Cyber operations and kinetic conflict: Cyber operations and kinetic conflict

Grdic Kukulic, Tina

Universiteit Leiden

Cyber operations and kinetic conflict

A thesis submitted in fulfilment of the requirements of the Master of Science: Executive Master's Programme in Cyber Security degree, Faculty of Governance and Global Affairs, Leiden University

Author: Tina Grdić Kukulić

Supervisor: Dr. Daan Weggemans

Second Reader: Dr. Alexandru Stefanov

19th March 2023

Table of Contents

Table of Figures

List of Abbreviations

APT	Advanced Persistent Threat
CERT-UA	Computer Emergency Response Team of Ukraine
CFR	Council of Foreign Relations
CIA	Confidentiality, Availability, Integrity
CISA	Cybersecurity and Infrastructure Security Agency
CNA	Computer Network Attack
CNE	Computer Network Exploitation
DLL	Dynamic Link Library
DNS	Distributed Name Server
DDoS	Distributed Denial of Service
DoS	Denial of Service
EPRS	European Parliamentary Research Service
EU	European Union
GPO	Group Policy Object
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre
NIST	US National Institute of Standards and Technology
TCP/IP	Transmission Control Protocol/Internet Protocol
UK	United Kingdom
US	United States
USSR	Soviet Union
VPN	Virtual Private Network

Chapter 1 – Introduction

1.1 Cyberspace and warfare

At the dawn of February 24, 2022, Russia invaded Ukraine.[1] Tanks and aircraft entered the country and unleashed fierce strikes. Heavy bombardment of cities, hospitals, and residential buildings made the global news.[2] Thousands fled homes in search of safety, and many were killed. While kinetic conflict raged across the land and air, the "invisible" warfare occurred in cyberspace.[3] Adversaries deployed cyber operations against state and private organizations, damaging and disrupting digital services. Among others, they performed denial of service (DoS) attacks that obstructed bank services and telecoms, leaving citizens without access to their finances and the Internet.[4] Likewise, data wipers were executed, infecting border control systems.[5] As a result, the escape of the Ukrainian refugees to neighbouring Romania was delayed as their data had to be processed manually. In peacetime, such attacks would cause inconvenience and primarily financial damage. But, during wartime, their effects can impact the state's security and society. For instance, military defense systems can be obstructed, preventing the timely identification of enemies entering the state's airspace. Similarly, due to the unavailability of banking services, citizens may not be able to obtain the finance to flee the unsafety of a war zone.

The use of cyber operations in the context of war or conflict emerged in the last decades following the rapid development of information technology (IT).[6] The new and powerful tools enabled fast network connections, quick processing abilities, and instant access to data. Countries hurried to digitalize their services for accessibility and efficiency. But, the growing complexity of the systems has led to increased vulnerabilities, which actors, such as other nations, can exploit.[7] In response, states started building their offensive and defensive cyber capabilities. By 2022, forty countries, including the United States (US), Estonia, and Nigeria, claimed to have established a cyber command.[8] And according to the largest military Alliance, North Atlantic Treaty Organization (NATO), having adequate cyber capabilities is a must in modern, hybrid conflict. While wars were long fought only on land, air, sea, and space, they can now occur in and through the fifth domain, cyberspace.[9] NATO even considers that it may be possible to suffer from such a cyber-attack that can match an armed attack in intensity.[10] And if it occurs, in response it could invoke a collective defense from all member states.

Still, critics claim that we should not expect events resembling cyber-9/11 or cyberwar. Instead, cyber operations are better suited for performing activities below the threshold of armed conflicts, for example, espionage, sabotage, and subversion.[11] With those operations, states can accumulate gains over time, finally leading to the accomplishment of strategic goals.[12] For

instance, by breaking into opponents' systems, states can gather intelligence on, e.g., military equipment designs. Those can be used to pinpoint weaknesses or build equipment with equal or better capabilities. Both scenarios can result in strategic advancements.

In short, cyber operations are versatile tools that can be used in numerous ways and with different goals. Therefore, they have the potential to contribute to shaping international relations, either as a part of modern warfare or as a standalone means.

1.2 Research on cyber operations in warfare

The growing number of (state) actors in cyberspace and increased threats to nations' digital services caught the attention of researchers, policymakers, and military officials. For decades, they have been contributing to the debate on topics such as cyberwar and cyber operations, discussing their (warfare) utility.

Among the first to discuss the phenomenon of the freshly discovered cyber capabilities were defense scholars Arquilla and Ronfeldt (1997). In their work from 1997, "Cyberwar is Coming!", they said that technological advances changed warfare and that "cyberwar" will likely occur.[13] And by cyberwar, they meant disruption or destruction of systems that store key knowledge on opponents' military structure, such as troops' locations and imminent threats. They also suggested that besides disruption, the collection of such data could help with planning surprising attacks. Hence, for them, cyberwar was about getting or destroying digitally stored information to ensure their advantage in, and outside of the conflict. Those thoughts partially overlap with the opinion of Thomas Rid (2013), who extensively explored the subject. In his well-known work, "Cyberwar will not take place", Rid argued that cyber operations are used to perform espionage, subversion, and sabotage.[14] According to him, catastrophic cyberattacks or cyberwar did never occur, nor will happen. Rid explained that because there is no cyber offense that can meet all criteria of war, and those are that it needs to be violent, instrumental, and political. However, he acknowledged that the cyber operations could be used in military actions or even be critical for its success. In support of this claim, he pointed out the case from Syria, which occurred in 2007. Namely, during Operation Orchard, Syrian air defense systems were manipulated with cyber operations, which ensured that Israeli warplanes entered the country's airspace undetected. That allowed them to perform raids on what was allegedly a nuclear facility.

Scholar Eric Gratzke (2013) also agrees with Rid's opinion. He argues that cyber-attacks can only contribute to achieving military goals when deployed jointly with terrestrial forces.[15] That is because cyber operations as a standalone resource have limitations. While they are costly, their effects are short-lasting and reversible. According to him, damage resulting from shutting

airports or power grids with cyber-attacks can be repaired with moderate resources. So, per Gratzke, cyber operations cannot be the final arbiter in any conflict. Similarly, David Betz and Tim Stevens (2011) acknowledged that the military cyber-power is an important complement to other military capabilities. Still, regardless of that, cyber means did not change the nature of war.[16] Per Martin Libicki (2014), their contribution to warfare would probably be modest.[17]

On the contrary, state, military, and intelligence officials continuously express their worries regarding cyber operations and their devastating potential. Former director of the Central Intelligence Agency, Leon Panetta, famously said there is the possibility that a "cyber-Pearl Harbour" will occur.[18] He expected that a single, sophisticated malware attack could paralyze the country by disabling the critical infrastructure.[19] According to Mike McConnel, former director of the US National Security Agency, cyberwar can occur and, if it happens, it can damage our way of life as drastically as a nuclear attack.[20] In his view, coordinated and continuous cyber-attack from afar on the US electric grid, transport, and banking system could result in damage that is as significant as one caused by the nuclear weapons.[21] In the same vein, a senior Chinese general stated that the consequences of a large cyber-attack may be "as serious as a nuclear bomb".[22] Lastly, in the opinion of Russian President Vladimir Putin, cyberattacks could cause more significant damage than conventional weapons.[23]

This brief overview of the discussion on cyber operations and warfare has a common denominator: the belief that cyber operations have their place in modern conflict. However, the opinions part when it comes to an understanding of their effects and impacts during warfare. While some expect doomsday scenarios, others take it lighter. That might be to an extent because the research often included theorizing and describing single conflict events and re-analysing a handful of well-known cases in which military and cyber operations were seemingly coordinated.[24] Not many empirical analyses have been done to add to the debate on their utility in warfare. However, those are much needed to deepen the understanding of the subject further.

1.3 Aim, motivation, and research question

The goal of this research is to gain more insights into warfare' changing nature by exploring cyber operations' role in modern conflict. As previously noted, today's armies maintain military and cyber capabilities, which can be deployed in concert to support the broader use of force.[25] When writing this thesis, one case of such warfare is taking place in Eastern Europe. During the already mentioned Russian war on Ukraine, cyber operations appeared integral to the conflict. For instance, some reports indicated that media companies in Kyiv were attacked with destructive malware in early March 2022, a few days before and after missiles hit the Kyiv

television tower. [26] Similarly, the Ukrainian nuclear power company was targeted with a cyber-attack the day after the largest nuclear plant fell under Russian occupation.

All those events occurred during the recent, less-studied conflict and therefore served as motivation for the following research question:

"What role do cyber operations play in kinetic conflict?"

This thesis aims to first answer the question conceptually by exploring the existing literature. Then, to contribute to the study of cyber operations, this research proposes a modified, literature-based framework for assessing their role in kinetic conflict. The framework is tested using data from the 2022 Russian war on Ukraine, selected as this thesis case study. This ongoing conflict was chosen during the planning of this thesis as it was not yet extensively studied in this context. The case study analysis results delivered the data-driven answer. The combined insights from the literature review and outcomes of data analysis contributed to building up a holistic answer to the research question.

1.4 Thesis Outline

This thesis is divided into five segments: literature review, introduction to the case study, research method, data analysis, and finally, the conclusion.

The answer to the research question is first sought in the literature on the subject. The literature review (Chapter 2) discusses cyber operations, how they can be used, and their shortcomings. During the exploration, several theories and classifications were identified that could be utilized to analyse cyber operations in the context of kinetic conflict. Those theories explain the types of cyber operations, their effects, and the logic of integration into the military structure. Hence, this chapter serves to conceptualize the answer to the research question.

Following the literature review, an introduction to the description of case study is provided (Chapter 3). As identified in this initial chapter, the current body of research seldom contains the structured analysis of data correlating cyber operations and military actions. That was mostly the case, as not many events could be observed in this context. However, the current war in Ukraine provided an opportunity for data-supported analysis; therefore, it was selected as the case study for this research. To provide background on the chosen case, the chapter examines key military and cyber events from the ongoing war and presents an overview of the modern Russo-Ukrainian relationship.

Then, the research method is outlined. It includes a description of the proposed assessment framework, details data collection, and discusses possible limitations (Chapter 4). The research aims to gain insight into the types of cyber operations that occurred during the beginning of the

Russian war on Ukraine and what were the effects they achieved. Moreover, the goal is also to understand how they were integrated into the kinetic conflict. The data analysis results are summarized, and the usability of suggested framework is discussed (Chapter 5).

Lastly, the outcomes of theoretical exploration and data analysis are discussed in the conclusion to answer the research question "What role do cyber operations play in kinetic conflict?" (Chapter 6). Besides the conclusion, the chapter suggests future research opportunities.

Chapter 2 - Cyber Operations: Literature Review

This chapter introduces the concept of cyberspace and discusses cyber operations which can occur within or through it. It explores the role of cyber operations in the military context by reviewing which effects they can achieve and how they can be integrated into the conflict. Additionally, it discusses their shortcomings.

