within the population by disrupting the energy sector, finance, transportation, and other central government services.

Despite its usefulness for espionage and criminal activity, cyberattacks alone are not sufficient to ensure victory in an armed conflict. After the first few weeks of invasion, with a large amount of targeted destructive attacks, the Russian cyberattacks started to seem uncoordinated and sporadic in fashion. In addition to the state sponsored APT groups, hacktivist groups have done massive amounts of disruptive attacks on both sides of the war. A list of some of the hacktivist groups can be seen in table 6.3. The hacktivist groups seem to primarily target non-military websites and services [90] [7].

To directly answer the question, we are unable to find concrete evidence of any significant impact to the armed forces on both sides due to cyberattacks. Simultaneously, our analysis of documented cyberattacks show that they have mostly targeted civilian infrastructure, and governmental communications.

6.5 Discussing the results

According to our findings, August was the month with the most amount of cyberattacks. Later during the same period, on the 21st of September 2022, towards the end of Q3 (5.2.3) Russia announced a further mobilisation of 300 000 troops [91].

These two facts could be put together, and perhaps serve as causation for the observation that we've made in the significant decrease in Russian cyberattacks after the mobilisation order. From August to September the amount of cyberattacks decreased by 18.9%, from 37 to 30 attacks.

Again, from September to October, we observe a further decrease by 13.3%, from 30 to 26 registered attacks.²

It is important to note that the majority of these attacks are disruptive attacks which are attributed to hacktivist organisations, and not advanced operations perpetrated by known APT groups or other serious actors.

Without making any definitive claim, we can suggest the theory that the Russian mobilisation could have contributed to a decrease in the amount of attacks performed by pro-Russian threat actors.

On the other hand, this decrease can also be theorised to be a result of the amount of time that sophisticated threat actors need to plan new attacks. We base this on the fact that none of the attacks performed in August and September are destructive attacks.

Another theory we would like to propose is the idea that the Russian government may have decided to concentrate their cyberattack efforts on one group, Sandworm. This theory stems from the fact that Sandworm has been the most active threat actor in the ongoing cyberwar, having performed a significantly higher number of destructive attacks than other identified threat actors. This observation suggests that the Russian government may have directed all of their available resources towards this particular group. Other threat actors may have been tasked with creating initial access vectors, which the Sandworm group could then use for launching more sophisticated destructive operations at a later time.

²Raw numerical data can be found in Appendix A.1.

Chapter 7

Discussion

This chapter will discuss all aspects of the group's work on this thesis. It will cover the entire work process from the start of the project period to completing the product. It will provide an overview of the choices the group has made, what the members have learned from the process, and what has deviated from the original plan.

Also discussed in this chapter are the group's thoughts on negative and positive aspects of the project and what could have been done differently.

7.1 Reflection on the thesis

This section covers our thoughts and reflections on our choice of subject for the thesis, as well as our experienced positive and negative sides to the project.

7.1.1 Thesis choice

Before the initiation of the last semester, a variety of prospective clients came to campus at NTNU in Gjøvik to present their tasks that they would provide for the students. One task in particular stood out as a likely candidate for our final choice. This task focused on a highly relevant, and ongoing, topic that the group already had been following individually beforehand; the war in Ukraine. Additionally, the task focused on the topic of cybersecurity, and with all group members studying Digital Infrastructure and Cybersecurity, the probability of selecting this task increased significantly.

Following the conclusion of the presentations, the group decided to initiate a conversation with the client responsible for our desired task. The group discussed the ongoing Russo-Ukrainian conflict, the background for the thesis, our thoughts,

and his expectations. Raymond Hagen, the client, met the group with mutual enthusiasm and it became apparent that him and the group would mutually benefit from working together on this task. After concluding the meeting, there was a dialogue within the group where it was decided that the task would be our primary choice.

7.1.2 Assessment of project strengths and weaknesses

Choosing this task gave us the opportunity to further research a conflict that we already found engaging, making it more motivating to work on than the other options available to us. Additionally, it provided the chance to research the first large scale conflict that makes use of both offensive and defensive cyberoperations, and analysing the cyberattacks that are part of the ongoing Russo-Ukrainian war. What we have written also aids in shining a light on a part of modern warfare, the cyberdomain, which is growing in importance, and gaining credibility and interest. Alongside the group's personal positives, the project also provides the possibility of our research and analysis being of use in further research by other academics and interested parties.

On the other hand, while the general experience of working on this project has been positive, there were some negative aspects that have affected, or hindered, progress. Due to the nature of the thesis being a literature study, there were often difficulties with finding good and reputable sources, resulting in more time spent on trying to identify usable sources instead of analysing information found or actually writing the thesis. While working on the project, avoiding scope creep also posed a challenge, since we often discovered recent interesting and useful data outside our scope that may have fit our research if we did not have to a set such a hard time limit. Additionally, we would at times start asking ourselves if we perhaps should write more on some specific subjects resulting in more research and analysing. At times, this did lead to us adding valuable content to our work, but we were otherwise aware of our constraints and avoided adding more to our workload.

An aspect to working on the subject of an ongoing conflict, has been objectivity. We wouldn't classify this as a negative, but we have had to focus more on it than we perhaps would have if we had chosen to research something else. All members have done their utmost to make sure that the conflict, research, analysis, and writing has been approached as objectively as possible.

7.2 Process and methods

Covering our methods used and progression for this project, this section also provides an overview of the group's decision making process and choices made.

7.2.1 Project process

As a group we started the process of planning our project early by completing a project plan as seen in Appendix C. This plan was fundamental and provided vital groundwork for our thesis as a whole. We covered subjects ranging from goals, scope, and organisation, to project phases and quality assurance. We followed our project plan and dedicated the first month of the project period to our planning phase. In addition to finalising the project plan, we wrote and signed a group contract and a standard agreement on execution of a student thesis in collaboration with an external part.

The next phase was our research phase, providing essential information crucial to our work. All group members searched for, and gathered, open-source information needed for our research. This was shared within the group within a dedicated text-channel for vetted relevant sources and resources, as well as an overview of our more central sources in an Excel-file. In addition to our own searching, we received guidance and information from our client and supervisor. It was during this phase that we attempted to gain high quality data and information from several serious actors in relevant fields as explained in section 3.3.5.

After gathering and sorting all of our resources, we began our final phase which we had titled the *Final report phase*. In this phase our work consisted of setting up the project file, determining formatting and sectioning, analysing our gathered information, as well as writing the actual thesis itself. Additionally, we had to perform some additional research during our analysis when presented with topics and themes that we had insufficient knowledge of and sources on.

The project file underwent several minor to more substantial changes during this period. As work on the project went forwards it was inevitable that the document would require modification, in the form of additional sections, merging of topics, and discarded sections & paragraphs.

During the final fortnight our focus was on finalising the last two chapters, *Discussion & Conclusion*, while also reviewing and editing the chapters that were written beforehand. As well as scrutinising our product, this time period also required dialogue with our supervisor and client to acquire feedback in order to improve upon the product and ensure the highest possible quality before submission.

7.2.2 Decisions and choices

Many of the choices we made relied on the requirements and preferences that the client had for the task and the process as a whole. This includes using the English language for writing the thesis, and using Microsoft Teams for communication and sharing files between both parties. These decisions were also beneficial for cooperating with the supervisor. The meeting hours were also dependant on when the client or supervisor were available, meaning that the specific meeting times that were decided on were also based on their preferences.

To maintain a professional and cohesive structure within the thesis, the group chose to follow standards that had been agreed upon internally. Therefore, the main working method was using Overleaf and writing in LaTeX. This allowed us to work on documents and made it simple to maintain structure throughout the whole product. The template used for this thesis is NTNU's standard thesis template.

Regarding the research itself, the framework that ended up being used is a modified version of the scientific method. Whereas the scientific method conventionally includes forming a hypothesis, this was disregarded in our modified framework. As mentioned before, this framework aimed to set a clear structure to be followed, making it more cohesive.

For citations, the choice was initially to use the APA 7th style, however upon beginning to write the thesis the group discovered that referencing within the text would quickly become tedious. Therefore, the citation style was changed to the numeric style so as to make it easier for the group to utilise correct citation, improve reading experience, and to make it easy to verify & check our sources. This style was also recommended in a seminar on report writing that we participated in.

Several of the choices were also made for the group's benefit regarding convenience and accessibility for all members. For communication, Discord was mainly used between the group members, as everyone had already been using it prior to starting work on the thesis. This allowed for simple and informal messaging, along with voice chat to be used in digital general work sessions.

For the digital weekly focus update meetings, Microsoft Teams would be used due to its convenience with setting up meetings, sending meeting notices, and using the calendar. Another feature of Microsoft Teams that was used was their storage, due to being reliable and easily available. Initially, the plan was also to use two apps on Teams called Milestones and Tasks, with each of them being used for what their name indicates.

These however, felt excessive to use, as tasks would be planned and delegated spontaneously while communicating, or within the Overleaf project by utilising the built-in comment function.

At the same time, the milestones in Teams were rendered redundant with the use of a Gantt-chart. The group attempted to follow the Gantt-chart shown on page 20 of the Project plan included in Appendix C, however some of the milestones exceeded the initially allotted time. Therefore, we have produced an updated Gantt-chart that better reflects our progress throughout the project period, which can be found in section 7.4.3.

Regarding working locations, the plan that was initially established was a hybrid solution with two hybrid workdays, Mondays and Fridays, where members could work from home, and three workdays physically on campus. During the first two months, the group followed the original plan, however over time it became harder to keep to it as external factors such as injuries, illnesses and other disrupting events occurred. This resulted in an increase in working from home and cooperating digitally, however this did not negatively affect the overall progress on the project. This is likely a result of the group members having experience working together online.

The work hours that were set while working on the project plan were 09:00 through 16:00 from Monday to Thursday, and 09:00 through 12:00 on Fridays. The group followed the original plan in the beginning, however as time passed we realised that we had estimated an excessive amount of hours when comparing the state of the thesis to the time left on the project. The routine of starting work at 09:00 was followed throughout the whole project period, however the time that we ended our workdays changed based on the circumstances. The hours that the group spent on the project were logged using [Toggl](#), which we experienced to be a convenient and simple website used for logging work hours. More information on the time used on this project can be found in section 7.4.4.

7.3 Interpersonal cooperation

This section provides an overview on how we experienced working together as a group during the project period. Additionally, it covers dialogue and cooperation with both our client, or task giver, as well as the group's supervisor, Erjon Zoto.

7.3.1 Teamwork

During this project, each member has focused on good communication, honesty, trust, and the support of each other. These actions and qualities have ensured that each member has been able to work on the project and contribute to the best of their ability. Additionally, we made sure to produce a group contract in order to establish a baseline, as well as serve as a guarantee in case of unforeseen interpersonal conflicts.

Working together as a group has been straightforward and uncomplicated, largely due to the members having worked together on other large projects during our time at NTNU. Whenever something took place that rendered a group member unable to work on the project, this was accepted by the rest as long as the need for absence was communicated properly. The absence of any members didn't end up seriously hindering progress due to good planning, delegation of tasks, and everyone making up for any time lost.

During this time period, we have endeavoured to keep an optimistic view on the project course. Any setbacks have been met with a determined response to move forward and learn from any mistakes, while continuously working towards a high quality end product.

7.3.2 Collaboration with client

The primary goal and focus of our weekly meetings with our client, Raymond Hagen, was to provide him with updates on our work, while also acting as an arena for open discussion between all participants. Simultaneously, these meetings were used by Hagen to support our work in the form of sharing information gathered by himself, as well as giving constructive criticism and positive feedback.

In this way, one could almost say that Hagen has functioned not only as an attentive and involved client, but also as a form of supervisor. He has presented himself as an optimist when regarding our work on this project, and has wholeheartedly supported the group throughout this endeavour, always open to our ideas and understanding of any shortcomings.

In addition to our weekly meetings, a Teams workspace was created to host said meetings, share files, and send updates, already in November 2022. This virtual space has served as a low-threshold platform for communication between us and Hagen, and has provided an easy channel for planning and information sharing.

Meeting minutes are provided in Appendix D for more in-depth information on what has been discussed and worked on with the client.

7.3.3 Supervision

During this project period our group has had a total of seven meetings with our supervisor Erjon Zoto. The goal of these meetings was to provide Zoto updates on our work, create an arena where we could ask for guidance on specific subjects, and where we could receive direct feedback on our work & progress.

While working on our product, we always made sure to keep our minds open and display a willingness to consider all of Zoto's proposals, while still working independently and making own choices based on the knowledge we had and any information provided. While we did not always implement all of the feedback we received, we made a point of carefully considering it and using it to inform our decisions. All feedback received, implemented or not, has been greatly appreciated.

The relatively low number of meetings with our supervisor is in part due to the aforementioned working relationship with our client and his supervision on subjects relating to our research and analysis. Our requests for feedback from Zoto were usually limited to formatting, administrative issues, and the addition or removal of content. Simultaneously, Zoto has several times provided applicable feedback on other topics than what we usually requested.

7.4 Outcome

This section will reflect upon the thesis' findings and potentials for improvement. Also discussed in this section are the achievement of goals that we set out to accomplish, as well as feedback received from our client.

7.4.1 Possible improvement

We believe we could have improved our work by starting on the written parts of the thesis earlier, during our research. This would have given us better short term goals such as finishing chapter 4 at an earlier date. At the same time, we should have also divided the research better and made sure that multiple group members were not researching the same topics simultaneously.

Regarding our research, we should have put more effort into trying to find sources on possible Ukrainian cyberattacks towards their adversaries. Additionally, we should have tried to provide an overview of possible active pro-Ukrainian threat actors located in countries other than Russia or Ukraine, and cyberattacks perpetrated by them.

7.4.2 Academic contribution of our work

As stated in table 1.1, our effect goal was to provide the client with a thesis that could be used for further research. In addition to providing a foundation for the client's further research, it could also be used by other academically inclined individuals interested in researching the topics covered in this thesis. Due to the fact that the conflict is still ongoing¹ and how relevant it is regarding geopolitics, cybersecurity, and defense, this thesis could provide a well written and reputable source for persons needing such a product for their own research or other work.

¹As of May 2023.

7.4.3 Updated Gantt-chart

Included in our project plan found in Appendix C, is our original Gantt-chart which we created during the planning phase. We were mostly able to follow this plan, but ended up with a few deviations. Our updated Gantt chart with our actual milestones can be seen in the following figure.

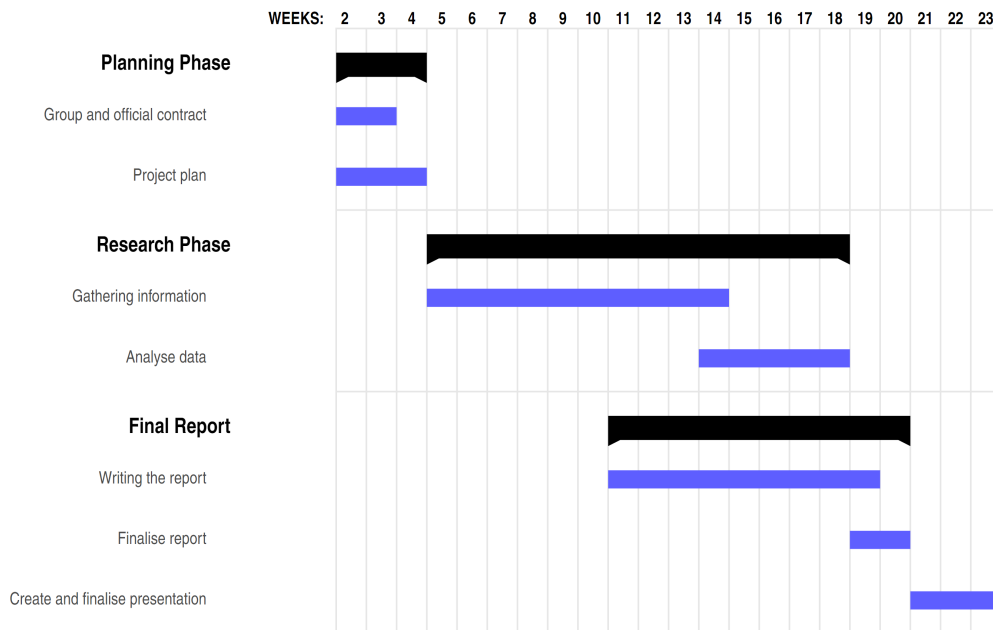


Figure 7.1: Updated Gantt-chart

To summarise:

- Spent two more weeks than planned on the *Analyse data* part of the research phase.
- Ended the *Writing the report* milestone two weeks earlier.
- Finalisation of the report has been shortened to two weeks rather than three.
- The *Presentation* milestone has been extended by one week

7.4.4 Time analysis

According to logged hours, our work on the project started on the 11th of January 2023. Work on the main product, the thesis, started at the same time, and was concluded by the 22nd of May. The project period itself will continue until the 7th of June, with that period consisting of preparing the presentation, as well as the presentation itself.

As discussed in section 7.2.2, the group's original plan was to work an average of 124 hours per week. This was because NTNU recommended about 30 work hours per group member each week to ensure project completion.

During the final days of writing, the total number of logged work hours was 1505 hours distributed over a 19 week project period. This leads to the following out-takes:

- An average of approximately 79 work hours per week.²
- Thus, approximately 20 hours per week per group member.³
- Meaning 4 hours spent on this project per day per member.⁴

This, of course, is less time than what has been recommended, and without context could minimise the credibility of our work. Thus one must take into consideration the different circumstances that give a more truthful account of the time spent on this project.

Some circumstances that have made an impact on our work include working on the mandatory subject IØ2000, which by seminar- and project days alone shaves off over a week from the total project period. Additionally group members have had many personal events taking up valuable time, such as working next to their studies, other subjects, volunteer work, and health issues – which have led to a lot of absence. At the same time, the group has been positive to members taking time off for other activities, as long as there was sufficient progress on the project.

When taking this into account, one ends up with an effective project period of roughly 14 work weeks without significant disruption from other activities or events. This leads to the following outtakes based on updated data:

- An average of approximately 108 work hours per week.
- Thus, approximately 27 hours per week per group member.
- Meaning 5.5 hours spent on this project per day per member.

All things considered, the high quality of the end product more than makes up for the relatively low amount of logged hours. Additionally, this data shows how effectively the group has worked together.

²1505 hours divided by 19 weeks = 78.68 hours.

³78.68 weekly hours divided by 4 members = 19.71 hours.

⁴19.71 hours divided by 5 work days per week = 3.94 hours.

While logging hours, the use of tags in Toggl made it possible for us to easily link our logged hours to specific categories, where the main ones used were *general work*, *research*, and *meeting*. Additional tags used were *admin*, *seminar*, and *other*, though these were rarely used as activities most often fell into the three main categories.

A review of how the logged time has been tagged and sorted does not lead to any surprises regarding distribution of time spent on different activities. About 72% of the time spent on this project has been tagged as *general work*, which means normal work on the project such as writing and quality control. The second largest category, at 17%, is *research*. This is time spent on gathering information and researching sources. The remaining time has been spent on different meetings and other activities.

Additional data, including graphs, can be found in Appendix A.2.

7.5 Further work

Further work would include an in-depth analysis of each cyberattack. This would require a lot more time than we had available, but would likely yield interesting data. This is however not the main thesis task, but would be interesting and enlightening to perform.

We would also like to have had more correspondence with cybersecurity firms and other relevant entities. This could have allowed us to have more high-quality data to work with, and to craft even better theories based on said data.

We could also have had a more technological view on the attacks, providing insight into how an attack fits into the different steps of the Cyber Kill Chain and how each attack specifically utilises a method. This way, we could analyse each attack from an Incident Response point-of-view.

Our scope has also hindered us from analysing and discussing the more recent cyberactivities in the conflict, as discussed in section 7.1.2. This in turn meant that whenever new attacks which were interesting occurred, we could not include them in our thesis.

If we were to continue the research, we would delve deeper into hacktivists and their impact. This would give us a deeper understanding of such groups and the threat they pose in modern conflicts.

Chapter 8

Conclusion

The task that we set out to achieve was to analyse the cyberattacks performed throughout the first year of the Russo-Ukrainian war, by both sides, and document which methods were used in these attacks. We believe that we have thoroughly performed this task to the best of our abilities given the nature of the conflict and available information.

To perform the needed research, we used open-source information from reputable sources to get an overview of the cyberattacks which had been performed during our chosen scope.

Our product shows that we have documented the methods used in cyberattacks performed throughout the first year of the war. Every registered attack performed during the first year of the war, after analysing, has been categorised into one of the following four categories; Destructive, Cognitive, Disruptive or Reconnaissance.

Furthermore, we have also achieved answers to most of the research questions that we set out to answer. The answers to these questions were a result of our research and analysis, and could be seen as a by-product of our work which we have easily managed to wrap into the project as a whole.

In conclusion, the group believes that we have managed to achieve a high-quality thesis which has directly answered the task we set out to accomplish.

Bibliography

- [1] CSRC. *advanced persistent threat*. [Online; accessed 25. Apr. 2023]. 25th Apr. 2023. URL: https://csrc.nist.gov/glossary/term/advanced_persistent_threat (visited on 25/04/2023).
- [2] Library. *Grey literature*. [Online; accessed 27. Apr. 2023]. 27th Apr. 2023. URL: https://library.leeds.ac.uk/info/1110/resource_guides/7/grey_literature (visited on 27/04/2023).
- [3] jnguyen. 'What is Hactivism?' In: *Check Point Software* (11th May 2022). URL: <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-hactivism> (visited on 13/04/2023).
- [4] *What is Intelligence?* [Online; accessed 1. May 2023]. 30th Apr. 2023. URL: <https://www.dni.gov/index.php/what-we-do/what-is-intelligence> (visited on 01/05/2023).
- [5] Palo Alto Networks. *Malware | What is Malware & How to Stay Protected from Malware Attacks*. 2023. URL: <https://www.paloaltonetworks.com/cyberpedia/what-is-malware> (visited on 11/05/2023).
- [6] *What is Phishing? | Microsoft Security*. [Online; accessed 20. Apr. 2023]. 20th Apr. 2023. URL: <https://www.microsoft.com/en-us/security/business/security-101/what-is-phishing> (visited on 20/04/2023).
- [7] James Andrew Lewis. *Cyber War and Ukraine*. 16th June 2022. URL: <https://www.csis.org/analysis/cyber-war-and-ukraine> (visited on 20/03/2023).
- [8] M. Bassin, S. Glebov and M. Laruelle. *Between Europe and Asia*. Pittsburgh, PA, USA: University of Pittsburgh Press, 2015. ISBN: 978-0-82298091-9. URL: https://books.google.no/books?id=333lCQAAQBAJ&pg=PT135&redir_esc=y#v=onepage&q&f=false (visited on 19/05/2023).
- [9] BBC News. *Ukraine crisis: Timeline*. 14th Nov. 2014. URL: <https://www.bbc.com/news/world-middle-east-26248275> (visited on 13/03/2023).
- [10] Vladimir Putin. *On conducting a special military operation*. 24th Feb. 2022. URL: https://en.wikipedia.org/wiki/On_conducting_a_special_military_operation (visited on 26/02/2023).

- [11] Luciana B. Sollaci and Mauricio G. Pereira. 'The introduction, methods, results, and discussion (IMRAD) structure: a fifty-year survey'. In: *J. Med. Libr. Assoc.* 92.3 (July 2004), p. 364. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC442179> (visited on 20/03/2023).
- [12] *Soviet Union*. [Online; accessed 18. Apr. 2023]. 31st Mar. 2023. URL: <https://www.britannica.com/place/Soviet-Union> (visited on 18/04/2023).
- [13] Michael Ray. 'Why Did the Soviet Union Collapse?' In: *Encyclopedia Britannica* (). URL: <https://www.britannica.com/story/why-did-the-soviet-union-collapse> (visited on 18/04/2023).
- [14] *The Maidan protest movement*. [Online; accessed 20. Apr. 2023]. URL: <https://www.britannica.com/place/Ukraine/The-Maidan-protest-movement> (visited on 20/04/2023).
- [15] *The crisis in Crimea and eastern Ukraine*. [Online; accessed 20. Apr. 2023]. URL: <https://www.britannica.com/place/Ukraine/The-crisis-in-Crimea-and-eastern-Ukraine> (visited on 20/04/2023).
- [16] *General Assembly Adopts Resolution Calling upon States Not to Recognize Changes in Status of Crimea Region*. [Online; accessed 20. Apr. 2023]. 27th Mar. 2014. URL: <https://press.un.org/en/2014/gall493.doc.htm> (visited on 20/04/2023).
- [17] Andrew Katell. 'Putin's Ukraine gamble seen as biggest threat to his rule'. In: *AP NEWS* (20th Feb. 2023). URL: <https://apnews.com/article/russia-ukraine-war-putin-one-year-anniversary-df699dc348444c878bb4041158ccb84c> (visited on 22/03/2023).
- [18] *U.S. Relations With Ukraine*. [Online; accessed 20. Apr. 2023]. 27th Aug. 2021. URL: <https://www.state.gov/u-s-relations-with-ukraine/> (visited on 20/04/2023).
- [19] *EU relations with Ukraine*. [Online; accessed 20. Apr. 2023]. 9th Feb. 2023. URL: <https://www.consilium.europa.eu/en/policies/eastern-partnership/ukraine/> (visited on 20/04/2023).
- [20] *Relations with Ukraine*. [Online; accessed 20. Apr. 2023]. 4th Apr. 2023. URL: https://www.nato.int/cps/en/natohq/topics_37750.htm (visited on 20/04/2023).
- [21] *Ukraine's Euromaidan Revolution*. 17th Jan. 2022. URL: https://jisis.washington.edu/wordpress/wp-content/uploads/2018/02/Ukraine_Euromaidan_CCP_ii.pdf (visited on 23/03/2023).
- [22] By Reality Check Team. 'Ukraine war: President Putin speech fact-checked'. In: *BBC News* (21st Feb. 2023). URL: <https://www.bbc.com/news/64718139> (visited on 22/03/2023).
- [23] *Article by Vladimir Putin "On the Historical Unity of Russians and Ukrainians"*. 12th June 2021. URL: <http://en.kremlin.ru/events/president/news/66181> (visited on 22/03/2023).

- [24] Jeffrey Mankoff. *Russia's War in Ukraine: Identity, History, and Conflict*. 22nd Apr. 2022. URL: <https://www.csis.org/analysis/russias-war-ukraine-identity-history-and-conflict> (visited on 22/03/2023).
- [25] Sandra Knispel. 'Fact-checking Putin's claims that Ukraine and Russia are 'one people''. In: *News Center* (22nd Feb. 2023). URL: <https://www.rochester.edu/newscenter/ukraine-history-fact-checking-putin-513812> (visited on 22/03/2023).
- [26] *The UN and the war in Ukraine: key information*. [Online; accessed 20. Apr. 2023]. 14th Apr. 2023. URL: <https://news.un.org/en/focus/ukraine> (visited on 20/04/2023).
- [27] *Russia Cyber Threat Overview and Advisories | CISA*. [Online; accessed 25. Apr. 2023]. 25th Apr. 2023. URL: <https://www.cisa.gov/russia> (visited on 25/04/2023).
- [28] Kim Zetter. *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*. 3rd Mar. 2016. URL: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> (visited on 13/03/2023).
- [29] Andy Greenberg. 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History'. In: *WIRED* (22nd Aug. 2018). URL: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world> (visited on 23/03/2023).
- [30] United States Department of Justice. *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace: Unsealed Indictment*. 15th Oct. 2020. URL: <https://www.justice.gov/opa/press-release/file/1328521/download> (visited on 23/03/2023).
- [31] Mark Dr. Galeotti. *Russian intelligence is at (political) war*. 12th May 2017. URL: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-116a> (visited on 03/05/2023).
- [32] Robert W. Pringle. 'Federal Security Service - Russian government agency'. In: *Encyclopedia Britannica* (27th Apr. 2023). URL: <https://www.britannica.com/story/why-did-the-soviet-union-collapse> (visited on 03/05/2023).
- [33] FBI CISA and DHS. *Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders*. 26th Apr. 2021. URL: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-116a> (visited on 03/05/2023).
- [34] Andrew S. Bowen. *Russian Military Intelligence: Background and Issues for Congress*. 15th Nov. 2021. URL: <https://sgp.fas.org/crs/intel/R46616.pdf> (visited on 03/05/2023).
- [35] *An overview of Russia's cyberattack activity in Ukraine*. [Online; accessed 3. May 2023]. 27th Apr. 2022. URL: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd> (visited on 03/05/2023).

- [36] Dan Sabbagh. 'Cyber-attacks have tripled in past year, says Ukraine's cybersecurity agency'. In: *the Guardian* (19th Jan. 2023). URL: <https://www.theguardian.com/world/2023/jan/19/cyber-attacks-have-tripled-in-past-year-says-ukraine-cybersecurity-agency> (visited on 13/04/2023).
- [37] *Cyber Kill Chain*®. [Online; accessed 12. Apr. 2023]. 6th Feb. 2023. URL: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html> (visited on 12/04/2023).
- [38] Paul Pols. *The Unified Kill Chain*. [Online; accessed 12. Apr. 2023]. 7th Apr. 2023. URL: <https://www.unifiedkillchain.com> (visited on 12/04/2023).
- [39] Check Point Research Team. 'Hactivism in the Russia-Ukraine War - Check Point Software'. In: *Check Point Software* (6th Mar. 2022). URL: <https://blog.checkpoint.com/security/hactivism-in-the-russia-ukraine-war-questionable-claims-and-credits-war> (visited on 13/04/2023).
- [40] Johns Hopkins University & Imperial College London. 'NATO Review - Countering cognitive warfare: awareness and resilience'. In: *NATO Review* (20th May 2021). URL: <https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html> (visited on 19/04/2023).
- [41] *The threat of destructive cyber attacks*. [Online; accessed 24. Apr. 2023]. 18th June 2021. URL: <https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/the-threat-of-destructive-cyber-attacks.pdf> (visited on 24/04/2023).
- [42] *What is Stuxnet? | Malwarebytes*. [Online; accessed 24. Apr. 2023]. 24th Apr. 2023. URL: <https://www.malwarebytes.com/stuxnet> (visited on 24/04/2023).
- [43] Chris Odogwu. 'What Are Reconnaissance Attacks and How Do They Work?' In: *MUO* (22nd Mar. 2023). URL: <https://www.makeuseof.com/what-are-reconnaissance-attacks-and-how-do-they-work> (visited on 25/04/2023).
- [44] *Defending Ukraine: Early Lessons from the Cyber War - Microsoft On the Issues*. [Online; accessed 20. Apr. 2023]. 22nd June 2022. URL: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50K0K> (visited on 20/04/2023).
- [45] *A year of Russian hybrid warfare in Ukraine*. 15th Mar. 2023. URL: https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf (visited on 22/03/2023).
- [46] BBC News. *Global ransomware attack causes turmoil*. 28th June 2017. URL: <https://www.bbc.com/news/technology-40416611> (visited on 13/03/2023).