2.1 What are cyber operations?

Cyberspace is complex environment which does not exists in physical form, in which people, services, devices and networks are interconnected.[27] It is "macro resilient and micro vulnerable".[28] That means cyberspace is a stable environment, yet its participants have weaknesses that can be exploited.[29] The latter characteristic is attractive to many cyberspace actors, such as criminals and hacktivists, which seek to inflict damage on their targets. But, having the possibility to "digitally" harm and weaken the enemies also became an area of interest to many nation-states. Consequently, states started developing cyber capabilities, a mixture of skills, technology, and organizational attributes.[30] These equipped them with abilities to execute cyber operations, or "actions for achieving objectives in or through cyberspace".[31] The objectives of cyber operations are twofold: to offend the opponent's digital services or to defend its own. Hence, it is necessary to differentiate between offensive and defensive cyber operations.[32]

Offensive cyber operations are used to perform computer network attacks (CNA) and computer network exploitation (CNE). A CNA serves to access, alter, delete, corrupt, or deny access (to data and systems). It includes actions designed to destroy or otherwise incapacitate enemy networks to execute sabotage.[33] A well-known example of the CNA is Stuxnet, the "poster child of industrial malware", and the first discovered "weaponized computer malware".[34] The malware, released in 2007, was allegedly developed by the US and Israel to undermine the Iranian nuclear program. The malicious program was highly sophisticated and customized to propagate through the industrial control systems in the Natanz nuclear facility. Once it found the specific controllers, it managed to speed up centrifuges for the uranium enrichment, causing their destruction.[35] At the same time, the program reported false statuses to the operators, avoiding detection for a prolonged period.[36]

As opposed to the CNA, CNE serves to obtain information without affecting the functionality of systems and the data.[37] This cyber operations type is used for intelligence gathering or espionage, where adversarial networks are penetrated to obtain confidential information, all covertly. An instance of a (publicly) disclosed cyber espionage operation is Titan Rain, a

campaign allegedly performed by Chinese state actors.[38] Malicious intruders managed to access unclassified networks in the US and United Kingdom (UK) departments and ministries (e.g., Army Aviation and Missile Command, Ministry of Defense), and have stolen at least 10 to 20 terabytes of data.[39]

Defensive cyber operations are measures to protect own and friendly networks and systems.[40] States can implement numerous technical and administrative mechanisms to safeguard their digital assets.[41] For instance, they can install antimalware programs on endpoints (e.g., servers and workstations) to prevent infections with malicious software. Another case includes establishing and operating a security operations center. This unit can employ skilled individuals who can timely identify security incidents and perform mitigating actions.[42] Furthermore, states can protect their assets by applying specific configurations to systems to minimize the attack surface and installing secure software updates to prevent exploitation of known vulnerabilities.

Nevertheless, countries can as well perform even more targeted defensive cyber operations. For instance, the US identified that cyber threat represents a credible risk to their security – and if the risk is materialized, it can cause "death by a thousand cuts".[43] The US is especially concerned about possible cyber-attacks targeting their critical infrastructure and enabling espionage. Therefore, besides the traditional defense measures, the States also operate "defend forward" and "persistent engagement" activities. Namely, US cyber experts use (offensive) cyber operations to damage the opponent's cyber capabilities and infrastructure, causing high costs and damage. Hence, the US defends its networks from being attacked by impairing the enemy's ability to strike.

While for exploration in this thesis, both types can be relevant, the offensive cyber operations are further examined. This research focuses on cyber operations against Ukraine; therefore, the "attacking" cyber capabilities are of higher importance. While defensive cyber operations and protection measures are relevant, they are mostly kept in secrecy and, thereby, even more, challenging to assess.[44] For similar reasons, espionage activities that fall in the category of offensive cyber operations have been excluded from the assessment. That is due to their clandestine nature and lack of direct capability to offend systems and data.

2.2 Offensive cyber operation types and effects

So far in this chapter, two main categories of cyber operations have been discussed: offensive and defensive. As this thesis focuses on offensive cyber operations, it is necessary to discuss types of offensive cyber operations further and examine which effects they can produce when deployed.

2.2.1 Types of cyber operations

While exploring literature on cyber operation types, it was observed that organizations and authors discussed and classified cyber-attacks based on the effects they can produce (e.g., disruption).[45] However, the classification of effects alone does not provide insight into what type of cyber operations was used to achieve it. Then, in other cases, cyber operations were presented on a granular level, focusing on the actual means to perform them (e.g., logic bomb, a computer virus).[46] But, those means are subject to change – they can cease to be relevant or experience exponential growth in types over time. Thus, centring around means hinders the opportunity for a high-level classification, which could bring all attack types under the common umbrella.

This thesis aims to assemble a framework for analysis of cyber operations in conflict, which is then tested during the assessment of case study data. Therefore, the categorization of attack types on a more abstract level could reduce complexities during data evaluation (e.g., for cases where information on the actual means used to perform cyber-attack is unknown). Moreover, it would ensure that the framework remains operational over time.

For that reason, the categorization of cyber-attacks described by scholar Max Smeets (2022) has been selected for inclusion in the data analysis framework. He clustered cyber-attack types into three overarching groups: DoS, data manipulation, and system manipulation.[47] The author created a separate category for grouping the attacks on industrial systems such as the one controlling the electrical grid operations. However, to achieve the effects (e.g., power outage), the data (specific setting) should be modified or changed. Therefore, system manipulation could be considered a subcategory of data manipulation. While in some cases this category could be eliminated, in this thesis it has been kept as it directly implies the target type. Since industrial systems are regularly part of a state's critical infrastructure, the attack on them rightfully merits a separate category. Therefore, due to an adequate abstraction, the three categories present a viable frame for classifying the cyber operation types used in kinetic conflict.

The remainder of this section discusses three types of cyber operations: DoS, data, and system manipulation in more detail.

Denial of service

DoS deprives legitimate users of the services they are entitled to.[48] The DoS attack is performed by overwhelming the targeted system or network with traffic until it becomes unresponsive. In that way, legitimate users cannot access the service, and the victim organization can suffer operational and monetary costs. Some of the well-known attack techniques for executing DoS are Smurf and SYN Flood.[49] In the Smurf attack, the malicious actors use Internet Control

Message Protocol (ICMP) to broadcast packets to devices on the network by using the victims' Internet Protocol (IP) address as a source. Once the devices on the network receive the packet with a spoofed IP address, they will send their response to the targeted host, flooding it with responses and making it unavailable. In an SYN Flood attack, Transmission Control Protocol/Internet Protocol (TCP)/IP network protocol properties are misused. The TCP/IP protocol is utilized in network communication between the devices. To start the connection, a three-way handshake should occur between the parties. In an SYN attack, the attacker begins a handshake by flooding the targeted system with initiating SYN packages. Since the attacker never replies to the requests, the victim system ports become occupied, preventing legitimate users from connecting.

Furthermore, DoS attacks can also be executed from multiple systems instead of one location.[50] Such a type of attack is named Distributed Denial of Service (DDoS). Typically, to perform DDoS, adversaries misuse vulnerabilities of various network-connected devices to gain control over them. Once they are in control, they can organize compromised systems into "botnets". Botnets can then attack a party with many requests, magnifying the effects. DDoS attacks are more challenging to solve for their victims, as the attacking systems are mainly distributed worldwide and are subject to change.

Additionally, since many devices are used to perform DDoS, it is also challenging to identify the malicious actors behind them.[51] The resolution for DoS attacks can be blocking the malicious IP or changing the name and IP address of the victim. However, to resolve large-scale attacks, which comprise thousands of changing IP addresses, organizations may need the assistance of their Internet Service Providers (ISP), or they can use specific network appliances to reroute or stop the malicious traffic.[52]

An example of a DDoS cyber operation is a well-known cyber-attack on Estonia in 2007. This digitalized state was a target of a series of DDoS attacks that lasted for weeks.[53] Adversaries targeted web servers, email servers, Distributed Name Servers (DNSs), and routers used by different sectors, such as government, media, finance, and telecom. As a result, the underlying IT infrastructure became unresponsive and unavailable to citizens.[54] The attacks allegedly caused by Russia produced reputational and financial losses to Estonia and its organizations.[55]

Data manipulation

Data manipulation assumes the modification of data to achieve an effect.[56] More specifically, in cyber security, data can be manipulated to impair its Confidentiality, Availability, or Integrity (also known as CIA Triad).[57]

Confidentiality relates to keeping the data private or secret. A famous example of a data confidentiality breach is the Equifax hack.[58] Equifax is one of several credit rating providers in the US, and in 2019 it was the target of a cyber-attack. Malicious actors have exploited application vulnerability on the servers to steal the US residents' private data such as social security numbers, birth dates, addresses, and similar. The total costs of the breach were estimated to be 700 million dollars, and numerous citizens suffered from loss of privacy. The US department of justice announced charges against Chinese military-backed hackers in connection to this attack in which the private data of nearly half of US citizens were stolen.[59] Confidentiality breaches in the context of cyber operations are closely related to espionage activities, which, as discussed, are not explored in this thesis.

Availability relates to data being accessible to consumers when needed, and in a way, it was intended to be available.[60] One instance of cyber operation that endangered data availability is the NotPetya case. In 2017, attackers planted the NotPetya malware on the updated servers of Ukrainian accountancy software.[61] The malware was pushed to the user's devices as the software update file. Once users executed the code, it encrypted their devices and data. At first, the incident resembled a ransomware attack, as payment was requested in exchange for the decryption key. However, the code analysis showed that the keys for encryption were randomly generated and thus unavailable to the attacker. That confirmed that the end goal of the attack was destruction rather than financial gain. Malware destroyed the data of Ukrainian enterprises and multinational companies with offices in Ukraine, such as Maersk, Merck, and FedEx.[62] Due to the cyberspace properties of interconnectedness and lack of borders, infections swiftly spread globally. The financial loss caused by the attack is estimated to be 10 billion dollars. The US Government accused Russia of sponsoring the attack as "part of an ongoing effort to destabilize Ukraine".[63] The Russian officials denied involvement, calling the accusations "Russo phobic".[64]

Lastly, data integrity entails being kept free from unauthorized modification and therefore being accurate, reliable, and trustworthy.[65] Web defacement attacks are well-known examples of data manipulation.[66] In such an attack, adversaries manipulate website configuration and data to replace original content with their own. Often the defacement is performed to propagate inappropriate content and religious and political messages. Attackers can change files by, e.g., misusing unauthorized access to servers. Such a defacement attack, in which adversaries deleted the content of websites and planted their own, occurred in January 2022 in Ukraine. Hackers defaced governmental websites just a month before the start of the Russian invasion. The message told Ukrainian citizens that all their private data was breached and then destroyed on their local devices and mentioned the ethnic cleansing of Polish people.[67] By displaying those

messages, attackers aimed to create discord between ethnic groups and saw distrust in the government.

According to Smeets (2022), data manipulation can be accomplished in three ways: encrypting, deleting, and modifying it.[68] All three actions could directly impair the data availability and integrity principles, as demonstrated in provided examples. Per his classification, the confidentiality principle is not considered. The loss of confidentiality is intimately related to data intelligence (espionage), an activity not explored in this thesis.

System manipulation

System manipulation refers to changing the (industrial) system to achieve the effects.[69] Adequate examples of such cyber operations are related to deploying various industrial malware. Two such notable attacks occurred in Ukraine in 2015 and 2016, in which adversaries targeted industrial control systems controlling the electrical grid. The attack in 2015 was the first publicly acknowledged cyber operation that disrupted the power grid. While no party claimed responsibility for attacking the critical infrastructure, it is suspected that the Russian state or its affiliates performed the operations.[70] The attack occurred in December in Ivano-Frankivsk Region (western Ukraine) and caused a blackout that lasted three hours and affected 225,000 citizens.[71] The attackers performed reconnaissance and identified plant operators to whom they had sent spear-phished emails. Operators opened emails and executed the attached Excel file. That caused the installation of BlackEnergy3 malware, which was obfuscated in a macro task. The malware stole the operator's credentials and established a persistent backdoor on the business devices. Attackers compromised domain controllers (authentication servers) from which they harvested additional credentials. Then, they misused stolen information and poorly designed network access controls to move laterally into the industrial network. There they connected to the controllers and opened circuit breakers, causing blackouts. The sophisticated attack also included actions to prevent effective incident response and resolution. For example, the call center was congested with fake calls to prevent customers from reporting the problem, backup power was cut in the data center, and industrial systems disks were made unusable with the KillDisk utility.