- [47] GReAT (Global Research and Analysis Team). 'Schroedinger's Pet(ya)'. In: *Securelist by Kaspersky* (27th June 2017). URL: <https://securelist.com/schroedingers-petya/78870> (visited on 14/04/2023).
- [48] Anton Ivanov and Orkhan Mamedov. 'ExPetr/Petya/NotPetya is a Wiper, Not Ransomware'. In: *Securelist by Kaspersky* (28th June 2017). URL: <https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902> (visited on 14/04/2023).
- [49] *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*. [Online; accessed 14. Apr. 2023]. 9th Oct. 2020. URL: <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and> (visited on 14/04/2023).
- [50] Morgan Chalfant. 'NATO chief says cyberattack could trigger collective defense'. In: *Hill* (28th June 2017). URL: <https://thehill.com/policy/cybersecurity/339851-nato-chief-says-cyberattack-could-trigger-collective-defense> (visited on 14/04/2023).
- [51] Alex Hern. "'NotPetya' malware attacks could warrant retaliation, says Nato affiliated-researcher". In: *the Guardian* (6th July 2017). URL: <https://www.theguardian.com/technology/2017/jul/03/notpetya-malware-attacks-ukraine-warrant-retaliation-nato-researcher-tomas-minarik> (visited on 14/04/2023).
- [52] *NATO agrees master plan to deter growing Russian threat*. [Online; accessed 14. Apr. 2023]. 21st Oct. 2021. URL: <https://www.reuters.com/world/europe/nato-agree-master-plan-deter-growing-russian-threat-diplomats-say-2021-10-21> (visited on 14/04/2023).
- [53] Harriet Salem, Shaun Walker and Oksana Grytsenko. *Russia puts military on high alert as Crimea protests leave one man dead*. 26th Feb. 2014. URL: <https://www.theguardian.com/world/2014/feb/26/ukraine-new-leader-disbands-riot-police-crimea-separatism> (visited on 13/03/2023).
- [54] Charlie D'Agata. *Ukrainian city of Donetsk epitomizes country's crisis*. 6th Mar. 2014. URL: <https://www.cbsnews.com/news/ukrainian-city-of-donetsk-epitomizes-countrys-crisis/> (visited on 13/03/2023).
- [55] Shane Huntley. 'Fog of war: how the Ukraine conflict transformed the cyber threat landscape'. In: *Google* (16th Feb. 2023). URL: <https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape> (visited on 20/04/2023).
- [56] CISA, FBI and NSA. *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure*. 11th Jan. 2022. URL: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-011a> (visited on 02/03/2023).

- [57] ESET Research. *IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine*. 1st Mar. 2022. URL: <https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/> (visited on 06/03/2023).
- [58] Lorenzo Franceschi-Bicchierai. *Russian Government Websites Are Currently Down*. [Online; accessed 20. Apr. 2023]. 24th Feb. 2022. URL: <https://www.vice.com/en/article/bvnpnv/russian-government-websites-are-currently-down> (visited on 20/04/2023).
- [59] Mark Kleinman. 'Satellite giant Viasat probes suspected broadband cyber-attack amid Russia fears'. In: *Sky News* (28th Feb. 2022). URL: <https://news.sky.com/story/satellite-giant-viasat-probes-suspected-broadband-cyberattack-amid-russia-fears-12554004> (visited on 20/04/2023).
- [60] Jakub Przetacznik and Simona Tarpova. [Online; accessed 1. Feb. 2023]. 21st June 2022. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI\(2022\)733549_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf) (visited on 01/02/2023).
- [61] By Jane Wakefield. 'Deepfake presidents used in Russia-Ukraine war'. In: *BBC News* (18th Mar. 2022). URL: <https://www.bbc.com/news/technology-60780142> (visited on 19/04/2023).
- [62] CERT-UA. 12th Apr. 2022. URL: <https://cert.gov.ua/article/39518> (visited on 27/03/2023).
- [63] 'Industroyer2: Industroyer reloaded | WeLiveSecurity'. In: *WeLiveSecurity* (12th Apr. 2022). [Online; accessed 20. Apr. 2023]. URL: <https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded> (visited on 20/04/2023).
- [64] Billy Leonard. 'Continued cyber activity in Eastern Europe observed by TAG'. In: *Google* (19th July 2022). URL: <https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag> (visited on 24/04/2023).
- [65] *United States and Ukraine Expand Cooperation on Cybersecurity* | CISA. [Online; accessed 24. Apr. 2023]. 27th July 2022. URL: <https://www.cisa.gov/news-events/news/united-states-and-ukraine-expand-cooperation-cybersecurity> (visited on 24/04/2023).
- [66] *WAR IN UKRAINE. PULSE OF CYBER DEFENSE*. [Online; accessed 24. Apr. 2023]. 27th July 2022. URL: https://mcusercontent.com/95750673b8ed58984406ae56e/files/7d7f51a6-661f-a608-41ff-7f0828cb0e58/SSSCIP_Weekly_Digest_2022_07_ENG.pdf (visited on 24/04/2023).
- [67] *Ukrainian Nuclear Operator Accuses Russians Hackers Of Attacking Its Website*. [Online; accessed 24. Apr. 2023]. 16th Aug. 2022. URL: <https://www.facebook.com/energoatom.ua/posts/479937337471385> (visited on 24/04/2023).

- [68] Minsifra. [Online; accessed 24. Apr. 2023]. 22nd Aug. 2022. URL: <https://t.me/mintsyfra/3343> (visited on 24/04/2023).
- [69] Ukrinform. 'Ukraine, Poland sign memorandum on cyber security cooperation'. In: *UkrInform* (22nd Aug. 2022). URL: <https://www.ukrinform.net/rubric-society/3555753-ukraine-poland-sign-memorandum-on-cyber-security-cooperation.html> (visited on 24/04/2023).
- [70] *Anonymous hacked Russian Yandex taxi app causing a massive traffic jam*. [Online; accessed 24. Apr. 2023]. 2nd Sept. 2022. URL: <https://www.hackread.com/anonymous-russian-yandex-taxi-app-hacked> (visited on 24/04/2023).
- [71] Microsoft Threat Intelligence. 'New "Prestige" ransomware impacts organizations in Ukraine and Poland - Microsoft Security Blog'. In: *Microsoft Security Blog* (10th Nov. 2022). URL: <https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland> (visited on 28/03/2023).
- [72] *CERT-UA Email distribution, allegedly on behalf of the State Special Communications (CERT-UA#5570)*. [Online; accessed 24. Apr. 2023]. 8th Nov. 2022. URL: <https://cert.gov.ua/article/2681855> (visited on 24/04/2023).
- [73] *Preparing for a Russian cyber offensive against Ukraine this winter - Microsoft On the Issues*. [Online; accessed 24. Apr. 2023]. 5th Dec. 2022. URL: <https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine> (visited on 24/04/2023).
- [74] *Trojanized Windows 10 Operating System Installers Targeted Ukrainian Government | Mandiant*. [Online; accessed 24. Apr. 2023]. 15th Dec. 2022. URL: <https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government> (visited on 24/04/2023).
- [75] *Kremlin-linked journalist organised Quran-burning at Turkish embassy in Stockholm*. [Online; accessed 24. Apr. 2023]. 26th Jan. 2023. URL: <https://www.telegraph.co.uk/world-news/2023/01/26/kremlin-linked-journalist-organised-quran-burning-turkish-embassy> (visited on 24/04/2023).
- [76] *Shayan Sardarizadeh on Twitter*. [Online; accessed 2. May 2023]. 16th Mar. 2022. URL: <https://twitter.com/Shayan86/status/1504106312115888130> (visited on 02/05/2023).
- [77] *Nathaniel Gleicher @ngleicher@infosec.exchange on Twitter*. [Online; accessed 24. Apr. 2023]. 16th Mar. 2022. URL: <https://twitter.com/ngleicher/status/1504186935291506693> (visited on 24/04/2023).
- [78] *Timeline of Cyberattacks and Operations | CyberPeace Institute*. [Online; accessed 13. Apr. 2023]. 13th Apr. 2023. URL: <https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline> (visited on 13/04/2023).

- [79] Microsoft Digital Security Unit (dsu) Microsoft Threat Intelligence Center (mstic). 'Destructive malware targeting Ukrainian organizations - Microsoft Security Blog'. In: *Microsoft Security Blog* (8th Feb. 2022). URL: <https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations> (visited on 02/05/2023).
- [80] 'Quran burning' protest scuppers Turkey-Sweden NATO talks. [Online; accessed 24. Apr. 2023]. 21st Jan. 2023. URL: <https://www.euronews.com/2023/01/21/quran-burning-protest-scuppers-turkey-sweden-nato-talks> (visited on 24/04/2023).
- [81] Guardian staff Reporter. 'Sweden cannot expect Turkey's support for Nato membership, Erdoğan warns'. In: *the Guardian* (7th Feb. 2023). URL: <https://www.theguardian.com/world/2023/jan/24/sweden-can-not-expect-turkeys-support-for-nato-membership-erdogan-warns> (visited on 24/04/2023).
- [82] *National Security Agency/Central Security Service > Signals Intelligence > Overview*. [Online; accessed 2. May 2023]. 2nd May 2023. URL: <https://www.nsa.gov/Signals-Intelligence/Overview> (visited on 02/05/2023).
- [83] *What is OSINT (Open-Source Intelligence?) | SANS Institute*. [Online; accessed 2. May 2023]. 1st May 2023. URL: <https://www.sans.org/blog/what-is-open-source-intelligence> (visited on 02/05/2023).
- [84] Bruce W. Watson. 'Intelligence | military science'. In: *Encyclopedia Britannica* (19th Apr. 2023). URL: <https://www.britannica.com/topic/intelligence-military#ref511596> (visited on 02/05/2023).
- [85] By Laurence Peter. 'Russian air force planes test Nato defences'. In: *BBC News* (30th Oct. 2014). URL: <https://www.bbc.com/news/world-europe-29832879> (visited on 03/05/2023).
- [86] *Dette er QRA – Quick Reaction Alert*. [Online; accessed 3. May 2023]. 3rd May 2023. URL: <https://www.forsvaret.no/aktuelt-og-presse/aktuelt/norges-forsvarer-i-skyene> (visited on 03/05/2023).
- [87] *Cyber-Attack Against Ukrainian Critical Infrastructure | CISA*. [Online; accessed 3. May 2023]. 3rd May 2023. URL: <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01> (visited on 03/05/2023).
- [88] *What are Petya and NotPetya Ransomware? | Malwarebytes*. [Online; accessed 3. May 2023]. 3rd May 2023. URL: <https://www.malwarebytes.com/petya-and-notpetya> (visited on 03/05/2023).
- [89] *Sandworm Team, ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, Voodoo Bear, IRIDIUM, Group G0034 | MITRE ATT&CK®*. [Online; accessed 4. May 2023]. 27th Apr. 2023. URL: <https://attack.mitre.org/groups/G0034> (visited on 04/05/2023).

- [90] William Casey Biggerstaff. 'The Status of Ukraine's "IT Army" Under the Law of Armed Conflict - Lieber Institute West Point'. In: *Lieber Institute West Point* (10th May 2023). URL: <https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict> (visited on 11/05/2023).
- [91] *Putin announces partial mobilization in Russia*. [Online; accessed 12. May 2023]. 21st Sept. 2022. URL: <https://web.archive.org/web/20220921063159/https://www.bbc.com/russian/news-62977634> (visited on 12/05/2023).

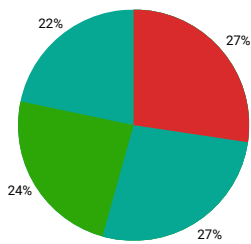
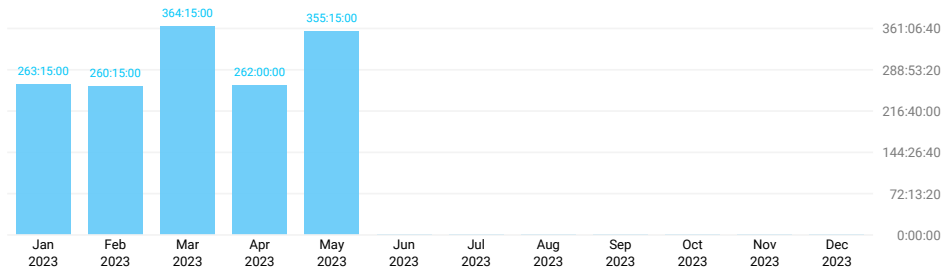
A.2 Toggl summary report

Summary Report



01-01-2023 – 31-12-2023

TOTAL HOURS: 1505:00:00

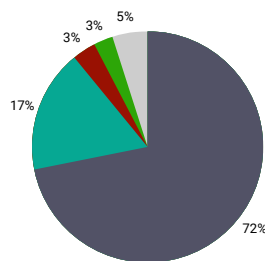


USER

- LA Lars
- DE Dennis
- ER Erki
- MA Magnus

DURATION

- 411:00:00
- 406:50:00
- 361:30:00
- 325:40:00



TIME ENTRY

- General work
- Research
- Meeting with Raymond
- Weekly focus update
- Other time entries

DURATION

- 1080:40:00
- 259:45:00
- 50:35:00
- 39:15:00
- 74:45:00

Appendix B

Standard agreement on thesis – NTNU



Norges teknisk-naturvitenskapelige universitet

Fastsatt av prorektor for utdanning 10.12.2020

STANDARDAVTALE

om utføring av studentoppgave i samarbeid med ekstern virksomhet

Avtalen er ufravikelig for studentoppgaver (heretter oppgave) ved NTNU som utføres i samarbeid med ekstern virksomhet.

Forklaring av begrep

Opphavsrett

Er den rett som den som skaper et åndsverk har til å fremstille eksemplarer av åndsverket og gjøre det tilgjengelig for allmennheten. Et åndsverk kan være et litterært, vitenskapelig eller kunstnerisk verk. En studentoppgave vil være et åndsverk.

Eiendomsrett til resultater

Betyr at den som eier resultatene bestemmer over disse. Utgangspunktet er at studenten eier resultatene fra sitt studentarbeid. Studenten kan også overføre eiendomsretten til den eksterne virksomheten.

Bruksrett til resultater

Den som eier resultatene kan gi andre en rett til å bruke resultatene, f.eks. at studenten gir NTNU og den eksterne virksomheten rett til å bruke resultatene fra studentoppgaven i deres virksomhet.

Prosjektbakgrunn

Det partene i avtalen har med seg inn i prosjektet, dvs. som vedkommende eier eller har rettigheter til fra før og som brukes i det videre arbeidet med studentoppgaven. Dette kan også være materiale som tredjepersoner (som ikke er part i avtalen) har rettigheter til.

Utsatt offentliggjøring

Betyr at oppgaven ikke blir tilgjengelig for allmennheten før etter en viss tid, f.eks. før etter tre år. Da vil det kun være veileder ved NTNU, sensorene og den eksterne virksomheten som har tilgang til studentarbeidet de tre første årene etter at studentarbeidet er innlevert.

1. Avtaleparter

Norges teknisk-naturvitenskapelige universitet (NTNU) Institutt: IIKG
Veileder ved NTNU: Erjon Zoto E-post og tlf.: erjon.zoto@ntnu.no , 98433097
Ekstern virksomhet: Digitaliseringsdirektoratet Ekstern virksomhet sin kontaktperson: Raymond Hagen E-post og tlf.: raymohag@stud.ntnu.no , 92685771
Student: Carl Dennis Flåte Fødselsdato: 27.07.1998
Student: Erki Sulg Fødselsdato: 21.04.2001
Student: Lars Magnus Lie Fødselsdato: 02.05.1996
Student: Magnus Sandem Dhelie Fødselsdato: 12.06.2001

Partene har ansvar for å klarere eventuelle immaterielle rettigheter som studenten, NTNU, den eksterne eller tredjeperson (som ikke er part i avtalen) har til prosjektbakgrunn før bruk i forbindelse med utførelse av oppgaven. Eierskap til prosjektbakgrunn skal fremgå av eget vedlegg til avtalen der dette kan ha betydning for utførelse av oppgaven.

2. Utførelse av oppgave

Studentene skal utføre: (sett kryss)

Masteroppgave	
Bacheloroppgave	x
Prosjektoppgave	
Annen oppgave	

Startdato: 09.01.2023

Sluttdato: 20.05.2023

Oppgavens arbeidstittel er:

Metodebruk for cyberangrep som har blitt brukt i krigen mellom Russland og Ukraina.

Ansvarlig veileder ved NTNU har det overordnede faglige ansvaret for utforming og godkjenning av prosjektbeskrivelse og studentens læring.

3. Ekstern virksomhet sine plikter

Ekstern virksomhet skal stille med en kontaktperson som har nødvendig faglig kompetanse til å gi studenten tilstrekkelig veiledning i samarbeid med veileder ved NTNU. Ekstern kontaktperson fremgår i punkt 1.

Formålet med oppgaven er studentarbeid. Oppgaven utføres som ledd i studiet. Studenten skal ikke motta lønn eller lignende godtgjørelse fra den eksterne for studentarbeidet. Utgifter knyttet til gjennomføring av oppgaven skal dekkes av den eksterne. Aktuelle utgifter kan for eksempel være reiser, materialer for bygging av prototyp, innkjøp av prøver, tester på lab, kjemikalier. Studenten skal klarere dekning av utgifter med ekstern virksomhet på forhånd.

Ekstern virksomhet skal dekke følgende utgifter til utførelse av oppgaven:
--

Dekning av utgifter til annet enn det som er oppført her avgjøres av den eksterne underveis i arbeidet.

4. Studentens rettigheter

Studenten har opphavsrett til oppgaven¹. Alle resultater av oppgaven, skapt av studenten alene gjennom arbeidet med oppgaven, eies av studenten med de begrensninger som følger av punkt 5, 6 og 7 nedenfor. Eiendomsretten til resultatene overføres til ekstern virksomhet hvis punkt 5 b er avkrysset eller for tilfelle som i punkt 6 (overføring ved patenterbare oppfinnelser).

I henhold til lov om opphavsrett til åndsverk beholder alltid studenten de ideelle rettigheter til eget åndsverk, dvs. retten til navngivelse og vern mot krenkende bruk.

Studenten har rett til å inngå egen avtale med NTNU om publisering av sin oppgave i NTNUs institusjonelle arkiv på Internett (NTNU Open). Studenten har også rett til å publisere oppgaven eller deler av den i andre sammenhenger dersom det ikke i denne avtalen er avtalt begrensninger i adgangen til å publisere, jf. punkt 8.

5. Den eksterne virksomheten sine rettigheter

Der oppgaven bygger på, eller videreutvikler materiale og/eller metoder (prosjektbakgrunn) som eies av den eksterne, eies prosjektbakgrunnen fortsatt av den eksterne. Hvis studenten skal utnytte resultater som inkluderer den eksterne sin prosjektbakgrunn, forutsetter dette at det er inngått egen avtale om dette mellom studenten og den eksterne virksomheten.

Alternativ a) (sett kryss) Hovedregel

<input checked="" type="checkbox"/>	Ekstern virksomhet skal ha bruksrett til resultatene av oppgaven
-------------------------------------	--

Dette innebærer at ekstern virksomhet skal ha rett til å benytte resultatene av oppgaven i egen virksomhet. Retten er ikke-eksklusiv.

Alternativ b) (sett kryss) Unntak

<input type="checkbox"/>	Ekstern virksomhet skal ha eiendomsretten til resultatene av oppgaven og studentens bidrag i ekstern virksomhet sitt prosjekt
--------------------------	---

Begrunnelse for at ekstern virksomhet har behov for å få overført eiendomsrett til resultatene:

¹ Jf. Lov om opphavsrett til åndsverk mv. av 15.06.2018 § 1

6. Godtgjøring ved patenterbare oppfinnelser

Dersom studenten i forbindelse med utførelsen av oppgaven har nådd frem til en patenterbar oppfinnelse, enten alene eller sammen med andre, kan den eksterne kreve retten til oppfinnelsen overført til seg. Dette forutsetter at utnyttelsen av oppfinnelsen faller inn under den eksterne sitt virksomhetsområde. I så fall har studenten krav på rimelig godtgjøring. Godtgjøringen skal fastsettes i samsvar med arbeidstakeroppfinnelsesloven § 7. Fristbestemmelsene i § 7 gis tilsvarende anvendelse.

7. NTNU sine rettigheter

De innleverte filer av oppgaven med vedlegg, som er nødvendig for sensur og arkivering ved NTNU, tilhører NTNU. NTNU får en vederlagsfri bruksrett til resultatene av oppgaven, inkludert vedlegg til denne, og kan benytte dette til undervisnings- og forskningsformål med de eventuelle begrensninger som fremgår i punkt 8.

8. Utsatt offentliggjøring

Hovedregelen er at studentoppgaver skal være offentlige.

Sett kryss

<input checked="" type="checkbox"/>	Oppgaven skal være offentlig
-------------------------------------	------------------------------

I særlige tilfeller kan partene bli enige om at hele eller deler av oppgaven skal være undergitt utsatt offentliggjøring i maksimalt tre år. Hvis oppgaven unntas fra offentliggjøring, vil den kun være tilgjengelig for student, ekstern virksomhet og veileder i denne perioden. Sensurkomiteen vil ha tilgang til oppgaven i forbindelse med sensur. Student, veileder og sensorer har taushetsplikt om innhold som er unntatt offentliggjøring.

Oppgaven skal være underlagt utsatt offentliggjøring i (sett kryss hvis dette er aktuelt):

Sett kryss

Sett dato

<input type="checkbox"/>	ett år	
<input type="checkbox"/>	to år	
<input type="checkbox"/>	tre år	

Behovet for utsatt offentliggjøring er begrunnet ut fra følgende:

Dersom partene, etter at oppgaven er ferdig, blir enig om at det ikke er behov for utsatt offentliggjøring, kan dette endres. I så fall skal dette avtales skriftlig.

Vedlegg til oppgaven kan unntas ut over tre år etter forespørsel fra ekstern virksomhet. NTNU (ved instituttet) og student skal godta dette hvis den eksterne har saklig grunn for å be om at et eller flere vedlegg unntas. Ekstern virksomhet må sende forespørsel før oppgaven leveres.

De delene av oppgaven som ikke er undergitt utsatt offentliggjøring, kan publiseres i NTNUs institusjonelle arkiv, jf. punkt 4, siste avsnitt. Selv om oppgaven er undergitt utsatt offentliggjøring, skal ekstern virksomhet legge til rette for at studenten kan benytte hele eller deler av oppgaven i forbindelse med jobbsøknader samt videreføring i et master- eller doktorgradsarbeid.

9. Generelt



Denne avtalen skal ha gyldighet foran andre avtaler som er eller blir opprettet mellom to av partene som er nevnt ovenfor. Dersom student og ekstern virksomhet skal inngå avtale om konfidensialitet om det som studenten får kjennskap til i eller gjennom den eksterne virksomheten, kan NTNUs standardmal for konfidensialitetsavtale benyttes.

Den eksterne sin egen konfidensialitetsavtale, eventuell konfidensialitetsavtale den eksterne har inngått i samarbeidprosjekter, kan også brukes forutsatt at den ikke inneholder punkter i motstrid med denne avtalen (om rettigheter, offentliggjøring mm). Dersom det likevel viser seg at det er motstrid, skal NTNUs standardavtale om utføring av studentoppgave gå foran. Eventuell avtale om konfidensialitet skal vedlegges denne avtalen.

Eventuell uenighet som følge av denne avtalen skal søkes løst ved forhandlinger. Hvis dette ikke fører frem, er partene enige om at tvisten avgjøres ved voldgift i henhold til norsk lov. Tvisten avgjøres av sorenskriveren ved Sør-Trøndelag tingrett eller den han/hun oppnevner.

Denne avtale er signert i fire eksemplarer hvor partene skal ha hvert sitt eksemplar. Avtalen er gyldig når den er underskrevet av NTNU v/instituttleder.

Signaturer:

Instituttleder: Dato:	
Veileder ved NTNU: Dato:	Erjon Zoto  18.01.2023
Ekstern virksomhet: Dato:	Raymond Hagen 24.01.2023
Student: Dato:	CARL DENNIS TILTE,  18.01.23
Student: Dato:	Erki Sulg, ESulg 18.01.23
Student: Dato:	LONES M LIL, LARS MAGNUS LIE 18.01.23
Student: Dato:	Magnus S. Dholie, Magnus S. Dholie 18.01.23

Appendix C

Project plan

Project Plan

Bachelor's thesis



Dhelie, Flåte, Lie, Sulg

Gjøvik, spring 2023

Table of Contents

1	Project information	3
2	Goals and framework	4
2.1	Background	4
2.2	Project goals	4
2.3	Framework	5
3	Scope	6
3.1	Problem domain	6
3.2	Problem limitations	6
3.3	Problem/Issue	6
4	Project organization	7
4.1	Roles and responsibilities	7
4.2	Routines and group rules	8
4.2.1	Routines	8
4.2.2	Rules	8
5	Planning, follow-up and reporting	9
5.1	Main division of the project	9
5.1.1	Planning Phase	9
5.1.2	Research Phase	9
5.1.3	Final report Phase	9
5.2	Plan for status meetings and decision points in the period	10
5.2.1	Status meetings	10
5.2.2	Decision points	10
6	Organizing quality assurance	11
6.1	Communication platforms	11
6.1.1	Microsoft Teams	11
6.1.2	Microsoft Outlook	11
6.1.3	Discord	11
6.2	Working platforms	12
6.2.1	Overleaf	12
6.2.2	Microsoft Teams	12
6.3	Additional platforms	12
6.3.1	Toggl	12
6.4	Documentation & standards	13
6.5	Risk analysis	14
6.5.1	Risk analysis after mitigation	19
7	Gantt chart	20
8	Appendix	22
8.1	Original task description (Norwegian)	22
8.2	Group contract	23

1 Project information

Title: Methods used in cyberattacks in the Russia-Ukraine war	Date given: 22.11.2022 Date of delivery: 22.05.2023
Group members: Carl Dennis Flåte carldf@stud.ntnu.no Erki Sulg erkis@stud.ntnu.no Lars Magnus Lie larsmli@stud.ntnu.no Magnus Sandem Dhelie magnussd@stud.ntnu.no	Supervisor: Erjon Zoto erjon.zoto@ntnu.no
Client: Norwegian Digitalisation Agency / <i>Digitaliseringsdirektoratet</i>	Contact person at the client: Raymond André Hagen raymond.andre.hagen@digdir.no

Table 1: Project information

2 Goals and framework

This section describes the background for the project along with goals which we will work towards during this project period. It will also describe the framework that we will follow to ensure project completion, and successful delivery & presentation of the finished product.

2.1 Background

This project task has been provided as a bachelor's thesis task for BDIGSEC2020 students at NTNU Gjøvik, and was chosen by our group.

The finished project report and information will be used by the Norwegian Digitalisation Agency (Digitaliseringsdirektoratet) for a doctor's degree study in cyberwarfare in the Russia-Ukraine war.

The Russia-Ukraine war, while mainly known for its physical aspect in the war, also spans into the cyberspace. By incorporating cyberattacks into both sides' arsenal, the different actors have opened a new front to the war that in this project will be the subject of investigation and analysis.

2.2 Project goals

The project goals will be divided into 3 categories: effect goals, result goals, and learning goals.

The effect goal of the project is to provide a completed thesis which can be used by the client for their doctor's degree research. This goal favours all stakeholders and ensures the client's interest to assist us in reaching our goals.

The result goal of the project is to provide a completed thesis which will be graded to an "A". For the project to be graded to an "A" we have to fulfill the task goals which are listed in the task description. We will also have to show that we have fulfilled our learning goals as part of the entire bachelor course.

Our learning goal will be to gain valuable experience in researching a topic, learning about different kind of attacks and presenting the information found. While researching we will try to get a understanding of cyberattacks in an ongoing major conflict, and the impact this has on the fighting.

In addition to these specified goals we also aim to fulfill the learning goals which are described in the bachelor's thesis course description for our study program[4].

2.3 Framework

We are planning on using a modified scientific method framework. Due to our bachelor's thesis being a literature study, our version of the framework will not contain the hypothesis and test stage.

The points included in our framework:

- Observation/question
- Research topic area
- Analyse data
- Report conclusions

This means that through our work on the project we will either make observation or ask ourselves questions. After that we have to research the chosen topic area in depth, and then analyse our findings. Finally, we have to take our analysis and report our conclusions as a part of a larger product; our thesis.

This framework is derived from the "scientific method" framework[3] and modified to suit the needs of our project.

3 Scope

3.1 Problem domain

The problem domain is the scientific area of expertise in which our task is placed. Our problem domain is available information on cyberwarfare in a modern war. In this case we will focus on the Russian-Ukrainian conflict.

3.2 Problem limitations

There are likely to be a lot of withheld or hard-to-get pieces of information on some of the cyberattacks we want to document in our thesis.

The credibility of sources is also an aspect to take note of and keep in mind.

We will limit our timeline from 1. February 2022 to 1. February 2023. This ensures that we get solid coverage of the attacks so far during the conflict, while also ensuring enough time to actually process and refine our research.

3.3 Problem/Issue

What methods have been used in cyberattacks between the main actors in the Russian-Ukrainian war?

To address this problem statement, we have to research the topic through various sources such as social media, news & research articles and other relevant sources including interviews and other forms of consultation. The collected information will be used to carry out the process of addressing the problem statement.

While addressing the problem statement our focus will be on the methods used in cyberattacks, including attack vectors, tools etc. Simultaneously, we will be researching and working on the targets of the attacks, as well as the consequences of them. To be able to provide some closure in our work, we will also discuss perpetrators, and attribution if possible, as well as responses to the different attacks.

4 Project organization

4.1 Roles and responsibilities

The group has through discussion decided on the following roles and responsibilities necessary for this project.

- **Group leader:** Has the overall vote if there is a disagreement in the group that cannot be solved by a majority vote. The group leader also has the responsibility of booking rooms for the obligatory on-site work hours and adding this to the calendar.
- **Deputy group lead:** Has the role of group leader if the original group leader is absent.
- **Contact person:** Is responsible for the contact with the client and the supervisor on behalf of the group.
- **Secretary:** Has the responsibility of taking notes during meetings with the client, the supervisor, and general group meetings. These are to be written into a shared Overleaf document.

These roles has been assigned to following group members:

- **Group leader, contact person:** Carl Dennis Flåte.
- **Deputy group lead:** Magnus Sandem Dhelie
- **General workers:** Erki Sulg and Lars Magnus Lie

All group members have been assigned the role of secretary. This allows for a rotation on the taking of meeting notes throughout the project period.