The second attack on the power grid occurred in December 2016 in the power plant of the Kyiv region. The malware named CrashOverride was installed on the systems of the electric plant Ukrenergo.[72] Like in the attack in 2015, the circuit breakers were opened to cause an electricity outage, which lasted for more than one hour. During this incident, the operators swiftly

responded by manually restoring the state of the circuit breakers. Allegedly, the attack was conducted by the Russian state actors, the Sandworm group.[73]

2.2.2 Narrow effects of cyber operations

The section above discussed the cyber operation types. In this section it is discussed what are the possible effects they can achieve.

In literature and industry, the cyber operations effects are frequently expressed with comparable terminology. For instance, the Australian Strategic Policy Institute claims that cyber operations are used to "manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks".[74] Analogously, the US Air Force sees they can "destroy, deny, degrade, disrupt, deceive".[75] Some scholars and institutes, such as the US National Institute of Standards and Technology (NIST), provided a narrower outlining of the effects by compiling them into four categories: "disrupt, deny, degrade and destroy".[76] But, the properties of effects are often not further specified for clarification. Therefore, their definitions were searched in Cambridge University Dictionary.[77]

According to the Dictionary, the "deny" effect relates to not allowing someone to have or do something. In the context of cyber operations, this can be mapped to the impact of a denial-of-service attack, which prevents a user from accessing digital services, such as online banking. "Degrade" concerns spoiling or destroying the quality of something. For instance, cyber-attack can impair organizational network devices, and in turn, the users may not be able to access the required data on the agreed-upon network speed levels. "Destroy" entails damaging something so severely that it cannot be used. An example of destruction is permanently deleting a database that contains critical military information. Finally, "disrupt" implies preventing something from continuing as usual or as expected. Cyber-attack can disrupt the operations of electrical grid control systems, resulting in a power outage.

It could be argued that "degrade" and "disrupt" have the common denominator of not being permanent states. If the quality of something ("degrade") is hindered, and something is not continuing as expected ("disrupt"), it does mean that it is continuing, but on unpredictable and unexpected (capacity) levels. Translated to the cyber realm, the attack on ISP could result in preventing end-users from utilizing the Internet with expected bandwidth ("degrade") and at expected times ("disrupt"). Both of those share similarities with the "deny" effect - as by its definition, denying is not allowing someone to have or do something. On the contrary, the "destroy" effect appears permanent. For example, once the data is wiped or deleted from the system, it cannot be accessed periodically or partially. Therefore, it can be concluded that the

destructive effect is an everlasting "deny". Per this reasoning, the category of "deny" seems overarching and possibly needless.

In this thesis, cyber operations are observed per types and effects they have achieved during the conflict. Those two elements can aid in understanding what types of cyber operations were the most prevalent and their end results. Therefore, the adequate classification of effects should be integrated into the assessment framework. Based on the above argumentation, the effects categories "disrupt", "degrade," and "destroy" were selected as criteria for evaluation.

2.3 Cyber operations in the military domain

Until now, this chapter focused on providing a general understanding of cyber operations. Then it discussed their types and effects. This section continues exploring their utility within a military domain to get insights into what role they can play in and outside of kinetic conflict.

Many scholars explored the role of cyber operations in conflict and war and provided their perspectives. Maathuis, Pieters, and van den Berg (2018) claimed that the definition of cyber operations in that context is so important that lack of it can impair the ability to achieve military objectives.[78] In their attempt to describe them, they say cyber operations are a "type of or a part of a military operation in which cyber weapons/capabilities are used to achieve military objectives in front of adversaries inside and/or outside cyberspace".[79] Authors Herr and Herrick (2016) further explored the warfare utility of cyber operations. They identified that offensive cyber operations could come into play at all levels of war: strategic, operational, and tactical.[80] On a strategic level, their deployment can support the achievement of national aims and objectives of battlefield. On this level, targets can include civilian infrastructure with national security implications or military hardware to create digital and physical destructive effects.[81] On the operational level, cyber operations can be deployed to ensure wins in military campaigns. For instance, air defense systems can be disrupted by cyber-attack, hindering the enemy's ability to detect the enemy's aircraft. This can enable unobstructed strikes on selected physical targets. On a tactical level, cyber operations should be deployed in consideration of moving targets, distances and changing nature of vulnerabilities. However, in some cases adversaries may believe that the tactical level is less vulnerable than the operational or strategic environment, which can provide the attacker with an advantage, as the attack may come unexpectedly. An instance of tactical cyber operation is an exploit of the electromagnetic spectrum, which is used to degrade opponent radio services and impede communication during combat in specific areas. Based on the examples above, it is evident that cyber operations can play an important role in the modern, hybrid conflict.[82]

According to some authors, cyber operations can also achieve different impacts depending on if they are used in cyber conflict or cyberwar. Valeriano and Manes (2015) say that cyber conflict entails the malicious use of technology to impact, change or modify diplomatic and military interactions among states.[83] According to them, cyber conflict could escalate to cyberwar. In Nye's view, cyberwar is hostile action in cyberspace whose effects correspond to or amplify major kinetic violence.[84] The definitions show a difference between the two – cyberwar assumes the potential for a deathly outcome. But, since states practice restraint, such a scenario that includes cyberwar is unlikely to occur, and, per some scholars such as Rid, it is not even feasible.[85]

Rid argued that states use cyber operations to perform espionage, sabotage, and subversion, none of which is directly violent or will likely cause an armed response.[86] Such acts can undermine the link between population and government and cause a loss of faith in the state's ability to protect, which can be more damaging than violent attacks.[87] Comparably, Harknett and Smeets (2020) also claim that the value of cyber operations lies in the possibility of using them instead of catastrophic armed attacks while still influencing the sources of national power.[88] Harknett (2022) also co-authored the "cyber persistence theory", which states that countries persistently conduct campaigns within cyberspace. However, these are calibrated to avoid an armed response, while at the same time, they seek to produce small gains that can accumulate over time.[89] For instance, one state can frequently distribute malware to another nation's private companies and governmental agencies. Such attacks may not elicit an armed response, yet they can negatively influence the targeted country, causing destabilizing events.[90]

2.4 Logics of integration of offensive cyber operations into military structures

Previous sections introduced the subject of cyber operations more broadly, describing what types of cyber operations exist and how they can be utilized in warfare. This section explores how they can be incorporated into state military structures to achieve objectives.

During the literature review, it was established that there are few models developed for assessing how cyber operations are integrated into conflict. A notable attempt has been made by scholars Florian Egloff and James Shires (2022). They have researched how offensive cyber capabilities can be incorporated into (violent) state actions. As a result, they suggested three logics of integration: substitute, support, or complement.[91] While they have focused their research on reviewing state cyber capabilities in the context of violence, their logic and idea on how those are integrated in conflict is still viable for evaluating cyber operations during the kinetic conflict. In their paper, the authors have extensively discussed scenarios that can fall under those categories, probing their plausibility. However, their model has not been tested for

effectiveness.[92] Therefore, it was selected for this thesis assessment framework and tested for applicability.

The below text explains the three logics of integration, as represented by the authors.

Substitution logic *(Instead of)*

The first integration logic, substitution, authors described as "instead of" logic. Per this logic, the decision maker can deploy cyber operations to achieve the same (possibly reversible) outcome as the alternative. The choice of selecting a particular operation depends on the context. The authors offered a simple example of picking the lock to demonstrate tactical utility. The lock can be opened using keys or remote control, but the achieved effect is the same. Likewise, on a strategic level, cyber operations can be used instead of physical activity to sabotage the adversary control and command systems and sow doubt. US President Donald Trump made a famous choice of such substitution logic. In 2019, a US unmanned drone was shot down in the Persian Gulf, probably by Iranian forces. Instead of performing a retaliatory kinetic response, the president used a cyber-attack to target a group tracking shipment for the Iranian Islamic Revolutionary Guard Corps. Another instance of substitution can be using data wiper software to delete opponents' data instead of physically destroying the offices. Substitution should occur between cyber operations and realistic alternatives.

Support logic *(Part of)*

The second proposed way of integration is support or a "part of" logic. Per this logic, offensive cyber operations are "in service to another course of action" and used in tandem with noncyber capabilities. They are always part of conflict involving other means and become integrated into broader warfighting aims. There is almost always a larger plan for using cyber operations, even if that is "a deliberate chaotic intention".[93] On a tactical level, the goal of supportive integration logic is to "increase the probability of success, decrease risks around, or magnify the effects of another course of action".[94] An illustrative case occurred in Syria. In 2007 Israeli forces allegedly used cyber-attacks to disable Syrian air defense systems. That enabled them to enter Syrian airspace without being noticed and to conduct air raids against physical targets.[95] In this case, offensive cyber operations have helped Israel increase its success probability. Besides mentioned, support logic entails that cyber operations can help to increase the power, precision range, or resilience of conventional means. Another example of such integration (also sometimes called the first case of cyber operations in a war), occurred at the beginning of the Russian military invasion of Georgia in 2008.[96] Before and during the Russian kinetic attacks, Georgian governmental sites were targeted with DDoS attacks and defacements. Such cyber operations

were executed to achieve strategic goals, which were, at the time, degradation of Georgian critical services.

Complement logic *(In addition)*

Lastly, complement or "in addition" logic entails using cyber operations to achieve an end unavailable by other means, or more precisely where there are no alternatives for the effects which can be delivered by cyber operations. One example is a malware attack that can propagate swiftly and infect and disable thousands of systems across networks. Such attacks are possible as cyberspace has no borders, and actions taken can occur in real time and propagate swiftly. A well-known case of such cyber operations is the NotPetya malware case from 2017, allegedly executed by Russia. The malware at first infected Ukrainian systems and later spread across the globe due to unsegmented networks of multinational companies operating in Ukraine. On a strategic level, the attack may appear to be a part of, or supporting, Russian military operations in Ukraine. But it is more likely complementary since it did not occur during the military actions. Therefore, per complementary logic cyber operations can be deployed as additional means which state has at hand to use against the opponents.

2.5 Challenges and shortcomings

Previous sections discussed how cyber operations can be deployed, what effects they may produce to achieve specific goals, and how they contribute to conflict outcomes. However, the use and development of cyber operations are not without the challenges which may hinder their effectiveness or even influence the decision to use them in the first place.

In the introduction of this thesis, it was said that some senior military officials expect a devastating cyber-attack to occur. Still, there are many possible causes why we have not yet (publicly) witness such an event. One of the main reasons is the difficulty of producing adequate cyber capabilities to achieve such effects. Many states struggle with various challenges when developing and deploying cyber capabilities. The main barriers lie in the ability to (quickly) train and retain personnel, keep up the ever-changing vulnerability landscape and costs, and ensure that the weapons are up to date, among others.[97] Developing a customized toolset for specific attacks and IT environments is also difficult. Rid (2013) notes that "maximizing the destructive potential of cyber weapons will increase the resources, intelligence, and time to build and to deploy it".[98] He further says that narrowing down the weapon potential will lower the number of targets, collateral damage, and coercive utility of the weapon.