4.2 Routines and group rules

4.2.1 Routines

We have planned workdays Monday to Thursday from 09:00 to 16:00, and Fridays from 09:00 to 12:00. Still, it is expected of the group that members need to work as many hours as needed to deliver necessary products.

Mondays and Fridays are hybrid workdays while Tuesday through Thursday are obligatory campus presence. This means that Mondays and Fridays can be performed remote/online.

We allow for absence from obligatory campus workdays if there are other obligatory attendances e.g. work, other courses, planned meetings, appointments etc.

4.2.2 Rules

By signing, the group members have agreed to follow the rules written in the group contract which is included in this document at section 8.1 in the appendix. Breaching with said contract will result in consequences mentioned in that document.

5 Planning, follow-up and reporting

5.1 Main division of the project

The project is divided into three main phases where each parts have multiple sub phases. These phases are the planning, research and final report phases. The time each phase is active is shown in the [Gantt-chart in section 7](#).

5.1.1 Planning Phase

The planning phase consists of the creating and signing of the contracts (group and official), as well as the creation of this project plan. The project plan will be a guideline for the duration of the work on the bachelors thesis. The planning phase has a deadline for the 31.1.2023.

5.1.2 Research Phase

During the research phase we will spend most of our time gathering open source information, categorising and listing it in a database. We will contact different security firms as well as national security agencies, and people with special expertise in relevant subjects. After the research phase is done we will analyze the data gathered and discuss our findings.

5.1.3 Final report Phase

During the final report phase we will write the thesis itself, as well as the final report. There we will conclude our findings while also reporting on the work done during this period.

5.2 Plan for status meetings and decision points in the period

5.2.1 Status meetings

We have decided to hold weekly focus meetings on Mondays at 09:00. These meetings are to summarize what we need to focus on the coming week, but also serves as an arena where unfinished tasks can be discussed. Members are also free to bring forth any questions they may have regarding their tasks and the plan ahead. We can also discuss what to bring up with the supervisor or client during their meetings later in the week.

5.2.2 Decision points

The weekly focus meetings are our main point of making decisions, however we may discuss any input for decisions at any point as they occur. These decisions will be made internally in the group, but in case we are unable to make certain decisions, they will be taken up in the weekly meetings with either the supervisor or client.

See section 6.4 for documentation of choices made.

6 Organizing quality assurance

6.1 Communication platforms

Listed are all platforms used for communications and how they are utilised.

6.1.1 Microsoft Teams

- Used primarily as the primary communications platform between the group and our client, Raymond Hagen, and our supervisor, Erjon Zoto.
- Planned digital meetings are held through Microsoft Teams. (See ad-hoc group meetings, in section 6.1.3)

6.1.2 Microsoft Outlook

- Primary e-mail service.
- Used to send, receive, and answer to meeting notices.
- Shared Outlook-calendar, "Bachelor DIGSEC v23", used to provide overview of planned activities.

6.1.3 Discord

- Primary use is less formal and ad-hoc communications. This includes text messages, sharing of resources (URLs etc.), and voice communications.
- Ad-hoc meetings are held through Discord due to the group's familiarity and presence on the platform.
- Used during hybrid work-hours to be available for communications with other members.

6.2 Working platforms

Listed all platforms used for working on the project and how they are utilised.

6.2.1 Overleaf

- Overleaf is the primary document writing platform. Overleaf allows for easy LaTeX formatting and we can easily share and work simultaneously on project documents.

6.2.2 Microsoft Teams

- Microsoft Teams is used as a working platform to store and share documents and files.
- Project milestones are also managed through Teams built-in Milestones feature. This will be used to plan tasks and milestones.

6.3 Additional platforms

Platforms that do not fit the other categories.

6.3.1 Toggl

- Toggl is used to organize and document working hours.

6.4 Documentation & standards

- The APA 7th standard format will be used for referencing.

For example, a source being a book with one author would be referenced as such:
"Author, A. A. (year). *Title in italics* (edition). Publisher."^[1]

- Choices the group makes regarding project work and -management are documented in the internal document "choices.xlsx".

Only choices that impact the whole project are noted there. The document will be used in our work on the final report.

6.5 Risk analysis

We have chosen to conduct a risk analysis to map some of the risks we take on during this project. In our risk analysis table we have defined 4 levels of probability and consequence. The impact and time interval is hard to define, but as an example if something is likely to happen it might happen every 2 weeks to once a month. If the consequence is high it might delay the work for 1-2 weeks.

We have decided to develop mitigations all risks that we have found. Some planned mitigations are more detailed than others due to the nature of the risk they are mitigating.

New risks that occur, or risks that are not properly mitigated through this project plan, will be managed during group sessions.

	1 - Unlikely	2 - Less likely	3 - Likely	4 - Very likely
1 - Low consequence				
2 - Medium consequence	11			
3 - High consequence	9, 10	3, 4, 5	1, 2	
4 - Critical consequence	6, 7, 8			

Table 2: Risk analysis
Very high: Red, High: Orange, Medium: Yellow, Low: Green

Risk number 1:

Risk scenario	Scope creep
Description	The project's scope grows past the initial scope that had been determined beforehand.
Probability	Likely (3)
Consequence	High consequence (3)
Total risk	High (9)

Table 3: Risk 1

Mitigation: Discuss scope with client and most importantly the supervisor as often as needed to set up clear boundaries and ensure having an ideal scope.

Risk number 2:

Risk scenario	Scope kill
Description	Opposite of scope creep. The project's scope is too limited, resulting in a final product that does not reach the level of complexity the group aims for.
Probability	Likely (3)
Consequence	High consequence (3)
Total risk	High (9)

Table 4: Risk 2

Mitigation: Discuss scope with client and most importantly the supervisor as often as needed to set up clear boundaries and ensure having an ideal scope.

Risk number 3:

Risk scenario	Injury/illness
Description	A member of the group sustains an injury or illness that prevents them from working at full capacity.
Probability	Less likely (2)
Consequence	High consequence (3)
Total risk	Medium (6)

Table 5: Risk 3

Mitigation: Implement adaptive work methods for members with injuries or illnesses to attain an easier and better workflow for said members.

Risk number 4:

Risk scenario	Delays
Description	Parts of the project's deadlines are delayed. This does not include the final submission.
Probability	Less likely (2)
Consequence	High Consequence (3)
Total risk	Medium (6)

Table 6: Risk 4

Mitigation: Adherence to the project plan and group contract should ensure that deliverables are completed on time. It is harder to mitigate against delays caused by forces outside the group.

Risk number 5:

Risk scenario	Difficulty progressing
Description	Lack of information, knowledge, etc. may lead to difficulties progressing with the project, and in worse cases getting stuck and unable to proceed.
Probability	Less likely (2)
Consequence	High Consequence (3)
Total risk	Medium (6)

Table 7: Risk 5

Mitigation: Quality dialogue between group members, as well as being able to receive advice from project stakeholders.

Risk number 6:

Risk scenario	Internal group issues
Description	Disagreements, member is not following rules, member does not participate.
Probability	Unlikely (1)
Consequence	Critical Consequence (4)
Total risk	Medium (4)

Table 8: Risk 6

Mitigation: Adherence to the group contract combined with healthy dialogue within the group.

Risk number 7:

Risk scenario	Loss of data
Description	Data that has been gathered and/or processed has been lost with no way to recover it.
Probability	Unlikely (1)
Consequence	Critical consequence (4)
Total risk	Medium (4)

Table 9: Risk 7

Mitigation: Implement backup- and recovery methods to recover lost data. We have decided to use OneDrive through Teams as a cloud backup method. Data will also occasionally be saved locally on the members' devices.

Risk number 8:

Risk scenario	Loss of group member.
Probability	Unlikely (1)
Consequence	Critical Consequence (4)
Total risk	Medium (4)

Table 10: Risk 8

Mitigation: —

Risk number 9:

Risk scenario	Illness/loss of relatives.
Probability	Unlikely (1)
Consequence	High Consequence (3)
Total risk	Low (3)

Table 11: Risk 9

Mitigation: —

Risk number 10:

Risk scenario	Problems with client or supervisor,.
Description	Loss of contact with supervisor/client.
Probability	Unlikely (1)
Consequence	High Consequence (3)
Total risk	Low (3)

Table 12: Risk 10

Mitigation: Ensure quality dialogue and regular meetings.

Risk number 11:

Risk scenario	Working platforms are unavailable
Description	Online working platforms including Overleaf, Microsoft Teams and other crucial working platforms become unavailable. Working normally and at full capability like before is not possible.
Probability	Unlikely (1)
Consequence	Medium consequence (2)
Total risk	Low (2)

Table 13: Risk 11

Mitigation: Use backups as interim work documents until platforms are up and running again.

6.5.1 Risk analysis after mitigation

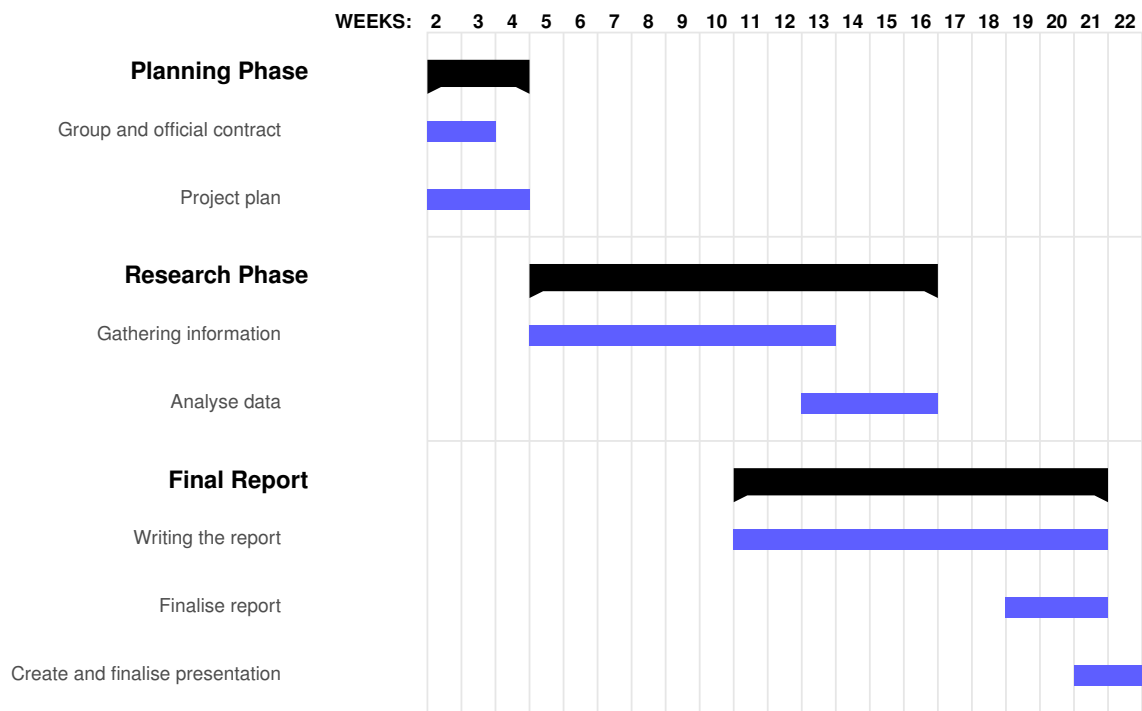
	1 - Unlikely	2 - Less likely	3 - Likely	4 - Very likely
1 - Low consequence	11			
2 - Medium consequence	7	3		
3 - High consequence	4, 5, 6, 9, 10	1, 2		
4 - Critical consequence	8			

Table 14: Risk analysis after mitigation

Very high: Red, **High:** Orange, **Medium:** Yellow, **Low:** Green

7 Gantt chart

We have a Gantt chart which is used to visualise our project milestones and provide an estimate over the project period.^[2]



References

- [1] Kildekompasset (2023, January 27). *APA 7th*. Kildekompasset.
<https://kildekompasset.no/en/referencing-styles/apa-7th/>
- [2] Skala, W. (2013). *Gantt Charts with the pgfgantt Package*. Overleaf.
<https://www.overleaf.com/latex/examples/gantt-charts-with-the-pgfgantt-package/jmkwfxrnfxnw>
- [3] Britannica (2022). *Scientific method*. Britannica.
<https://www.britannica.com/science/scientific-method>
- [4] NTNU (2023, January 31). *DCSG2900 - Bachelor Thesis Bachelor of Science in Digital Infrastructure and Cyber Security*. NTNU.
<https://www.ntnu.edu/studies/courses/DCSG2900/2022#tab=omEmnet>

8 Appendix

8.1 Original task description (Norwegian)

Metodebruk for cyberangrep som har blitt brukt i krigen mellom Russland og Ukraina.

Jeg tar en Off. PHD gjennom Digitaliseringsdirektoratet, som har tjenester for dialog mellom organisasjoner, virksomheter og individ med det offentlige. De mest kjente tjenestene som Digitaliseringsdirektoratet tilbyr, er Altinn og id-porten. I tillegg til 20 andre offentlig IKT løsninger

Oppgaven

En litteraturstudie av hvordan cyber angrep er blitt benyttet som en del av krigen mellom Russland og Ukraina. Det hadde vært en god del med angrep i noen uker før den Russiske invasjonen 24.2.2022. Så det er naturlig at denne perioden også er med i studien. Spesielt fokus på metoder, og ikke minst hvordan er angrep blitt besvart og håndtert. I tillegg til Russiske og Ukrainske aktører, så har flere andre hacktivistgrupper som anonymous vært aktive.

Oppgavens mål

Oppgaven er gjennom bruk av åpne kilder. Media, sikkerhetsfirma, trusslevurderinger, Facebook, Telegram finne ut og beskrive hvilke cyber angrep som er blitt gjennomført til nå i krigen. Metoder og mottiltak er spesielt interessant, men også om det finnes mulighet for å se hvem som har gjennomført operasjonene.

Oppgavens krav

- Forstå hvilke aktører som gjennomfører cyberangrep
- Beskrive de ulike cyberangrep som er blitt gjennomført
- Se hvilke aktører utenfor Russland og Ukraina som har gjennomført cyberangrep i relasjon til krigen
- Hvilke metoder og mottiltak er blitt benyttet?
- Hvilke type påvirkningsoperasjoner er blitt gjennomført?

Siden jeg arbeider med en PHD om avanserte statsfinansierte hackergrupper, ønsker derfor å ha mulighet til å kunne bruke eventuelle funn til å gjøre analyser på i forhold til forskningen min.

Raymond Andre Hagen

raymohag@stud.ntnu.no / raymond.andre.hagen@digdir.no

8.2 Group contract

Group Contract

Bachelor's thesis



Dhelie, Flåte, Lie, Sulg

Gjøvik, spring 2023

Table of contents

1	Introduction	3
1.1	Group members	3
1.2	Purpose of document	3
2	Roles & responsibilities	4
2.1	Roles	4
2.2	General responsibilities	5
2.2.1	Meetings	5
2.2.2	Information management	5
2.2.3	Academic responsibility	5
3	Administrative information	6
3.1	Rules	6
3.1.1	Attendance	6
3.1.2	Schedule	6
3.1.3	Disagreements	7
3.1.4	Tasks and workload	7
3.2	Conflicts & conflict resolution	8
3.3	Consequences	8
4	Signatures	9

1 Introduction

1.1 Group members

Group members and contact information.