Scholar Lennart Maschmeyer (2021) performed extensive research on the effectiveness of cyber operations. In his opinion, they are not a viable tool to use in an "attempt to shift the balance of power when diplomacy fails short".[99] Maschmeyer identified several roadblocks to their

effective execution on the operational level. Firstly, the attackers need to find an exploitable vulnerability in the system, which they did not design, to exploit it without being detected, access it, and maintain control over it to produce the wanted outcome. The main reasons for failure are negative correlations between speed, the intensity of effects, and control (over systems and effects) in this so-called "security trilemma". In the triangle, one factor is negatively affecting the remaining two. Prioritizing control and speed will impair the intensity. Such a scenario can negatively impact the achievement of strategic goals and even generate additional costs. If speed and intensity are prioritized, then the control is negatively impacted; hence, the attacker cannot remain undetected. Lastly, speed is low if intensity and control are prioritized, so the effects may come belated.

Another challenge in using cyber operations as complex weapons is the potential for collateral damage, as "small wars can spill" in cyberspace, causing civilian harm, unreliability, and the likelihood of backfiring.[100] The latter is an especially relevant factor for risk-averse states.[101] Furthermore, one of the main dangers of using cyber weapons is the risk of misattribution, which can cause the response action to the wrongly attributed party. This is due to the nature of cyberspace, whose primary traits are interconnectivity and anonymity of systems and various (state and non-state) actors. Even when feasible, the attribution may not always suit the political agendas and does not guarantee deterrence against subversive actions.[102] Lastly, the anonymity of cyberspace also reduces coercive power, as the aggressors often choose not to uncover their identity or will.[103]

2.6 Conclusion

Cyber operations can serve as a valuable tool for achieving the state's objectives. States, state actors, and individuals use cyber means to induce power shifts in cyberspace, participating in the new state of affairs: the "unpeace".[104] Cyber operations can be integrated with military operations on the battlefield or serve as instruments for maintaining the conflict below the threshold of armed attack. They can substitute or support military action or complement it to achieve tactical, operational, and strategic goals. When deployed, they can accomplish various effects, such as degradation, destruction, and disruption of the target. The illustrative cases presented in this chapter show the potential for cyber operations to cause significant issues, possibly leading to the loss of life or threatening the state's survival.[105] However, their development, deployment, and maintenance are not without challenges. Lack of adequate infrastructure, the velocity of changes in the vulnerability landscape, financial costs, risk of misattribution, and low coercive and deterrence power may hinder the effectiveness of cyber weapons or prevent their use in the first place.

Chapter 3 - Case Study: 2022 Russian War on Ukraine

As already stated, this thesis consists of two main parts. The first part entails a theoretical exploration of cyber operations' role in kinetic conflict. The second part analyses the cyber operations data in the context of a chosen military conflict. However, before discussing the research method and assessment results, it is valuable to provide an additional context of the selected case study – the 2022 Russian war on Ukraine. The background information is necessary, as cyber operations which occurred within it are not analysed only individually but also as part of the warfare. Therefore, this chapter provides an overview of Russo-Ukrainian relations, including military conflicts and cyber operations which occurred during the war.

3.1 Modern Russo-Ukrainian relationship

Ukraine, a state on the eastern European borders and homeland of 43 million citizens, was under Soviet rule for 70 years.[106] It was in 1991 that Ukraine declared independence from the Soviet Union (USSR), following a referendum in which around 90 percent of citizens voted in favour of leaving the federation.[107] The USSR was led mainly by Russia, which imposed its politics, language, and culture on other member states. In some views, Russia acted as a colonist, which exploited Ukrainian wealth for its own needs.[108] During the years of independence, Ukraine did not manage to achieve economic growth immediately and had continued issues with corruption in political rows. Nevertheless, it established the state structures, democratized the society, and enhanced its reputation in the international community.[109]

Still, even after declared independence, cultural and economic ties with Russia remained strong, causing societal division. Eastern border residents favoured Russia, while the West leaned towards a pro-western outlook and sought to enter alliances such as the European Union (EU) and NATO.[110]

As of 2010, Ukraine was led by Victor Yanukovych, a pro-Russian president who obstructed strengthening the formal EU-Ukraine economic bonds and instead decided to liaise with Russian-related associations.[111] Hence, in late 2013, pro-Western Ukrainians began their three-month-long protests, widely known as "Euromaidan". The bloody uprising resulted in the placement of the new interim government, which sealed the trade agreements with the EU.[112] However, those developments were not aligned with expectations from Moscow.

In 2014, Russian president Vladimir Putin gave a speech to the Russian parliament Duma, emphasizing the unity between the two nations claiming that the Russian and Ukrainian people are whole and thus inseparable.[113] Shortly after, Russia invaded Ukraine and annexed the Crimean Peninsula and later the Donbas region in the southeast.[114] This was the first time after

the Second World War that a state annexed the territory of another European state.[115] The annexations occurred as a response to likely NATO expansion to the eastern borders – especially as Ukraine had the prospect of joining the Alliance.[116] In his speeches, Putin strongly opposed the western influence in Ukraine, claiming that pro-western choices "fooled" millions of people, causing poverty and loss of technological potential.[117] Putin continued to maintain low-intensity conflict in the occupied regions. The conflicts cost Ukraine 10 billion dollars and 14,000 lives from 2014 to 2021.[118]

3.2 The 2022 War in Ukraine

In 2019, Volodymyr Zelensky was elected as Ukrainian president. The pro-western politician claimed to restore the Donbas region and improve relationships with Russia.[119] However, that agenda differed from that of Vladimir Putin, who insisted on keeping Ukraine under Russian influence. In 2021 and 2022, Putin requested from NATO and western governments guarantees that Ukraine would not join the Alliance, as well as the removal of previously instated troops from the country.[120] Those requirements were made to prevent the expansion of the military union to the Russian western borders.

Claiming that the West did not act on the promise, Putin announced a full-scale invasion of Ukraine on February 24th, 2022. In his speech, he noted that Ukraine must be demilitarized and de-Nazified with the "special military operation" and threatened other states should they intervene.[121] Most governments worldwide swiftly condemned the invasion and imposed economic sanctions on Russia.[122] However, this did not deter Moscow.

On the first day of the invasion, Ukraine was attacked from near Kharkiv, from Luhansk in the east, from neighbouring ex-Soviet state Belarus and previously annexed Crimea. Missiles hit the cities of Kyiv and Kharkiv, and fighting was occurring on the eastern flank and in the southern cities of Odessa and Mariupol.[123] Russian forces progressed in Ukraine's territory. Nevertheless, Ukraine provided fierce resistance. In March, Russia took the southern city of Kherson, aiming to cut access to the Black Sea, and seized Zaporizhzhya, the largest nuclear plant in Europe.[124] Still, its planned invasion of the capital, Kyiv, failed due to the logistics challenges which prevented the military convoy from progressing, forcing Russians to retreat in the north.

In the second phase of the war, Russia focused efforts on taking Donetsk and Luhansk, known as Donbas, and in the south, where it attacked the city of Mariupol. The Mariupol bombardment, which also included a maternity hospital, killed thousands of civilians.[125] Hundreds of citizens and soldiers found refuge in Mariupol's Azovstal steel plant, where they resisted the Russian occupation. Finally, after months of fighting, what has become the most known endurance bastion, fell to Russian forces in May 2022.[126] Meanwhile, the battles in Luhansk continued,

resulting in the fall of Lysychansk in July.[127] However, Russian troops failed to progress further in capturing the remaining parts of the Donbas. In August and September 2022, Ukraine launched a counteroffensive in northeast Kharkiv and southern Kherson. Using the weapons supplied by the Western allies, Ukraine managed to reclaim part of the Kharkiv region and the city of Izium, which served as the logistic hub for the Russians. Meanwhile, Vladimir Putin declared Donetsk, Luhansk, Kherson, and Zaporizhzhya Russian territories.[128]

In October, the Crimean bridge, which ties Russian territory with annexed Crimea, was attacked and damaged.[129] That has led to numerous retaliatory attacks on the Ukrainian critical infrastructure, which have left many cities without water and electricity.[130] In the meantime, Ukrainian forces managed to proceed with the liberation of the occupied areas near river Dnipro in the country's south.[131] In November, Russians started to retreat from Kherson in the south as Ukraine retook it.[132] Still, heavy attacks on the vital infrastructure continued, causing casualties and leaving civilians without water and power throughout November and December.[133] Ukraine launched attacks on occupied Melitopol, Donetsk, and Crimea.[134] In January 2023, Russia captured the city Soledar on the east and started to focus the efforts on strategically important Bakhmut.[135]

The above summarizes the key events of the war. However, many more attacks occurred on Ukrainian soil, which have already taken a tremendous human toll. The invasion caused the most extensive European refugee crisis since World War II; around 15 million people fled Ukraine.[136] As of November 2022, there are 16,780 civilian casualties reported.[137] Besides the life loss, the Ukrainian economy was severely damaged. The gross domestic product was forecasted to fall by 45 percent, and the estimated damage to the physical infrastructure is around 127 billion dollars damage (data from December 2022).[138]

So far, this chapter has discussed the Russo-Ukrainian relationship, the history of military actions, and the 2022 War. The remainder of the chapter describes the most notable cyber operations in Ukraine before and during the Russian War on Ukraine.

3.3 Cyber operations in Ukraine before the 2022 War

In the past, Ukraine was targeted with thousands of cyber operations, mostly attributed to pro-Russian actors.[139] According to a report issued by European Parliamentary Research Service (EPRS), attacks intensified and became more frequent after the Russian annexation of Crimea in 2014.[140] For instance, in 2014, pro-Russian actors launched cyber-attacks to meddle in the Ukrainian presidential election by attempting to manipulate data in Central Election Commission systems. In this case, the malware was removed shortly before the election started.

Then, a few days before the referendum on the status of Crimea, DDoS attacks were launched to divert public attention from the presence of Russian troops in the Peninsula.

Later, in 2015 and 2016, Ukraine's electrical grid was targeted with highly sophisticated cyber-attacks.[141] The 2015 incident left 230,000 customers without electricity for hours in wintertime. The attack from 2016 aimed to achieve the same effects. However, it was timely detected and contained. In 2017, the NotPetya cyber-attack, also considered one of the most impactful to date, started in Ukraine and spilled worldwide.[142] The NotPetya data encryption malware propagated through interconnected networks, destroying data and causing damage in billions of dollars to Ukrainian and multinational companies. Then, in 2021, the systems of Ukrainian governmental agencies used to exchange data were compromised to spread malware to public organizations.[143]

3.4 Cyber operations in Ukraine in 2022 and during the war

In 2022, Ukraine has been subjected to impactful cyber-attacks since January. Early in the year, 70 Ukrainian governmental websites were defaced, showing warning messages to visitors claiming that their data had been stolen and destroyed.[144] During the same period, many private, non-profit, and IT companies were targeted with malicious data-wiping software.[145] In February, the attacks intensified. Per the EPRS report, governmental and finance sector organizations suffered DDoS attacks for several hours in mid-February.[146] On the February 23rd, the day before the invasion started, public sector websites were defaced again.[147] HermeticWiper, malware that destroys data, was deployed against IT, aviation, and finance organizations.[148] On the date when Russia attacked Ukraine, adversaries targeted KA-SAT, a satellite ISP. As a result, many citizens and organizations have been left without access to the Internet.[149] The attacks continued in March, during which data wipers were executed against various entities, such as non-governmental and charity organizations, private companies, border control station, and governmental bodies.[150] Due to the attacks, medicine and food delivery were delayed. Next, the malicious actors targeted telecom Ukrtelecom, preventing the users from accessing the Internet service.[151] During March, April, and May, Ukrainian citizens and governmental organizations suffered multiple phishing attacks and data breaches following the exfiltration of sensitive information from government and media services.[152]

In April, adversaries attempted a cyber-attack on the Ukrainian electricity grid, which was timely stopped. In the aftermath, Ukrainian officials said that adversaries had breached the electricity plant network before February to set up the environment for the attack in April.[153] In May, Odessa City Council was targeted by a cyber-attack, while missiles struck the city's residential area and local airfield in the same period.[154] Then, from June until August, DDoS was

the most prevalent type of cyber operation against Ukrainian digital services.[155] According to reports from CyberPeace Institute, Russian state-sponsored actors led several campaigns in that period. For instance, they have delivered information-stealing malware and fake applications in support of Ukraine, which executed DDoS attacks against the Ukrainian systems.

At the end of 2022, DDoS remained the prevalent cyber operation type. However, the attacks on public organizations decreased.[156] The attacks focused on transport and trade companies. Russian state-sponsored actors remained active, spreading espionage tools and malware to various public and private entities. At the beginning of 2023, the Russian nation-state groups continued to spread new types of data wipers and data theft and surveillance software.[157]

Chapter 4 - Research Method

This thesis research question: "What role do cyber operations play in kinetic conflict?" has already been conceptualized in Chapter 2. This chapter defines the methods for answering the research question using the data from the case study (presented in Chapter 3). This chapter first explains the data analysis framework, then describes data collection. Lastly, it discusses limitations, such as bias and completeness of the information.

4.1 Data analysis framework

At the time of writing this thesis, it was found that there were no readily available comprehensive frameworks for the coherent assessment of cyber operations data in the context of a kinetic conflict. Therefore, this thesis proposes a framework to support such analysis. This thesis has tested the framework for effectiveness using case study data, and the reflection on its usability is discussed in Chapter 5 – Data Analysis.

The framework was constructed based on theories discussed in Chapter 2 – Literature review. This section provides only the key and simplified information on the concepts, such as descriptions and basic examples. A detailed explanation of the models, a discussion of their adequacy, and proposed modifications are documented in Chapter 2.[158]

The framework was built by combining three different classifications related to cyber operations as identified in the literature review: types of cyber operations *(Table 1),* their effects *(Table 2),* and the ways how they can be integrated into kinetic conflict *(Table 3)*. Besides the noted, additional attributes were added, as further described in this section.

The final framework is presented in *Table 4*.

4.1.1 Cyber operation types and effects

The knowledge of the types and effects of cyber operations is pertinent to understanding their role in the kinetic conflict. Therefore, they have been included in the assessment framework. The selected model for assessing cyber operation types consists of three main categories: DoS, data manipulation, and system manipulation (*Table 1*).

Cyber Operations Type	Description	Example of cyber operation type
DoS	Exhausting the digital services to achieve an effect.	Flooding of websites with network traffic to make them unavailable.
Data Manipulation	Data is modified (by encryption, deletion, or modification) to achieve an effect.	Encryption of data with malicious software to permanently destroy data.
System Manipulation	The (industrial) system is manipulated to achieve an effect.	Manipulating systems to destroy physical components in an industrial environment.

Table 1 - Cyber Operation Types

Once deployed, cyber operations could cause the following effects: degradation, destruction, and disruption (*Table 2*).

Cyber Operations Effects	Description (by leveraging Cambridge Dictionary)[159]	Example of effects in correlation with cyber-attack
Degrade	To spoil or destroy the quality of something.	Telecom infrastructure was attacked to cause decreased internet bandwidth, preventing users from using the agreed-upon internet speed.
Destroy	To damage something so severely that it cannot be used.	Data was encrypted with randomly generated encryption keys so that it could not be decrypted, causing permanent damage.
Disrupt	To prevent something from continuing as usual or as expected.	Attacking electrical grid systems with malware that opened circuit breakers, causing electrical outages, and denying electricity to, e.g., citizens.

Table 2 - Cyber Operations Effects

4.1.2 Integration of cyber operations into the military structures

Besides understanding cyber operation types and consequences, it is necessary to know how they were integrated into conflict. The assessment is based on the model of three logic of integration. According to it, cyber-attacks can substitute, support, or complement military action (*Table 3)*.

Logic of Integration	Description	Example of the logic of integration
Substitution (Instead of)	The cyber operation is deployed to achieve the same outcome as the military alternative.	Use of wiper malware to destroy the data instead of physically destroying the offices.
Support (Part of)	The cyber operation is in service to another course of action. It is used to increase the probability of success, decrease risks around, or magnify the effects of another course of action.	Use of DDoS attacks against critical digital services to magnify the effects of military invasion.
Complement (In addition)	The cyber-attack is deployed to achieve a goal that is impossible to produce with other means.	Deployment of encryptors to destroy critical data on a large scale.

Table 3 - Cyber Operations Integration

4.1.3 Proposed assessment framework

In addition to what was discussed in the previous section, new elements were added to enhance the framework further. The additions include "Cyber operation (ID)", "Date" of occurrence of the attack, and a "Short Description". Those are the attributes needed to provide basic information on the sample.

Next to those, other new attributes are "Military Action" and "Targeted Sector". The "Military Action" attribute was included to provide information on a kinetic event occurring in time proximity to a cyber operation. This attribute serves to help in the evaluation of which "Logic of Integration" was the attack incorporated in the conflict.

The "Targeted sector" was added to identify what services were affected by cyber-attacks. For instance, it is relevant to differentiate the cyber-attacks targeting the educational sector and the critical infrastructure such as electricity plant systems. It is unlikely that the cyber-attack on the university website will have the same influence on the kinetic conflict as the disruption of the electrical grid. Therefore, the US CISA derived a list of 16 critical sectors whose incapacitation

could significantly affect national security, public health, safety, or a combination of those.[160] These are: Chemical Sector, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, IT, Nuclear Reactors, Materials, and Waste, Transportation Systems, Water and Wastewater Systems. The CISA classification is used to assess cyber operations with the proposed framework.

Lastly, the "Attribution" element was included, as the cyber-attacks may not necessarily be conducted by only state actors but by many other participants in cyberspace (e.g., hacktivists and citizens). While attribution has challenges, as discussed in the next section, the added value is demonstrating the distinction in actors between military and cyber conflict. The parties in cyber conflict can be engaged expeditiously, regardless of their geolocation or skill level, from the protection of anonymity. It is therefore useful for the analysis to understand what parties were involved in the conflict from this perspective. Possible values for attribution can be nation-state (e.g., Russia) and nation-state supporters, cyber criminals, hacktivists, terrorist groups, thrill-seekers, and insider threats.[161]

Those added elements allow for modularity and provide sufficient angles for interpreting samples. As such, they contribute to understanding the role cyber operation plays in kinetic events. Besides the mentioned, those added attributes can also facilitate meaningful trend analysis. For instance, to ascertain what sectors mainly were targeted and at what intervals.

The finalized framework with all its criteria is presented in *Table 4.* The table includes an illustrative sample from the observed population.

Cyber Op. ID	Date	Short Description	Cyber Operation Type	Cyber Operation Effect	Logic of Integration	Military Action	Targeted Sector	Attribution
1	24/02/2022	DDoS attack against a Kyiv-based media	DoS	Disrupt	Substitute	Start of invasion and missiles attacks on Kyiv	Commercial Facilities	Russia

Table 4 – Data Analysis Framework with sample

Applicability of the proposed framework

The proposed framework's applicability was evaluated using a sample from the case study population, and coder reliability was ensured by a separate viewer. The analysis results are summarized in *Table 4* (above), and the evaluation of this single case is documented below. As per this test, it appears that the proposed framework can be utilized for such an assessment. However, the shortcomings could be identified while evaluating the total population. If noted, they are discussed, and the improvement points are suggested (Chapter 5).

Cyber Operation 1

DDoS against a Kyiv-based media

On February 24th, 2022, the day the Russian invasion of Ukraine started, the Kyiv Post, a media company located in the capital, got targeted by a DDoS cyber-attack.[162] Based on the details provided by its editor, Bohdan Nahaylo, presumably, Russian actors were behind the attack. The Kyiv Post issued a statement on Twitter claiming that the DDoS started from "the moment Russia launched its military offensive".[163] As a result, the news release, which is critical in wartime, was disrupted. The journalists had to use alternative channels and adjust the format to provide information to the public. At the same time, the Russian military launched missiles into several Ukrainian cities, including Kyiv.[164] It could be assumed that this cyber operation was integrated into conflict by using substitute logic, therefore using cyber means to cause the same effects which could have been achieved with military action (e.g., by damaging the media building and its IT infrastructure).

Analysis results and discussion

The cyber operations in the scope of this thesis were evaluated on a case-by-case basis by leveraging the proposed framework. Detailed evaluation is documented in *Appendix*, and the analysis results are summarized in Chapter 5. Reflection on the framework is documented in the same place. Their role in conflict is discussed in conclusion of this thesis (Chapter 6).

4.2 Data gathering

The previous section discussed the framework for data analysis. This section explains how and what data was collected and highlights the limitations that possibly influenced the analysis's accuracy.

4.2.1 Timeframe

This thesis focuses on the early period of the 2022 War on Ukraine, due to the limitations of researching the ongoing conflict in which data and events are volatile. This timeline was selected

as, in the first weeks of the Russian invasion, both military action and cyber operations were at their peaks, providing a suitable dataset for further exploration.[165] Additionally, as they occurred in the early phase of the conflict, they could influence the war's course. Thus, the data collection on offensive cyber operations included the beginning of the war, February 24th, 2022, and ended on March 24th, 2022. The collection stopped on January 10th, 2023, and new information related to those events could not be evaluated after that date.

Since the kinetic conflict occurred within the Ukrainian territorial borders, the only cyber operations selected for assessment were the ones that produced effects in Ukraine. For example, the cyber-attack on the ViaSat satellite company affected Ukraine and other European countries, such as Germany.[166] Still, for this thesis, only the effects in Ukraine were observed. In this case, the attack caused the outage of the satellite services in Ukraine, and as it falls within the scope of assessment, it is reviewed. Cyber operations collected for the evaluation included data wipers, data encryptors, and DDoS attacks, identified as the main activities at the beginning of the war in Ukraine.

Additionally, the data on the kinetic conflict which occurred on a specific day or period to support the conclusion on integration between cyber operations and military action was searched in major mainstream media such as CNN, BBC, Al Jazeera, The Guardian, Forbes, and Institute for the Study of War (ISW) website for tracking the war progress.

4.2.1 Sources

The data was obtained from various sources to ensure that the final data set represents an exhaustive and as complete as possible inventory of cyber operations. The search was performed by browsing the public cyber-attack databases maintained by different parties: Council of Foreign Relations (CFR), CyberPeace Institute, and Ukrainian Computer Emergency Response Team (CERT-UA), the Netherlands National Cyber Security Centre (NCSC).

The CFR database was used as a source as it independently and extensively tracks the offensive cyber campaigns across the globe, including those occurring in Ukraine.[167] It provides an overview of the most notable cyber-attacks in specific periods. Similarly, the CyberPeace Institute also maintains a public database on cyber operations. This non-governmental organization analyses cyber-attacks to show their impact on society and how they violate laws and norms, aiming to advance responsible behaviour in cyberspace.[168] The Institute maintains a separate timeline of the cyber-attacks in the 2022 war on Ukraine.