Member	E-mail	Telephone
Carl Dennis Flåte	carldf@stud.ntnu.no	+47 984 51 559
Erki Sulg	erkis@stud.ntnu.no	+47 986 55 634
Lars Magnus Lie	larsmli@stud.ntnu.no	+47 458 18 406
Magnus Sandem Dhelie	magnussd@stud.ntnu.no	+47 414 78 314

Table 1: Member information

1.2 Purpose of document

The purpose of this document is to be a contract for the work on the Bachelor's thesis written by the members listed above. It contains a list of the members with contact information, their roles, responsibilities, group rules, a conflict resolution guide and the signatures of all group members.

2 Roles & responsibilities

2.1 Roles

Group leader: Carl Dennis Flåte

Responsibilities:

- Formal contact person for the group. Is responsible for calling in to meetings with supervisor and client.
- Responsible for group cohesion and delegation of tasks.

Deputy group leader: Magnus Sandem Dhelie

Responsibilities:

- Take over group leader responsibilities in case of group leader absence.
- Assists group leader in administrative tasks relating to the project.

2.2 General responsibilities

2.2.1 Meetings

- Meeting notes are to be taken every pre-arranged meeting. During ad-hoc meetings only important decisions need to be noted.
- The role of referent is to be rotated after every meeting.
- The meetings should also be used as a resource for improvement. This includes asking relevant questions and requesting feedback on the group's work.

2.2.2 Information management

- The group members will ensure an organized file structure for any new or updated documents stored on any working platform.
- Any finished documents will be stored as a PDF and an understandable naming structure e.g. filename and date.
- Links to web pages/resources shall be sorted in the "resources.xlsx" document with all the relevant information about the source/article.

2.2.3 Academic responsibility

- Group members will, to the best of their knowledge, do their utmost to only use sources that are trustworthy. Due to the nature of the task one has to be prepared to filter through biased and untrustworthy information.
- Members are to always operate with good referral to sources used throughout the project.
- Members are to keep in mind the assessment criteria and task requirements while working on the thesis.

3 Administrative information

3.1 Rules

This section displays the rules that all group members have agreed upon, given that they signed the contract. The rules should be followed accordingly, and breach of contract will result in specified penalties that are usually resolved within the group, with severe cases being elevated to the supervisor or course coordinator.

3.1.1 Attendance

Rule 1.1: Absence must be notified to the group or group leader as soon as a member knows they will not be in attendance as expected.

Rule 1.1.1: Absence is allowed with a valid reason, and is to be validated by group leader.

Rule 1.1.2: In the event of a delay, other group members and eventual meeting participants should be notified through appropriate channels. If possible provide an estimated time of arrival.

3.1.2 Schedule

Rule 2.1: The following working schedules are to be followed: 09:00 - 16:00 Monday through Thursday, with Fridays being 09:00 - 12:00. This results in a 31 hour work-week.

Rule 2.1.1: Monday & Friday will be hybrid solutions, while Tuesday through Thursday will have compulsory physical attendance on campus or another pre-arranged location.

Rule 2.1.2: When working remotely, all members must be available for contact at all times during the specified working hours, unless a valid reason is provided as per rule 1.1.

3.1.3 Disagreements

Rule 3.1: Disagreements are to be resolved by a majority vote within the group.

Rule 3.1.1: If the group cannot come to an agreement by civil discussion, the group leader has the final vote.

Rule 3.1.2 Continued disagreement within the group will be resolved through contact with the supervisor and any further escalation will be taken to the course coordinator.

3.1.4 Tasks and workload

Rule 4.1: Tasks will be distributed as equally as possible to ensure a fair workload.

Rule 4.1.1: Expected time spent on working on the project is a minimum of 30 hours per week, less than the agreed upon schedule as per rule 2.1. This ensures that all members should be able to meet the agreed upon quota.

Rule 4.1.2: Tasks must have a deadline for planning reasons, and any task which cannot be completed within the deadline must be informed of to the group.

Rule 4.1.2.a: In the event that a member realises that they are unable to complete a task as planned, this is to be communicated to the group leader for further delegation.

3.2 Conflicts & conflict resolution

Any minor conflicts or first time conflicts will be attempted to be resolved within the group. Repeating conflicts and more significant conflicts that are not able to be resolved within the group, will be taken to the supervisor for attempted resolution. Critical conflicts that cannot be resolved with the supervisor will be elevated to a conflict resolution meeting with the course coordinator.

3.3 Consequences

Consequences will be decided based on a case-by-case basis should there be any need for them. Agreed upon consequences shall be appropriate and proportionate to the infraction.

Minor infractions will not result in any formal consequences.

4 Signatures

By signing this contract signers are contractually accepting all sections and rules contained in the document.



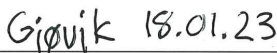
Carl Dennis Flåte



Place & Date



Erki Sulg



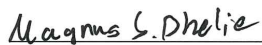
Place & Date



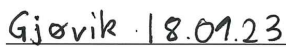
Lars Magnus Lie



Place & Date



Magnus Sandem Dhelie



Place & Date

This page intentionally left blank

Appendix D

Meeting minutes

Meeting Notes



Dhelie, Flåte, Lie, Sulg
Gjøvik, spring 2023

Table of contents

1	Group meetings	4
1.1	Planning meeting 13.01.2023	4
1.2	Weekly focus update 16.01.2023	6
1.3	Weekly focus update 23.01.2023	8
1.4	Weekly focus update 30.01.2023	9
1.5	Weekly focus update 06.02.2023	11
1.6	Weekly focus update 13.02.2023	12
1.7	Weekly focus update 20.02.2023	13
1.8	Weekly focus update 06.03.2023	13
1.9	Weekly focus update 13.03.2023	14
1.10	Weekly focus update 20.03.2023	14
1.11	Weekly focus update 27.03.2023	15
1.12	Weekly focus update 12.04.2023	15
1.13	Weekly focus update 17.04.2023	16
1.14	Weekly focus update 01.05.2023	16
1.15	Weekly focus update 08.05.2023	17
1.16	Weekly focus update 15.05.2023	18
2	Meetings with supervisor	19
2.1	Meeting with supervisor 18.01.2023	19
2.2	Meeting with supervisor 25.01.2023	21
2.3	Meeting with supervisor 01.02.2023	22
2.4	Meeting with supervisor 22.03.2023	23
2.5	Meeting with supervisor 27.04.2023	24
2.6	Meeting with supervisor 10.05.2023	25
2.7	Meeting with supervisor 19.05.2023	26
3	Meetings with client	27
3.1	Meeting with client 20.01.2023	27
3.2	Meeting with client 27.01.2023	28
3.3	Meeting with client 03.02.2023	29
3.4	Meeting with client 10.02.2023	30
3.5	Meeting with client 17.02.2023	31
3.6	Meeting with client 21.02.2023	32
3.7	Meeting with client 03.03.2023	34
3.8	Meeting with client 10.03.2023	35
3.9	Meeting with client 17.03.2023	36
3.10	Meeting with client 31.03.2023	37
3.11	Meeting with client 14.04.2023	39
3.12	Meeting with client 28.04.2023	40
3.13	Meeting with client 05.05.2023	41
3.14	Meeting with client 12.05.2023	42
3.15	Meeting with client 19.05.2023	43
4	Other meetings	44

4.1 Lecture on Ukraine 16.03.2023 44

1 Group meetings

1.1 Planning meeting 13.01.2023

Present members: Dennis, Erki, Lars, Magnus

Time: 10:00-15:00

Agenda: Project planning

Location: A158, Gjøvik Campus

Referent: Lars

- Where do we write the meeting references: Overleaf
- How we log hours: Toggl (<https://track.toggl.com/timer>).
- Where do we save files: OneDrive/Teams.
- Language to write: English (UK).
- How do we organise links/sources/references: Excel spreadsheet and a separate folder for complete pdf files.
- Where the team communicates between members: Discord.
- Where the team members work, ie. update tasks & milestones, upload resources etc.: Microsoft Teams.
- Where do we communicate with the client and supervisor: Microsoft Teams.
- What's our working method: Modified scientific method. Our method will make use of our open-source research into cyberattacks performed in the Russia-Ukraine war while at the same time presenting an analysis of some cases and research into the why, how, who and consequences.
- Workdays/hours Monday-Friday, 0900-1600 hours. During these hours it is expected of team members to be available and actively working on tasks related to the Bachelor's thesis.
- Tuesday-Thursday obligatory physical presence at campus. Mondays and Fridays are hybrid, form of presence is up to each individual member.
- Dennis is promoted to group leader.
- Lars is made responsible for the "resources" spreadsheet.
- Meeting referent changes each meeting.
- Read through individual work together every Friday.

- Create templates for adding pictures, tables and more in Latex-documents.
- Citation style is APA 7th.
- Meeting is finished.
- Tasks are updated.
- Refer to "choices.xlsx" on Teams for justification of choices made.
- "Weekly focus update" meeting every monday from 0900-1000.

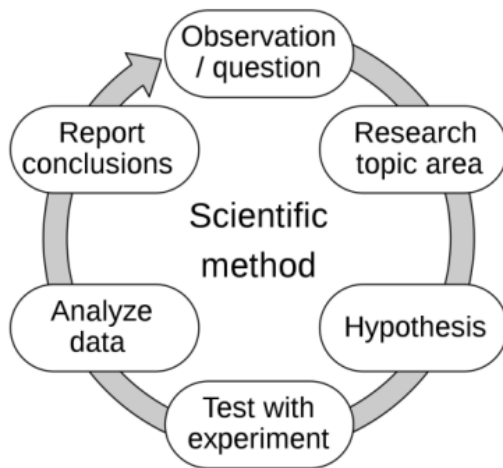


Figure 1: Scientific method graphic

Lorem	Ipsum	Dolor
Sit	Amet	Consectetur

Table 1: Table template

1.2 Weekly focus update 16.01.2023

Present members: Dennis, Erki, Lars, Magnus

Time: 09:00-10:00

Agenda: Plannings tasks for upcoming week

Location: Online, Teams Meeting

Referent: Magnus

Planned tasks from last week:

- Plan meeting with Erjon (supervisor).
 - Ask for general guidance and good bachelor's thesis's to take inspiration from.
 - Set to Dennis
 - Plan meeting between group and Raymond (client) and Erjon.
 - Set to Dennis and Magnus
 - *Finalise project plan and -contract.*
 - Part of this meeting.
 - Set to everyone.
-

New tasks:

- Gantt chart
 - Set to Erki
 - Look for earlier bachelor tasks to refer to.
 - Set to all
 - Discuss our scope
 - Set to all
 - Project plan creation
 - Set to Magnus and Lars
-

Minutes:

- Magnus is referent
- Dennis explains Weekly Focus Update purpose. To check in on task updates and plan new tasks for the coming week.
- **Task update:** Meeting with Erjon: Dennis will plan this. Physical meeting this week.

- **Task update:** Meeting between Raymond, Erjon and group. Plan to next week after discussing with them both.
- **Task update:** Finalise project plan and -contract. Not too critical right now, but it should not be a task that takes too much time.
- **New task:** Start working on Gantt Chart. Erki takes responsibility for this.
- **New task:** We should start looking for (2-3) bachelor tasks that have done well so we can refer to them while writing our own task.
- **IMPORTANT!:** Discuss our scope. Raymond is our client and not our supervisor. He may have a lot of good information, but we need to remember our task criteria.
- Write a short summary of what we have done throughout this week to present to Raymond on Friday.
- **New task:** Create the project plan and start writing it.
- Looking into Toggl time-export

1.3 Weekly focus update 23.01.2023

Present members: Dennis, Erki, Lars

Time: 09:00-10:00

Agenda: Review previous week and plan tasks for upcoming week

Location: Online, Teams Meeting

Referent: Lars

Information from past week:

- Asked Erik Hjelmås if he knew any good thesis's written by previous DIGSEC students that are relevant to our work.

According to Hjelmås, "[Åpenhetens dilemma](#)" & "[En analyse av passfraser fra skjønnlitterære bøker](#)" are thesis's that we should look at for inspiration.

- Magnus is absent due to an injury requiring surgery.
 - Dennis will be somewhat absent this week until his fever subsides.
-

Planned tasks from last week:

- Plan meeting between Erjon and supervisor.
 - Send meeting request.
 - Have Erjon join weekly meeting with Raymond (just this once).
 - Finalise project plan.
 - Has to be finished this week.
 - Get signatures for all documents that require them.
 - Lars is on the task, but has been unable get the relevant persons to meet for signing.
-

New tasks:

- All members read through the mentioned relevant bachelor's thesis's for inspiration.
 - Create presentation about the project plan.
-

Minutes:

Nothing to note.

1.4 Weekly focus update 30.01.2023

Present members: Magnus, Lars, Erki

Time: 09:00-10:00

Agenda: Review previous week and plan tasks for upcoming week

Location: Online, Teams Meeting

Referent: Magnus

Information from past week:

- Magnus is back. Right arm has some handicap, but he can write.
 - Lars has delivered the project agreement (Blackboard -> Bacheloroppgave/Arbeidsskrav -> Prosjektavtale).
 - Dennis is away on a trip. He will be back tomorrow.
-

Planned tasks from last week:

- All members read through the mentioned relevant bachelor's thesis's for inspiration.
 - According to Hjelmås, "[Åpenhetens dilemma](#)" & "[En analyse av passfraser fra skjønnlitterære bøker](#)" are thesis's that we should look at for inspiration.
 - Magnus has not read these, but will read them this week.
 - Create presentation about the project plan.
 - This was done and presented on Friday 27.01 for Raymond. Still waiting for confirmation from Erjon.
-

New tasks:

- Find out where we want to research. We should start with pre-war and at the start of war first. Jan-Feb 2022. Also lay some background information.
- Start creating a timeline.
- Where do we want to collect our research? Another overleaf doc so we can write a few words about the article/resource we have found?
- For each resource/article: Where, When, Attack Method, Analysis, Discuss (Proposed format).

Minutes:

- Start creating the timeline of the war. Can use it to input our weekly research.
- Researching how to best create a timeline in LaTeX. In resources in Discord.

1.5 Weekly focus update 06.02.2023

Present members: Dennis, Magnus, Lars, Erki

Time: 09:00-10:00

Agenda: Review previous week and plan tasks for upcoming week

Location: Online, Teams Meeting

Referent: Erki

Minutes:

- More individual work this week
- Continuing work from last week: check the older bachelor theses, mostly reading and research
- Attempt filling out one of the incident report form to check out how it works.
- Some of the work time will be replaced with the IØ2000 seminars.
- Dennis will set up a new meeting with the supervisor
- Raymond has sent us a list of useful Telegram channels.
- Dennis has booked a room for Thursday.
- Meeting with the supervisor 14:00 on Thursday.

1.6 Weekly focus update 13.02.2023

Present members: Dennis, Magnus, Erki, Lars

Time: 09:00-10:00

Agenda: Review previous week and plan tasks for upcoming week

Location: Online, Teams Meeting

Referent: Dennis

Minutes:

- Discussed last week's activities, and how the results were subpar. All agree that more work needs to be done regardless of other subjects and happenings.
- Continue on tasks set down last week, with a focus on information gathering and document structuring.
- Magnus has found some promising sources he will follow up on, and will test the functionality of the Cyber Incident Report Form that Dennis has made for the project.
- Discussion regarding future work and expectations. A lot happening outside "work hours" in the next weeks but we have made it clear to one another that expectations have to be met.
- Everyone informed each other of their schedules for the week. All members will spend some time at career days this week as well as the following:
 - Dennis is busy with Login-work due to the career days this Tuesday and Wednesday.
 - Lars has a seminar from 10:00-15:00 on Thursday.
 - Erki is busy from 13:15-14:45 on Friday.
 - Magnus has to remove his stitches on Tuesday.