Furthermore, the data was collected from the website of Ukrainian CERT.[169] This governmental body publicly communicates information on cyber-attacks that occurred in Ukraine, including technical details, effects, and attribution. The content of the CERT is used by policymakers and

scholars as it is an authoritative source of such information for a specific country. The CERT-UA website was browsed to collect the articles which describe the events that have occurred in the selected timeframe of the current war.

Besides those three databases, the websites of cyber security and technology companies were searched for data on cyber-attacks in Ukraine to add to, supplement, or reconfirm collected information. While many companies might have participated in identifying and documenting attacks in Ukraine, the selection included the following: Microsoft, Cisco Talos, Fortinet, ESET, Sophos, Mandiant, Symantec, SentinelOne, and Trellix. Besides the technological companies, other sources, such as media, threat intelligence companies, European institutions, and national security organizations, were browsed for data on cyber operations in Ukraine. Those are Cybersecurity and Infrastructure Security Agency (CISA), the UK NCSC, European Parliament, Dark Reading, Recorded Future, and Bleeping Computer. When the main source did not provide sufficient information on the sample cyber-attack, the search engine Google was used for snowballing – inquiring for supplementary data.

All the above sources were searched by either using the keywords "Ukraine", "Ukraine 2022", "Ukraine cyber operations", and "Ukraine cyber-attacks", or their content was browsed to navigate (from x to y) to the data related to cyber operations which occurred during 2022 War on Ukraine.

The cyber-attacks selected as the population were the ones for which there was sufficient data for drawing further conclusions based on the assessment criteria. The minimum required data to perform the analysis were the date, type of cyber-attack and caused effects, and the information that attack occurred (it was not prevented).

Considering the above-described search criteria, the final population for analysis consists of 14 cyber operations. However, it is necessary to emphasize that the number does not reflect a complete universe of cases. For example, The State Service of special communication and information protection of Ukraine noted that Ukrainian CERT faced at least 1,500 cyber-attacks since the invasion started.[170] Yet, the CERT-UA published reports for a subset of cyber-attacks, which were evaluated and included in the total number of offensive cyber operations. The assumption was made that only the most impactful and notable offensive cyber-attacks were presented to the public.

4.3 Limitations

Before continuing with data analysis, it is necessary to discuss its potential limitations. Besides the already mentioned completeness issue, several other constraints may have

influenced the outcome of data gathering and consequently impaired the analysis accuracy. Those include language barriers, biased reporting, and attribution problems.

Firstly, the sources were searched almost exclusively by using the English language. Only exceptionally, the translation services embedded into search engines and web browsers were used to identify and translate, e.g., CERT-UA reports initially published in the Ukrainian language. Therefore, the sources and data may have been limited, which could have impaired the accuracy and comprehensiveness of the information.

Secondly, data collection also involved commercial reports as sources, and such reports can be biased. In their paper "Tale of two cyber", authors Maschmeyer, Deibert, and Lindsay (2020) say that public and academic knowledge relies heavily on the data from commercial threat reporting. Yet such data can provide a "distorted view of cyber threat activity", consequently affecting the academic debate and public policy.[171] According to them, most of the reported threats and attacks in such reporting come from high-profile threat actors towards high-profile targets. Conversely, such reporting rarely includes threats to civil society and low-end cyber conflict, which can potentially impair democracy. Similarly, Smeets (2022) states that threat intelligence firms do not "not discover every operation, and for those they do discover, they often do not write up a public report", especially if it is a low-level activity.[172]

Lastly, actors in cyberspace mostly do not claim responsibility for cyber operations, enjoying the protection of anonymity. This causes an attribution problem; hence, some cyber operations evaluated in this thesis might have been wrongly attributed to inaccurate actors. However, advanced persistent threats (APTs) nowadays exhibit "relatively consistent preferences in motivation, types of targets, techniques, tactics, and procedures that increase confidence in conclusions regarding the source of behaviours".[173] Thus, while there is no absolute certainty in attribution, a combination of technical data, political context, and established behavioural patterns can draw "reasonable conclusions" about the actors behind the attacks.[174]

Many of the cyber operations gathered for this analysis were attributed to Russia, the state that initiated the invasion. In support of the attribution, it is relevant to note that Russia have minimal constraints related to executions of cyber operations and a high degree of financial and organizational resources, which made it "a dangerous state" in cyberspace.[175] Russia is equipped to perform aggressive cyber operations, expanding its warfare capabilities to cyber weapons. Due to its capacities, it is suspected that Russia and its associates performed some of the most notable cyber-attacks to date. Examples include previously discussed Ukrainian electricity grid takedown, and the NotPetya incident. Therefore, it is plausible that the attribution of the attacks in this thesis have been accurately assigned.

Chapter 5 –Data Analysis

This chapter summarizes the analysis of cyber operations which occurred in the first month of the 2022 War in Ukraine. First, this chapter discusses the types of offensive cyber operations and their effects. Then, it elaborates on how those were integrated into the kinetic conflict. Additionally, it points out the most targeted sectors and which actors have possibly conducted the cyber-attacks. The analysis results are summarized in this section and discussed in Chapter 6 – Conclusion. Furthermore, this section also includes a reflection on the usability of the proposed framework.

As noted, this chapter provides a summary of the evaluation. The detailed analysis of all 14 collected cyber operations is provided in the *Appendix*. In the *Appendix,* cyber operations are elaborated on and evaluated on a case-by-case basis using the framework proposed in Chapter 4.

The assessment summary with relevant references is also provided in *Appendix* (*Table 5)*.

5.1 Offensive cyber operation types and effects in early War in Ukraine

The analysis of the 14 cyber operations has shown that the Ukrainian digital services were primarily targeted with data manipulation (11), and DoS (3) types of attacks *(Figure 1).* No successfully performed system manipulation cyber-attack was identified in the population. The adversaries used those to cause disruptive (9) and destructive (5) effects on various sectors' assets, such as communications, governmental facilities, financial companies, and media.

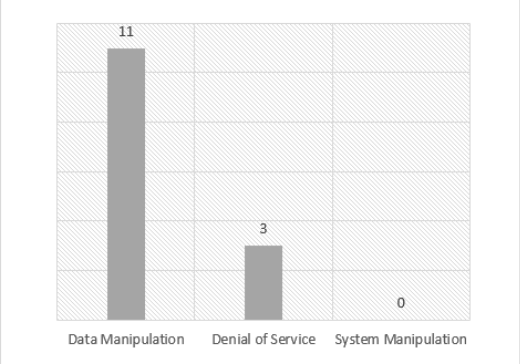

Figure 1 - Cyber Operation Types

5.1.1 Cyber operation types

Data Manipulation attacks

The data manipulation attacks were mostly executed with data wipers. The wiper is specific malware created to make data and systems unavailable by using destructive actions. The program usually overwrites the disks and system files of the targeted device, which makes the targeted device unusable.

During the first week of the war, at least four versions of data wipers were executed across various networks in Ukraine. For instance, adversaries ran IsaacWiper malware (created months before the invasion) against governmental systems on the first day of the invasion. In

that initial week, another malware was deployed against the border control station towards Romania. The attack caused delays in processing refugee data in the period when many fled to safety. In Kyiv, the media company suffered data loss due to an attack with DesertBlade wiper, which delayed news publishing in the critical wartime period. Other wipers, such as Junkmail and DoubleZero, were distributed to various organizations and private companies to cause data destruction. All the data wipers caused effects of either destruction of the data or disruption of the services.

The most notable incident caused by data wipers is the ViaSat hack. The adversaries attacked this satellite-based ISP, by misusing the vulnerability of externally facing virtual network appliance to gain access to the provider's internal network. Once they obtained it, they navigated to the segment dedicated to managing the devices located at customer premises. From there, they executed the AcidRain malware against the customer modems. The program wiped their memory and made devices unusable. The incident caused disruptive effects to customers in Ukraine, but the effects also spilled to other European countries such as Germany and France. In the aftermath of the incident, ViaSat had to replace 27,000 permanently damaged devices. Due to this event, thousands of Ukrainian citizens and companies were left without Internet access for at least a week. The attack came at a time when the war started to rage – when means of communication are pertinent to ensure the safety of civilians, and when internet connectivity is crucial in ensuring continuity of critical businesses.

ViaSat was not the only ISP harmed by a data manipulation attack. Triolan, another ISP, experienced two disruptions in the early phase of the war. According to sources, in both cases, adversaries reset the ISP's network device configurations, which resulted in an outage of Internet services in cities such as Kyiv and Kharkiv when they were under Russian military attacks.

Besides the mentioned, data manipulation attacks were executed against the media and educational websites. The sites were defaced, and their legitimate content was replaced with Russian propaganda or messages supporting invaders. Such events disrupted the provision of legitimate content, such as news information, on which the citizens greatly rely during wartime.

DoS attacks

While data manipulation attacks were the most prevalent cyber operation types in the first month of the war, the analysis also identified three DoS attacks, mainly occurring at the beginning of the invasion (from February 24th to March 4th). On the first day of the war, Kyiv-based media experienced DDoS attacks. The incident disrupted the delivery of essential news to Ukrainian citizens who had just experienced the start of Russian military strikes across the

country. The Kyiv Post journalists had to find alternative channels to deliver the information to the public. A few days later, the botnet "Zhadnost" was deployed to execute a DDoS attack against several Ukrainian governmental and financial services. The botnet used the Domain Name System (DNS) amplification technique to perform the attack. Bots, infected systems controlled by adversaries, have sent the request to legitimate DNS servers for internet name resolution. The requests were created to require a large amount of data in reply, which is sent to the targeted systems due to spoofed IP addresses. That caused the exhaustion of the resources and consequently made systems unavailable. Lastly, a DDoS attack was performed against the mail server of the Ukrainian Ministry of Defense. There is no available technical data for this specific attack to understand how it was executed and how severely it impacted the service.

System Manipulation attacks

During the assessment, the third category of cyber operations type, system manipulation, was not identified. In the first month of the war, there were no publicly disclosed successful attacks on specific systems, such as the ones controlling electricity grid operations.

5.1.2 Cyber operations effects

The most common effect of cyber operations in the war's early phase was disruption (9), followed by destruction (5). There were no instances of degradation identified in the population.

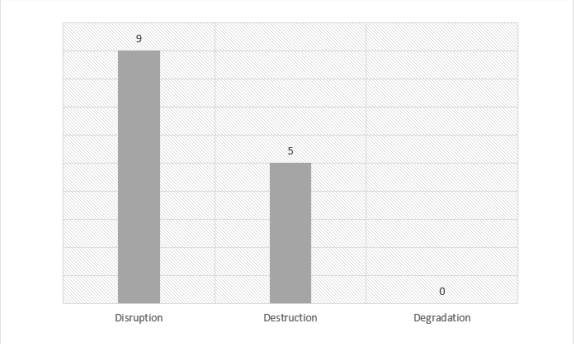

Figure 2 - Cyber Operations Effects

In some cases, disruption of services was caused by denial-of-service attacks and sometimes by data manipulation. DoS attacks are regularly used to obstruct the continuity of services, and in observed cases, they have successfully disrupted media, governmental and financial services. However, some data manipulation attacks also yielded disruptive effects. For instance, reset of network devices or wipe of their configurations has led to Internet connectivity outages. Similarly, due to manipulated, defaced media and education websites, legitimate content was unavailable to its end users as expected.

Destructive effects were caused mainly by deploying data wipers, the most common malware type identified in the first month of the war. The harmful software was executed against private companies, governmental networks, border control station, and media, permanently deleting their data and making their systems unusable. Still, the destructive and disruptive effects

remained limited to the cyberspace. They did not cause damage in physical domain, and therefore did not contribute directly to the kinetic conflict.

5.2 Integration in conflict

The previous section discussed the types and effects of cyber operations in the first month of the war in Ukraine. This section explains how they were integrated into the conflict. It is important to emphasize that certain assumptions were made during the analysis, as the relevant data was either limited or unavailable. That was especially the case where some cyber operations could be assigned to a few integration categories due to their properties, but one was chosen which appeared the most likely. The argumentation on selection is provided in *Appendix* where necessary for each case.

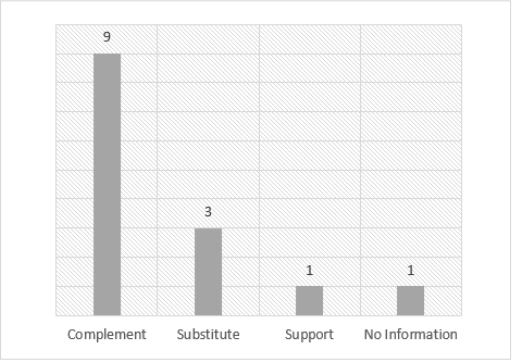

Figure 3 – Integration of cyber operations in the early Russian war on Ukraine

Upon conclusion of the analysis, it was identified that the majority of observed cyber operations were executed in addition to military actions (9 out of 14 cases) *(Figure 2).* In 3 cases, cyber-attack appeared to be used instead of military activity, and only one case appeared supportive of it. For one event, there was a lack of information to conclude.

Complement logic *(In addition)*

As noted, cyber-attacks mainly appeared integrated into the war per complementary logic. According to the categorization of Egloff and Shires (2022), complementary means are deployed to achieve results that cannot be produced with traditional military actions. Particularly, those are closely related to characteristics typical only for cyber-attacks, such as scale and velocity. For instance, the destruction of data on multiple devices in various organizations and locations in a short period may not be achieved with military action. Similarly, this principle applies to other types of attacks as well. For instance, remote, centralized reset of the geographically dispersed systems and DoS against physically distant targets. Another example is a web defacement attack. It is impossible to use military action to change the website's content to spread, e.g., propaganda.

Per the assessment of the population of cases, it was noted that Ukraine was faced with data wiper attacks (4), remote manipulation of data (2), web defacements (2), and DoS attacks (1), which were integrated into the conflict in per complement logic, so in addition to existing capabilities.

At the beginning of the invasion, Russian forces attacked Ukraine from three fronts, north, east, and south. The missiles hit multiple cities: Kyiv, Kharkiv, Odesa, Mariupol, residential buildings, and military bases.[176] At the same time, Ukrainian IT services were attacked from cyberspace.

Adversaries executed data wipers against governmental organizations and ISP ViaSat. Moreover, the malicious actors also changed the configurations of the network devices of telecom Triolan. Hence, on the first day of the invasion, the internet connectivity of thousands of users was disrupted for at least hours, and the governmental systems were exposed to data loss. Then, during the first week of the war, the websites of 30 Ukrainian universities were defaced, displaying messages from pro-Russian supporters. Furthermore, financial, and governmental services suffered a DDoS attack executed by using the botnet "Zhadnost", which caused disruptions in their operations.

In the remaining three weeks, Triolan ISP was again attacked in the same way as in the first week, which caused an Internet connectivity outage in several cities, including Kyiv and Kharkiv. Other than that, private companies and organizations suffered data destruction due to the deployment of Double Zero and CaddyWiper malware. Lastly, the leading media websites in Ukraine were defaced, and the legitimate news content was replaced with Russian symbols.

Substitution logic *(Instead of)*

Only three cyber operations appeared as possible substitutions for military actions. In the first case, which occurred on the start date of the invasion, the Kyiv media company suffered a DDoS attack. It may seem that this attack was used in addition to available military means. However, as the target was single media, and Russian forces fired missiles on Kyiv, it may also be assumed that it was used instead of military action. If Russian troops attacked the media office with strikes, it would probably achieve the same or similar effect: disruption in news delivery during this critical period. In the second case, the border control systems for entering Romania were attacked with a data wiper. The attack slowed down the processing of the refugee crossing. The same effects could have been achieved with military action. Lastly, a media company in Kyiv was attacked with DesertBlade data wiper on the same day Russian forces struck missiles against the Kyiv television tower. Therefore, it could be presumed that the invading army had the capabilities to attack the media company as well, which suffered a malware attack.

Support logic *(Part of)*

A single cyber operation appeared supportive of military action. On the 4th of March 2022, it was reported that the Ukrainian Ministry of Defense webmail was under DDoS attacks. On and around that date, Russian forces attacked Zaporizhzhya nuclear plant and besieged Mariupol and Kharkiv. It was therefore assumed that disrupting the communication means of the

Ukrainian army could have helped Russian forces to increase the probability of success of their military actions.

This analysis did not cover one event, in which an unspecified organization was targeted with a data wiper just a few hours before president Zelensky was to request the US Congress to introduce a no-fly zone over Ukraine. There was no sufficient data available to presume the possible integration in conflict. If the organization had direct relevance to the Ukrainian military (e.g., arms producers, military data centers), such operations could be classified as supportive of achieving the Russian objectives.

In sum, cyber operations were integrated into this war in several possible ways on a tactical and operational level. However, from a strategic perspective, they seemed organized in a cyber campaign combined with broader warfighting. The attackers' objective was to at least impair digital services and deprive the public of information and means of communication essential for ensuring the safety of civilians and the continuity of businesses. In some cases, the attacks were performed to spread Russian propaganda.

5.3 Targeted Sectors

Based on the population of 14 cases, it was noted that the governmental sector was the most targeted *(Figure 3).* Specifically, various state-managed services were attacked: border control station, universities, the webmail of the Ministry of Defense, and some unspecified governmental organizations. Next, ISPs and media were disrupted in several ways to prevent access to communication and timely news delivery. Financial services suffered only one attack. For several cases, there was no information available on the sector type.

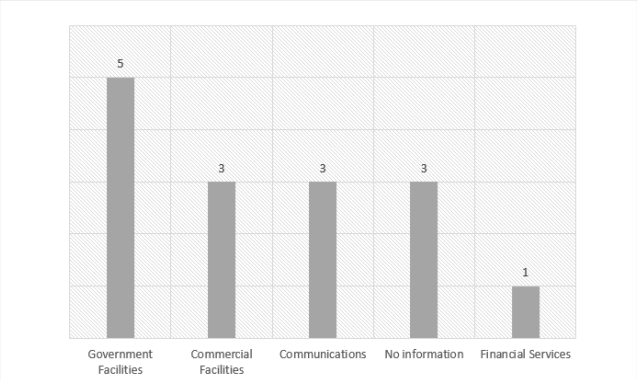

Figure 4 – Targeted Sectors

The above conclusions were drawn based on the publicly available data, which may have limitations, such as accuracy and completeness. Still, per existing information, it appears that the adversaries either did not attack or did not manage to successfully disrupt or destroy services relevant to Ukrainian defense.

5.4 Attribution

Most cyber operations were attributed to nation-state Russia by private (cyber security) companies, targeted organizations, states such as Ukraine and the US, or by international alliances such as the EU *(Figure 4)*. For several cyber operations, the attribution was not assigned. In one case, which included web defacement of university websites, the attribution was assigned to theMxOnday, a Brazilian-based threat actor publicly supporting Russia. Therefore, it is plausible to conclude most of the cyber operations were performed by Russian state actors or affiliates supporting the invasion.

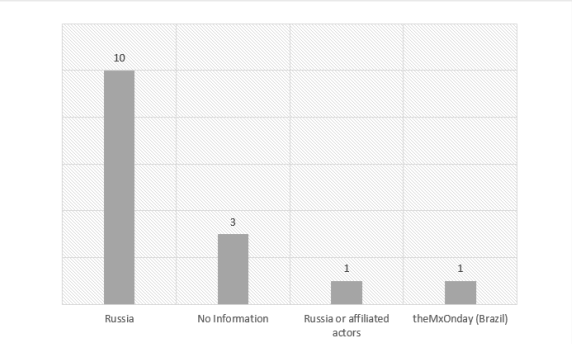

Figure 5 - Attribution

5.5 Summary

So far, this chapter has provided key points from the analysis of 14 cyber operations which occurred in the first month of the War in Ukraine. The cyber-attacks were evaluated by leveraging the framework proposed in Chapter 4. The assessment was segmented per key elements: types, effects, integration in conflict, targeted sectors, and attribution.

The combined results of the assessments showed no notable occasions in which cyber operations directly supported the Russian offensive military actions. The executed cyber operations were primarily conducted in addition to military actions or possibly as a substitute. Furthermore, Russia or Russian affiliates have successfully targeted sectors relevant to society. For instance, they made media websites unavailable and caused outages of Internet connection in critical times. But they did not successfully impair military IT infrastructure. It was also found that most cyber operations caused destructive and disruptive effects, which remained limited to cyberspace.

5.6 Reflection on the proposed framework and limitations of the analysis

The main insights from the data analysis have been provided in the previous section. This section reflects on the assessment framework's usability and highlights this analysis's main limitations.

The framework for assessment of cyber operations, which this thesis proposed, has been demonstrated as operable. During the evaluation of the cases, its structure and pre-defined values have helped to categorize cyber operations in a coherent manner. The selected elements

and their attributes have been sufficient to observe the case from different angles (e.g., types of cyber operations, integration in conflict, etc.)

However, the framework can be fully effective only if used for assessment against complete and accurate data. Otherwise, it serves as a tool that can help to estimate the approximate values. In this thesis, certain assumptions were drawn due to the absence of data or its incompleteness. Those were based on the overall understanding of the case and its circumstances. The most favourable data to use within the framework is the one most explicit and as unambiguous as possible. For instance, to say that cyber-attack was a substitute for military action should be best supported with a quote from the military official that decided. Due to the nature of cyber operations, such a complete dataset may never be available for the researcher that conducts the analysis.

It is also relevant to note that the analysis was performed against a subset of known cyber-attacks, for which the publicly available data is reduced. As discussed in Chapter 4, Ukrainian digital services have been targeted with at least 1,500 cyber-attacks since the invasion started. But only some have been disclosed with the minimum data (effects and type of cyber operation), and those have been selected in the observed population. Potentially, the conclusion could have been different if all possible events with a complete dataset had been analysed with this framework.

Regardless, the proposed assessment framework represents a valuable tool that can be further modified and used for analysing cyber operations in kinetic conflict. Where necessary, it should be adjusted to accommodate the changing nature of warfare and offensive cyber operations.