1.7 Weekly focus update 20.02.2023

Present members: Dennis, Magnus, Lars

Time: 09:00-10:00

Agenda: Review previous week and plan tasks for upcoming week

Location: Online, Teams Meeting

Referent: Lars

Minutes:

- No news about the news Raymond showed us in the meeting. Will keep an eye out.
- Nothing new, continue working as last week.

1.8 Weekly focus update 06.03.2023

Present members: Dennis, Magnus, Lars, Erki

Time: 10:00-11:00

Agenda: Review previous week and plan tasks for upcoming week

Location: Online, Teams Meeting

Referent: Lars

Minutes:

- We must create a disposition.
- Gather more sources about what we have.
- Have an example on how to do a writeup on a attack.
- Erki has driving lessons on Friday from 7-12.
- Think about questions for the history professor.

1.9 Weekly focus update 13.03.2023

Present members: Dennis, Magnus, Lars, Erki

Time: 10:00-11:00

Agenda: Review previous week and plan tasks for upcoming week

Location: Online, Teams Meeting

Referent: Magnus

Minutes:

- IØ2000 this week (Tuesday and Wednesday).
- Lars has SMF on Thursday. Erki has driving lessons on Thursday.
- "Keep up the good work"
- Get some structural work done on the bachelor document. Chapters and subsections.

1.10 Weekly focus update 20.03.2023

Present members: Dennis, Magnus, Lars, Erki

Time: 10:00-11:00

Agenda: Review previous week and plan tasks for upcoming week

Location: Online, Teams Meeting

Referent: Erki

Minutes:

- Working on the thesis all week to ensure significant progress.
- Magnus has work Wednesday-Thursday, however it does not affect the project work too much.
- A meeting with the supervisor has been set up.

1.11 Weekly focus update 27.03.2023

Present members: Lars, Erki

Time: 09:00-09:15

Agenda: Review previous week and plan tasks for upcoming week

Location: Online, Teams Meeting

Referent: Lars

Minutes:

- Did okay amount of work last week.
- Continue working on the thesis this week.

1.12 Weekly focus update 12.04.2023

Present members: Dennis, Erki, Magnus

Time: 09:00-09:30

Agenda: Progress update, discussion

Location: Online, Teams Meeting

Referent: Dennis

Minutes:

- Discussed where we are on the project versus where we want to be.
 - We are slightly behind on finishing chapters 2 & 3, and we need to start writing more on chapter 5.
 - Otherwise we are keeping up with the original plan regarding progress.
 - We should finish chapters 2 & 3 this week.
- Will send a copy of the first iteration to our supervisor, Erjon, when we think it's ready. Most likely at the end of this week (15).
- Need to prepare for Friday's meeting with Raymond regarding progress and findings.
- All members need to get back into "work mode" after the holiday and keep up the good work.

1.13 Weekly focus update 17.04.2023

Present members: Dennis, Erki, Lars

Time: 09:00-09:30

Agenda: Progress update, discussion

Location: Online, Teams Meeting

Referent: Dennis

Minutes:

- In general just keep working on the thesis.
- Also need to get the timelines to a level where we can portray the data that has been requested by Raymond.
- The first iteration has been sent over to Erjon Zoto, and we're waiting on feedback before we make any significant changes to our existing product.

1.14 Weekly focus update 01.05.2023

Present members: Dennis, Erki, Lars

Time: 09:30-10:00

Agenda: Progress update, discussion

Location: Online, Teams Meeting

Referent: Dennis

Minutes:

- Keep on working with the remaining chapters.
- Review existing product, especially with regards to chapter 3 *Method*.
- Ensure that there is sufficient progress on the thesis to be able to request further feedback from supervisor and/or Raymond in the near future.
- Officially last month of work on the thesis. Graduation next!

1.15 Weekly focus update 08.05.2023

Present members: Dennis, Erki, Lars, Magnus

Time: 10:00-10:30

Agenda: Progress update, discussion, planning

Location: Online, Teams Meeting

Referent: Dennis

Minutes:

- Parts of Monday and Tuesday will be unavailable for work on the thesis due to IØ2000.
Additionally, Lars is unavailable during Tuesday afternoon due to a job interview.
- Need to reach a certain level of new content on the thesis before Wednesday's meeting with Erjon, and then again before Friday's meeting with Raymond, if we want updated guidance and feedback. This, of course, needs to be sent to each of them respectively before each meeting.
- Focus on finishing chapter 6, while also making significant progress on chapter 7 if we are to be finished with the first true draft sometime next week.
- In chapter 6, pay special attention to answering the research questions.
- Start reviewing "finished" chapters. See if more content is needed, or if something needs to be removed, check for spelling and grammar mistakes, make sure all statements are cited, and generally ensure a high level of quality throughout the paper.
- Review formatting on the document to ensure no mistakes stem from that.

1.16 Weekly focus update 15.05.2023

Present members: Dennis, Erki, Lars, Magnus

Time: 09:30-10:00

Agenda: Progress update, discussion, planning

Location: Online, Teams Meeting

Referent: Dennis

Minutes:

- Discussed what needed to be finished by the end of the day:
 - Chapter 7 is almost finished.
 - Chapter 8 Conclusion has to be written.
 - Sections here and there that aren't finished.
- When done, go over everything and send to Erjon for feedback.
- Will continue editing, correcting and so on while we are waiting for feedback this week.
- Re-structure meeting minutes document into sections for group meetings, meetings with client, meetings with supervisor, and other meetings.
- Go over all meeting minutes and fix any issues there.

2 Meetings with supervisor

2.1 Meeting with supervisor 18.01.2023

Present members: Dennis, Erki, Lars, Magnus, Erjon

Time: 10:00-11:00

Agenda: First meeting with supervisor, update & consult

Location: K108, Gjøvik Campus

Referent: Erki

Minutes:

- Upload more to Teams for supervisor to access.
- Upload proposal from client to Teams for the supervisor to access.
- Discuss choices of platforms, language and etc. with supervisor (choices.xlsx).
- Discuss finished parts, and what we aim to progress and finish.
- Mention new meeting with client on Friday, and that it's weekly.
- Joint meeting with supervisor and client. Propose the meeting to be on Friday 27.01.2023.
- Take up the joint meeting with the client on Friday 20.01.2023.
- Discuss "Oppgavens mål" from the proposal task, and mention that we should be able to complete the tasks.
- Discuss available sources.
- Most of February will be finding sources and reading for research.
- Mention that we will contact NSM and other agencies/organizations to find out if they have relevant information available to share with us.
- Discuss source credibility.
- Supervisor recommends <https://www.techtarget.com/> for data
- Discuss scope of the thesis. Cannot mention every single incident.
- On Friday when meeting the client, discuss mentioning older incidents preceding the war before with the client. Focus should still be the time after the start of the war.
- Stop gathering new information at some point where it feels appropriate because of the scope.

- Timeline, pick the most severe and relevant events in the war.
- Idea: main focus, a number of larger attacks and surrounding events
- Look at both sides of the war. (Both Russian and Ukrainian cyberattacks)
- Discuss deadlines, 7th of April should be the desired deadline for first draft
- Decide a common time for meeting with the supervisor, Wednesdays 10:00.
- Sign the common agreement with every group member and supervisor.
- The meeting has concluded.

2.2 Meeting with supervisor 25.01.2023

Present members: Erki, Lars, Erjon

Time: 10:00-11:00

Agenda: Meeting with supervisor, update & consult

Location: Online, Teams Meeting

Referent: Erki

Minutes:

- Erjon thinks "client" should be replaced with "task giver".
- Elaborate more on 02_goals and 05_planning.
- Risk number 5 - consequence too low?
- Gantt - start writing thesis from week 10.
- More resources/references in project plan.
- Mention something about the cyberwarfare in the scope (or wherever it fits).
- Add group contract to the appendix of the project plan.
- (Presentation) Do not focus too much on rules etc... More on the background, planning etc. During the presentation focus on the scope and what is interesting for the client. Keep it short, about 5 min.

2.3 Meeting with supervisor 01.02.2023

Present members: Dennis, Magnus, Lars, Erki, Erjon

Time: 10:00-10:15

Agenda: Review tasks done and the plan forward.

Location: Online, Teams Meeting

Referent: Dennis

Minutes:

- Showed Erjon the final version of the project plan.
- Discussed what we plan to do during the next week, and how we are now moving in to the research phase of the project.
- Erjon will include a colleague of his in our meetings forward. This colleague supposedly has insight on the conflict we are covering.
- Short meetings with supervisor. Will update Erjon on our status and any questions we may have each week.

2.4 Meeting with supervisor 22.03.2023

Present members: Erki, Dennis, Lars, Magnus, Erjon

Time: 10:00-11:00

Agenda: Meeting with supervisor, update & consult

Location: Online, Teams Meeting

Referent: Lars

Minutes:

- It's not basic theory so he thinks ch.2 should be called Background.
- Theory part: talk about the different aspects that helped us define the method.
- Make sure to add the history parts.
- Make a image of the timeline with just dates? And put it in the appendix?
- Presentation: have a image of the timeline?
- When we think we have something good enough to be a first draft, we send it to Erjon.
- Mention how we looked up our sources in Validity & reliability.

2.5 Meeting with supervisor 27.04.2023

Present members: Dennis, Erki, Lars, Magnus, Erjon

Time: 10:02-11:00

Agenda: Progress update, discussion, guidance

Location: Online, Teams Meeting

Referent: Lars

Minutes:

Main focus for the meeting was discussing Erjon's comments on our latest iteration.

- Try to have 3 research questions to focus on, then have the other's as add on questions.
- Change result goal to something other than "an A".
- Write down language limitations, ex. only sources in English and Norwegian.
- Mention the historic nature of conflict between the nations, or that we are not covering it.
- In chapter 2.2.4 write about the buildup of troops etc.
- Write more details before the APT image.
- Make subsection apt clickable to glossary.
- Chapter 3.3 literature, qualitative, gray papers... high level info on the study.
- Change outside communication to something else?
- Fix chapter 5.
- Maybe remove the 2 last research questions, just mention them in the discussion/results.

2.6 Meeting with supervisor 10.05.2023

Present members: Dennis, Erki, Lars, Magnus, Erjon

Time: 12:15-13:00

Agenda: Progress update, discussion, feedback

Location: Online, Teams Meeting

Referent: Dennis

Minutes:

- The goal of this meeting is to get answers on some questions regarding the thesis. General questions on structure, and if there are parts that need to be modified, added on, or removed.
- Most of the discussion is focused on chapter 6 and answering our research questions. Erjon thinks we should cut down on our amount of research questions, that 3 to 4 questions is too much given the time frame of the project (2 should be enough). We argue that the questions blend into each other and or not too distinct, and therefore should stay as they are. Nevertheless, we will look into it and see if we should make some changes to them.
- Erjon wonders if we should use our research questions as sections, and then have our existing content sorted and inserted as subsections or paragraphs under them.
- Asked for feedback/thoughts on the visuals on some of our graphs, and if we should change them based on a reader's first impression. Will ask Raymond the same thing.
- Will send an updated version of the thesis to Erjon this afternoon. Mark up what we want him to read and give feedback on. Work on this feedback next week as soon as it is received.
- Send a "final draft" to Erjon early Tuesday (16.05) at the latest, and schedule a final meeting on Friday (19.05).

2.7 Meeting with supervisor 19.05.2023

Present members: Dennis, Erki, Lars, Magnus, Erjon

Time: 12:15-13:00

Agenda: Progress update, discussion, feedback

Location: Online, Teams Meeting

Referent: Lars

Minutes:

- Timeline War in Donbas should lead into an aftermath chapter.
- Be more specific with titles?
- Move image of the deepfake to the first time it is mentioned.
- Simplify the names of the attacks in chapter 5.
- Insert a table with numbers for each type each quarter. Have it in the beginning of chapter 6.
- Move the most of Reconnaissance to chapter 2.
- We have too many research questions.

3 Meetings with client

3.1 Meeting with client 20.01.2023

Present members: Dennis, Erki, Lars, Magnus, Raymond

Time: 10:30-11:00

Agenda: Status update

Location: Online, Teams Meeting

Referent: Erki

- Recapped previous work
- bleepingcomputer.com, understandingwar.org are recommended
- In addition to "retelling" from sources, making assessments about them is also important.
- Russia is not as active in cyberattacks as expected. Theory: state-sponsored do not know about each other, so they are sent to fight in the war.
- Questions such as the one above are really important to impress for a better grade.
- Meeting with supervisor + client next Friday, 27.01.2023.
- Have a plan ready for the meeting to present for them.
- Invitation has been sent to the supervisor for the meeting next week.

3.2 Meeting with client 27.01.2023

Present members: Dennis, Erki, Lars, Magnus, Raymond

Time: 13:00-13:30

Agenda: Status update/presentation

Location: Online, Teams Meeting

Referent: Lars

- Present our project plan. Lead by Dennis.
- Erjon could not join.
- Include relevant sources from outside the main scope.
- Killnet attacked Germany when they approved tank donations, and Norway last June.
- Take the big questions and answers with a bit of uncertainty.
- Look at strategies and technologies, and why.
- Question Raymond wants included: Why haven't we seen more cyberattacks? It was expected when the attack occurred that there would be a lot more hacking attacks than what we have seen until now. Raymond thinks many hackers might have been drafted, but that is just his theory.
- Timeline on scope is OK, but the war started in 2014 and we need to mention this and be open to look at data from before 2022.
- Attack on oil installations before the attack to try and split Europe. Microsoft report is very important.
- Triangulation of sources.

3.3 Meeting with client 03.02.2023

Present members: Dennis, Erki, Lars, Magnus, Raymond

Time: 10:30-11:00

Agenda: Status update

Location: Online, Teams Meeting

Referent: Magnus

- Find one attack done by Ukraine and one attack done by Russia.
- Up to 4 days for Norwegian media to report an attack done by Russia.
- A lot is reported and sources must be verified.
- Find one thing said from official Russian media and see how long until international media reports it.
- A lot of misinformation from many sources.
- Russia has a lot of weapons, but it is very old. From the Soviet Union. Pictures showed up in media of Russian T34 being sent to Ukraine. Old weapons being taken into use. "Is the picture the truth?". T34 is still in use in Vietnam, North-Korea and Cuba. The picture was from export to Vietnam. Ukrainian propaganda.
- 1 piece of news from official Russian media. 1 hour to VG. 1 or 2 attacks in Ukraine from Ukrainian media. Does it take 2-4 days for verification.
- Receive Telegram-channels from Raymond. "Generalsvr" may be interesting. Possible close contact to Putin.
- Getting the timeline up and running is fine, but use this time to get an overview of the propaganda so you can be informed in the news.

3.4 Meeting with client 10.02.2023

Present members: Dennis, Erki, Lars, Raymond

Time: 09:30-10:25

Agenda: Status update

Location: Online, Teams Meeting

Referent: Lars

- Discussing IØ2000.
- First phase: Finish timeline.
- Second phase: What happened in the weeks before the war broke out. Then what happened during the rest of the war.
- We don't need to describe all propaganda attacks. Just that they're used a lot.
- They use a lot of ransomware/wiperware, trojans, supervisory control and data acquisition(ex stuxnet), IT vs OT systems.
- Raymond is interested that we can show width. To get an A we must show that we have learned new things. About 60% of our pages could describe different cyber attacks.

3.5 Meeting with client 17.02.2023

Present members: Dennis, Magnus, Erki, Lars, Raymond

Time: 09:30-10:25

Agenda: Review previous week and plan tasks for upcoming week

Location: Online, Teams Meeting

Referent: Erki

Minutes:

- Physical meeting on campus with Raymond on Tuesday 21.02.2023, 12:00.
- Recap what we worked on this week.
- Raymond explains a potential interesting source for information.
- "Most soldiers were from the two poorest states in Russia. Ingushetia... If a specific news he mentioned appears to be true, Raymond believes that the Norwegian media will report that some republics in Russia are rebelling and will demand independence from Russia."
- Ukraine informed that Russia had plans to invade Moldova. Russia denied.
- Raymond mentions that we should read the three reports he will send to us later on Teams.

3.6 Meeting with client 21.02.2023

Present members: Dennis, Magnus, Lars, Erki, Raymond

Time: 12:00-13:30

Agenda: Discuss progress and share information

Location: Topas building public area

Referent: Magnus

Minutes:

- Discussing some progress during this semester, including IØ-2000 etc...
- Showing our resources and research. Need to sort them and understand what we can use.
- Document that we sent mails to cybersecurity firms but received no answers. Shows initiative to collect information.
- 2 timelines for our task. 1.2.2022-1.2.2023 (Main timeline and scope) and 2014-2023 (background and war-information)
- Possible talk with professor that Raymond recommends about Ukrainian history and war. Raymond will contact him and ask.
- Current active operations: IT, pre-war: Operational tech attacks (OT). Netherlands is active in war operations. They have the largest gas-supply which is currently not active, but they may save Europe by opening it. MH17 plane from Amsterdam was shot down by Russia in 2014.
- PsyOps (Psychological operations). (Rasmus Paludan Quran burning) Destabilising NATO is a priority for Russia. Turkish election in May where Erdogan wants to win. Russia is trying to pressure/destabilize the Turkish election.
- Methods for attack: primarily DoS and DDoS. Shut down government institutions, power supply infrastructure and critical communications infrastructure. ("Non-violent methods")
Ransomware/Wipers. Destructive malware.
Data exfiltration for information which can be used for different purposes. "Kill lists", planned military actions, disinformation campaigns.
Spoofing to spread disinformation. Zelensky deepfake. Data-generated attacks for deceptive purposes in war.
- Actors: Russia (65-70% of our project is probably about Russia), Ukraine and friends (propaganda videos)
Organization map of Russian digital military services. FSB, SVR, GRU

- Impressed with structure in the task. Also shows broad understanding with information about other countries and relations pertinent to digital attacks and psychological operations.
- Don't describe what a DDoS is. Describe how a certain DDoS attack works in this specific war. What PsyOps are performed and how do they affect relations between countries.
- Russia plays 3D-chess. Complexity behind certain events may indicate Russian implication. But it is also easy to deny, but the implication is that a certain action will have a response by Russia.

3.7 Meeting with client 03.03.2023

Present members: Dennis, Magnus, Erki, Lars, Raymond

Time: 09:30-10:25

Agenda: Review previous week and plan tasks for upcoming week

Location: Online, Teams Meeting

Referent: Erki

Minutes:

- Client mentions that the history between Russia and Ukraine (+ other relevant regions) could be interesting and useful for the project.
- Delegate sources into most credible and less credible. If ChatGPT has major relevancy in finding some sources, we should clarify what we asked it. If we directly quote ChatGPT, we have to mention that.
- Fancy Bear attack in 2014 against Ukraine.
- Define types of attack early, so that it doesn't have to be done (possibly repeatedly) later in the thesis.
- Perhaps use ChatGPT to assist in formatting/making templates/etc. in Overleaf/LaTeX.
- If we find news that might seem a little less credible (or "too good to be true - Raymond"), we should find at least 3 sources on it.

3.8 Meeting with client 10.03.2023

Present members: Dennis, Magnus, Lars, Raymond

Time: 09:30-10:25

Agenda: Present our progress so far

Location: Online, Teams Meeting

Referent: Dennis

Minutes:

- Raymond asked how our progress has been so far.
- Magnus and Dennis explained where the group is regarding the amount of good sources and how much has been written until now.
- We are reminded that the abstract and preface should be written when all else is finished.
- Raymond talks about how we should work on writing parts of the report. Our group should start with the "results" and then write about our methods.
- General discussion about the state of the conflict the past few weeks. Bakhmut, Vuhledar, the Wagner-group.
- Raymond talked about being critical towards all information we find, and that there will also be bias in western "reputable" sources. We are encouraged to always try to find multiple sources for everything we write about.
- Showed Raymond our document. He provided constructive criticism and tips.
- Important to note that the war is not over when we deliver.

3.9 Meeting with client 17.03.2023

Present members: Erki, Magnus, Lars, Raymond

Time: 09:30-10:25

Agenda: Present our progress so far

Location: Online, Teams Meeting

Referent: Lars

Minutes:

- Raymond talks about the presentation by the Professor Karl Erik Haug.
- Talks about how Russia thinks Ukraine should not exist.
- No higher diplomatic rules apply for Russia anymore. Death threats to other nations leaders and politicians.
- Talks about the brutality and suppression of the Russian peoples for the past 500-600 years.
- Write an introduction with historical philosophical questions.
- If we have any questions for Prof. Haug, just send him questions.
- Go through what was said on Thursday and see if we have any other questions.

3.10 Meeting with client 31.03.2023

Present members: Dennis, Magnus, Raymond

Time: 09:30-10:03

Agenda: Progress update, discussion

Location: Online, Teams Meeting

Referent: Dennis

Minutes:

- Discussed what we have been working on the previous weeks, and how working on IØ2000 has impacted our work on our thesis.
- Raymond tells us how even though IØ2000 can seem disruptive to our work, it still has it's merits and will be useful in future.
- Talked about how it seems that Russia "burned a lot of bridges" regarding cyber-attacks. They had access to Ukrainian systems at first, but after launching their attacks, have not been able to regain access to new systems. One must discuss if this is due a better cyber-defense by Ukraine, or a loss of capabilities from Russia's side.
- Raymond was very impressed with the above. He said that what we told him was central to our thesis, and that it's important for us to build upon it, and write about it in a way that secures a good letter grade.
- Raymond tells us about how he uses ChatGPT in his work (search engine, re-writing his text, spell checks). He says that we could also use it as a tool to secure better academic writing.
- Raymond talked about how the fact that the conflict is ongoing presents us with other issues than other groups face for their thesis'.
- Though there is no documentation, Raymond thinks that the reason Russia hasn't deployed more offensive cyber-operations is due to Russia having 3 intelligence organisations that don't work together. Due to mass mobilisation, Raymond thinks that young professionals working in the cyberdomain for these agencies have been drafted.
- Building upon that, one can also presume that many Russians with the competency required to work on large-scale cyber-operations have fled the country.
- Discussed historical parallels to the conflict (eg. "Operation Paperclip").
- Raymond asked us what we think about how Russian propaganda seems to increase in line with their low performance on the battlefield. Discussion.

- Raymond is very clear on that we have to take time off work during the Easter-break. He says that in this final phase of the project, it's important that we avoid getting burn out.
- Raymond is overall impressed by our level of understanding of the conflict, general knowledge, and our conclusions. He is looking forward to reading our final product, and thinks we will do well.

3.11 Meeting with client 14.04.2023

Present members: Dennis, Erki, Magnus, Raymond

Time: 09:30-10:03

Agenda: Progress update, discussion, guidance

Location: Online, Teams Meeting

Referent: Erki & Dennis

Minutes:

- Discussing our progress, slightly behind schedule due to misunderstanding when working on chapter 3 "Methods". No more than a day's setback.
- Client is interested about the timeline, and wants to see it on the next next meeting next Friday.
- Client wonders about our observations about the whole conflict, and how we interpret the attacks. Is satisfied with our findings until now.
- Raymond also stated that he needs a rough timeline on cyberattacks for the period from before the illegal annexation of Crimea and the full-scale invasion in 2022 (2012-2022). Wants us to present parts of this next week.
- In the observation (results?) chapter, take what has happened, describe it, compare it to the timeline, "what does it mean?", show how repeated cyberattacks were targeted for a reason other than plain harassment.
- If we decide to use a psyop as an example, Raymond vaguely recommends using the demonstration in Sweden, with Paludan burning the Quran in front of the Turkish Embassy (Not cyber though).
- Short discussion about the recent leak of Pentagon documents concerning the war in Ukraine.

3.12 Meeting with client 28.04.2023

Present members: Dennis, Magnus, Lars, Erki, Raymond

Time: 09:30-10:30

Agenda: Progress update, guidance

Location: Online, Teams Meeting

Referent: Magnus

Minutes:

- Reconnaissance as an attack method: IPOE (Intended Planning of Operational Environment) is important for war.
- To show understanding and learning something from cyberattacks in war: Understand that a cyberattack in a (Cyber Kill Chain) can be the reconnaissance part in the war effort and further attacks can be more destructive.
- Baltic countries have been 100% sure that Russia could invade a neighboring country in the past 10 years. Rearmament of tanks and artillery show that these countries are aware of Russian warfare. This is due to reconnaissance.
- Have a "questions" chapter where you look at potential Russian reconnaissance against neighboring countries as a potential prelude to invasion of Ukraine.
- Cyber Kill Chain part 2: Prepare the battlefield when you are going to fight a war. Perform reconnaissance.
- Change "pre-war timeline" to another name.
- Raymond is very impressed with our LaTeX capabilities and structure of the document.

3.13 Meeting with client 05.05.2023

Present members: Dennis, Lars, Erki, Magnus, Raymond

Time: 09:30-10:15

Agenda: Progress update, guidance

Location: Online, Teams Meeting

Referent: Erki

Minutes:

- Results: pure results from what we have observed
- Discussion: what do these results mean? We will use this chapter to discuss how, why etc. we used the methods
- Conclusion: Focus on the big picture, find and create a general statement(s) that is based on our results. Nothing new should be presented here.
- Structure: focus on clear language, so that it is understandable for the future readers (correctly placing commas, etc.); we will perform numerous instances of proofreading to ensure this.
- Presenting a 2 minute summary to Raymond about the most important results that we have discovered.
- Russia and their agencies are disorganised, which could indicate that this could have been the reason behind the reduction in cyberattacks.
- Ukraine/Zelenskyy uses Telegram that is knowingly monitored by Russia and could be used for finding geolocations, however they are unable to avoid detection by applying measures/methods.
- How would the war have gone if Ukraine was unable to counter the cyberattacks during the war (especially the beginning)? Perhaps it would have given Russia a considerable advantage? What are the connections of cyberwarfare to conventional warfare?

3.14 Meeting with client 12.05.2023

Present members: Dennis, Erki, Lars, Magnus, Raymond

Time: 9:30-10:30

Agenda: Progress update, guidance

Location: Online, Teams Meeting

Referent: Erki

Minutes:

- Final draft Monday 15.05, will be sent to supervisor and client
- 01.06, meeting with Raymond on campus. Lars is unavailable due to an exam the same day, however the other members will be available.
- Discussing our conclusion about the conflict; What have we found out?
- Discussing the feedback from the supervisor, and what we did to improve upon it.
- Raymond approves of the research questions and how they have been limited.
- Raymond says that he is impressed with our work.

"Bachelor projects are mostly about researching what already exists and what has been found out beforehand. Making new theories and discovering groundbreaking information about the task would be considered as above the level of Bachelor's degree." - Raymond

3.15 Meeting with client 19.05.2023

Present members: Dennis, Erki, Magnus, Raymond

Time: 9:30-10:05

Agenda: Progress update, guidance

Location: Online, Teams Meeting

Referent: Magnus

Minutes:

- "Sandworm theory" interesting. Explain a bit more. - Raymond
- Raymond praises our product
"Jeg synes dette er veldig, veldig bra." - Raymond
- Most important in Abstract: "Literature study of ongoing war. See how cyber has been used in an ongoing war. Present the 4 methods we have seen."
- In Abstract: "Aggressive, destructive attacks have been seen since 2014. Russia stepped up their intensity right around the start of the invasion."
- Cyberattacks are used in the mixed methods of a hot war. Cyberattacks are being used in modern conflict and we see this throughout the course of the conflict.
- Raymond believes we have done a great job with our work. Our content, structure and methods are high-level.
- Write a 3/4 page Abstract.
- Use Raymond as a contact later in our careers.

4 Other meetings

4.1 Lecture on Ukraine 16.03.2023

Present members: Dennis, Magnus, Raymond, Karl Erik

Time: 10:00-11:00

Agenda: Lecture on Ukraine

Location: Online, Teams Meeting

Referent: Magnus

Minutes:

- "How can Russia argue that Ukraine is not a country?"
- A lot we don't have the answer to in this conflict. How should we understand Russia?
- When Russia attacked Ukraine: free Ukraine from the Nazism. Putin said Ukrainians are Russian. "A great Russia"
- We understand the world based on what is around us. "Our box" and what is outside our box. 9. April 1940 when Norway was invaded. Reporters followed German troops into the city. The word "War" is missing from the interviews and reports.
- November 2021: NATO was sure that this invasion was possible. But argued what was actually happening. NATO had information: blood hospitals
- Western society/democratic people have a rational view that freedom is what people want. Revolutions and war are outside our box.
- Power = "Vlast" in Russian. You have power because you practice it. If you don't use it you lose it.
- Relatively new borders between Ukraine and Russia. Is there a relatively strong difference between how Ukrainians and Russians think?: "Likely, based on the past year of actions"
- Ukraine vs Russian sovereignty is more different than Norwegian vs Swedish.
- Donbas-area has a very tight relationship with Russia. Donbas has been relatively Pro-Russia.
- Building a society through war effort.
- Ukrainians with Russian family and close ties to Russian culture still identify themselves as Ukrainian.

- Russian military doctrine is based on Soviet Union doctrine. It has not changed much. This allows Russian military to view infantry as expendable.
- No "Renaissance" in Soviet. Tsar until 1917. Communist regime since 1919 to 1991.
- Putin wants to bring back a great historical Russia. But this history does not exist. Munich 2007 speech.
- Putin did not foresee the consequences of the invasion. He expected that the West would not react and ally themselves.
- Geo-economics. Energy becomes a weapon.
- 2010. NATO has a task to implement Russia as an ally.
- Caucasus and Georgia are important resources to Russia.
- Russia, communist or fascist? Putin is a fascist based on his race-theory views.
- Our understanding of corruption is based on individual to individual. Russian corruption is systemic: Money moves upwards.
- Putin is using the common views on Nazism as a driving force behind the invasion. The fight against Nazism still stands strong in the Soviet/Russian society.
- Putin has started nation building in Ukraine. This would otherwise have taken a long time. Norway did this in the 1800s. A minority (Russians in Ukraine) which needs to be protected against the majority of the Ukrainians.
- What is a nation? What constitutes a nation? Nationalism appeared in the Balkan area in 1991/92 after the fall of the Soviet Union.
- People of the old soviet states said: The Russian bear must go. There has to be a way to remove it.
- China's relation to Russia does not depend on Russia but on the US and the West. Resources from the US are more important to China than the exporting from Russia.
- Superpowers balance each other. China builds unknown capacities. Russia fight for power and to grow greater.
- The Norwegian Armed Forces and NATO state in 2005: War between states is very unlikely. Wars would be fought together and against others.
2008: War between Russia and Georgia, leading to us having to rethink things.
- Cannot trust anything which the Russian state proclaims.
- Putin has succeeded in growing NATO's influence. We may see further NATO countries in the close future after the end of the war. (Moldova, Georgia, Ukraine)

This page intentionally left blank.



NTNU

Norwegian University of
Science and Technology