Chapter 6 – Conclusion

6.1 Conclusion

This thesis aimed to answer the research question "What role do cyber operations play in kinetic conflict?". The answer was first conceptualized based on insights from the existing body of literature. It was discovered that scholars and public officials consider cyber operations an important tool in conflict. Their opinions depart when it comes to recognizing their capabilities. Officials, such as Leon Panetta, former director of the Central Intelligence Agency, expect cyber-Pearl Harbour to occur and warn of dangers looming from the digital realm.[177] Similarly, Mike McConnel, former director of the US National Security Agency, said that cyberwar could occur damage our way of life as drastically as a nuclear attack.[178]

On the contrary, scholars are more moderate in their views. In the opinion of Thomas Rid (2013), cyber operations are a great tool for performing sabotage and espionage, yet they cannot directly change the nature of war.[179] According to Eric Gratzke (2013), they are not as impactful as standalone means, but they can assist terrestrial forces in achieving their goals.[180] However, many challenges must be overcome to ensure the effectiveness of offensive cyber operations. For instance, Max Smeets (2022) identified some of the main impediments, such as a lack of skills and resources to develop and maintain such offensive capabilities and swift changes in the vulnerability landscape.[181] Nevertheless, there are some rare well-known cases in which offensive cyber operations played a role. Florian Egloff and James Shires (2021) provided the example of the Russo-Georgian war, in which public digital services were disrupted for prolonged periods, and Rid (2013) noted the obstruction of Syrian air defense systems before the Israeli forces conducted air raids.[182]

The theories discussed in the literature review served as the starting point in building the framework for evaluating the role of cyber operations in kinetic conflict. Therefore, this thesis proposed an assessment model consisting of multiple descriptors that can be leveraged to assess cyber operations in conflict. The classifications included are: types and effects of cyber operations, ways of integration in conflict, targeted sectors, attribution, and kinetic action. The goal was to provide means for coherent processing of cyber operations data, which can simultaneously offer a variety of angles to observe their role in the conflict. This framework was tested against the data of the selected case study, the 2022 Russian war in Ukraine. The analysis results provided a possible answer to the research question from the context of this ongoing conflict.

The Russian War in Ukraine started on 24th February 2022 with a full-scale invasion.[183] During the initial phase, Russia aimed to swiftly capture the capital Kyiv and overthrow the pro-western

government.[184] Invaders bombed Ukrainian cities, and destroyed residential buildings and hospitals, but Ukrainians showed robust resistance. After a month into War, Russian forces started to retreat from the northern battlefield due to logistics issues and the counter-offensive. They began to focus on the eastern provinces of Luhansk and Donetsk.[185]

The beginning of the invasion was also marked by intensive activities in cyberspace. Russia, its affiliates, and backers attacked Ukrainian digital services at least 14 times in the first month of the war. The extensive analysis of those 14 cyber operations (performed in the *Appendix* and summarized in Chapter 5) showed that they were most likely used to support broader warfighting.

The destabilization of Ukrainian IT-dependent services could have helped Russia achieve strategic goals. However, it appears that such an objective has not been fully attained. Namely, no evidence shows that cyber-attacks have significantly influenced the outcome of battles in the war's early phase. Several possible explanations for why that was the case were derived from the performed evaluation.

Firstly, the adversaries have attacked organizations in sectors that do not have direct military relevance. For instance, attacked entities were mainly media, government, and ISPs. The Russian forces could have benefitted from (successfully) attacking specific systems the Ukrainian military uses to manage its defense operations. Examples include communication equipment, command, and control systems, and, more broadly – the electrical grid. In that way, Russian forces could have debilitated the Ukrainian ability to resist with organized defense.

Secondly, it appears that cyber operations were integrated into conflict as an addition to existing military means. In most cases, they were complementary resources deployed in overall warfare. But there is no evidence that they have been effectively used to support military actions. In the observed population, just a few cases could have made a difference. The most notable is the attack on the ViaSat ISP. While it caused a loss of connection to thousands of customers, it did not produce connectivity issues for the Ukrainian military as initially assumed. Therefore, the most potent cyber-attack has not been proven particularly influential, let alone, pivotal.

In general, in the observed period of this conflict, cyber-attacks were used to cause destruction and disruption. As a result, Ukraine faced major communication outages, and some companies suffered data loss. But the effects remained restricted to cyberspace and did not spill to the physical domain, which is of key significance to kinetic conflict.

The above results were derived from the analysis performed using the proposed assessment framework. The framework has been proven effective for evaluating cyber operations in conflict. Still, the data used within was, to an extent, possibly incomplete, and some assumptions had to

be made while performing the evaluation. At the time of writing this conclusion, no publicly available information would invalidate the established opinion.

A few studies and explorations were already published on this subject. In particular, the authors delved into the potential reasons why offensive cyber operations did not yield the expected results in this war.

Some believe Russia focused its cyber efforts on espionage, representing Ukraine's largest cyber risk.[186] During the data collection for this analysis, it was observed that presumably Russian actors indeed conducted phishing campaigns delivering data collection malware to Ukrainian citizens, government, and media organizations.[187] It was, therefore, possibly crucial for Russia to preserve digital services for this purpose. For instance, they have perhaps safeguarded communication infrastructure to both "eavesdrop", and use it for their needs.[188]

Furthermore, the frequently mentioned rationale for the lack of expected impact from cyber operations is the Ukrainian readiness to defend its digital space.[189] Namely, past significant cyber-attacks, such as NotPetya and attacks on the electrical grid, raised cyber security awareness. As a result, the Ukrainian cyber security posture was "enhanced by assistance from intelligence, cyber security, and other government agencies from the US and UK".[190] The technical experts have come to help build the defending capacities, which Ukrainians have considerably improved over time. Besides, Ukraine benefited from collaborating with private companies, such as Microsoft and ESET, which provided their tools and expertise to combat the cyber-attacks as they unfolded along with kinetic conflict.[191]

So far, as claimed in the literature and confirmed with case study analysis, it appears that kinetic action is still the key to achieving military goals. But the more the states rely on technology in wartime and peacetime, the more vulnerable they will be to offensive cyber operations. Therefore, it is pertinent for states to ensure that defensive measures and resilience mechanisms become an integral part of their critical military and state infrastructure.

6.2 Future Research

In this thesis, the scope was limited to offensive cyber operations which Russia and affiliated actors have performed against Ukraine in wartime. While Ukraine primarily focused its efforts on defending its infrastructure, this nation-state also performed offensive cyber operations. During the war, Ukraine and pro-Ukrainian actors conducted cyber-attacks against the Russian infrastructure and companies, impairing their digital services.[192] Since the kinetic conflict was occurring on Ukrainian territory, the effort of using cyber operations was not directed towards support to kinetic capabilities. Still, it could have had some (possibly indirect) influence on the

war in Ukraine. Therefore, assessing such cyber operations (on conflict or society) could further contribute to the growing body of research on subject of cyber operation.

Appendix

This Appendix contains an analysis of the population of cyber operations, documented on a case-by-case basis. A summary of the results is documented in *Table 5*.

1.1 Cases

Cyber Operation 1

DDoS against a Kyiv-based media

See Chapter 4 – Applicability of proposed framework.

Cyber Operation 2

Governmental network devices targeted with destructive malware IsaacWiper

On February 24th, 2022, Russia started the invasion of Ukraine. On the same day, security researchers from ESET discovered that the governmental network suffered cyber-attacks. The malicious actors have deployed the data wiper IsaacWiper.[193] The analysts have found that the oldest compilation date of this malicious software dates to October 2021. Therefore, it is possible that this strain of malware was used in attacks even before the Russian military invasion. The malware was found in Windows Dynamic Link Library (DDL) or executable files (EXE).[194] Based on the research, malware recursively wiped each disk on the devices, destroying data and making them unusable. The attackers also included debugging functionality in a malware version deployed on the 25th of February, possibly because the program was not always performing as expected. This data manipulation attack was destructive, as the devices were wiped and made useless. The attack was attributed to Russia.[195]

The cyber-attack occurred at the start of the invasion, on 24th February 2022. On that date, Russian forces struck the military installation in the international airport at Boryspil and airports in Kharkiv, Ozerne, Kulbakino, Chuhuiv, Kramatorsk, and Chornobaivka.[196] Civilian infrastructure, such as residential buildings, has also been damaged by long-range artillery or missiles. Cities Kyiv, Odesa, and Mariupol suffered many attacks, and a hospital in Donetsk was hit, causing the death of four people and the injury of ten more.[197] The military operation focused on critical infrastructure on the ground and in cyberspace. It can be assumed that this cyber operation was integrated into conflict per complementary logic (in addition) since it produced effects that can be made only with cyber means on such a scale.

Cyber Operation 3

ISP Triolan experienced an outage due to changed configurations of the network devices (1)

On February 24th, 2022, Kharkiv-based ISP Triolan experienced an outage, leaving thousands of users without Internet access. The technical details on the attack are scarce, but a source disclosed to Forbes that the adversaries reset the network device settings to factory settings, which made them unusable.[198] To recover the service, engineers needed to restore devices physically, but they couldn't reach the ISP premises for safety reasons. The disruptive effects were primarily felt in the Kyiv and Kharkiv region. NetBlocks, a global internet monitoring service, noted a dip in traffic as the attack occurred.[199] Triolan estimated that the outage, which started early in the day, could last until late afternoon.[200] Since the attackers allegedly modified the configurations of network assets, this attack can be classified as data manipulation. It can be concluded that the service was disrupted, as customers could not access the internet. The attack was not attributed.[201]

The attack occurred on the first day of the Russian invasion. As noted in Case 1 and Case 2, which happened on the same date, the Russian forces attacked Kyiv and Kharkiv, cities in which effects of this incident were the most impactful. It appears that this cyber-attack occurred in addition (complementary logic) to conventional military attacks because it had properties typical to cyber-attack, such as large scale and character (reset of distributed devices).

Cyber Operation 4

ISP ViaSat experienced an outage after AcidRain data wiper attack

On February 24th, 2022, ISP ViaSat experienced an outage. In the early morning of the first day of the invasion, its internet modems located at customer premises started to go offline. The attack allegedly began once the adversaries misused the vulnerability of a virtual private network (VPN) appliance that provided access to the ViaSat internal network from the Internet.[202] Once they gained access, adversaries passed the demilitarized zone (a buffer zone between the Internet and the internal network) and accessed the trusted satellite Intranet. There, they navigated to a specific management network segment, where they selected a subset of Surfbeam2 modems based on their geographical properties. Once they reached the modem, they misused the vulnerable VPN system to escalate privileges. That allowed them to deploy the malicious executable AcidRain, which deleted data from the modem's memory. The analysis has shown that malware was pushed to the systems without obstacles, as modems were not configured to require authentication.[203] Besides Ukraine, the attack had effects across Europe as it spilled over. And so, the providers in various European states such as the UK, France, and the Czech Republic experienced outages of their services.[204] In Germany, for example, 5800 wind

turbines stopped working. And to restart them, the operators had to access each one of them physically. The total number of affected devices was about 27,000, which ViaSat started replacing soon after the incident. However, due to the scale of the incident, the Internet was not available for at least a week.[205]

In the aftermath of the attack, Ukrainian officials reported that the ViaSat hack caused "a really huge loss in communications at the very beginning of the war".[206] Later, those claims were clarified by their author. Victor Zhora, chief digital transformation officer at Ukraine's State Service of Special Communications and Information Protection, confirmed that communication loss occurred.[207] But, he stressed that the Ukrainian military used the Viasat satellite network as their backup. Hence, their primary communication means, the landlines and mobile network, remained operational as they were unaffected by the attack. Thus, the Viasat attack left private customers without access to the Internet during the critical first days of the war. Still, as initially speculated, it possibly did not impact Ukrainian military operations. In short, this cyber-attack involved data manipulation and disrupted Internet services in Ukraine in the critical first week of the war. The UK, US, and EU attributed this "unacceptable" attack to Russia.[208]

This cyber operation occurred on the first day of the invasion, the same as the past three discussed cases. On the 24th of February, Russian forces entered Ukraine from various directions attacking already-mentioned cities and destroying military facilities, such as the defense air base in Mariupol.[209] Based on this information, it can be assumed that the attackers aimed to impair the Ukrainian military and defense capabilities. Therefore, on a tactical level, attackers might have chosen to integrate the attack on ViaSat services with support logic to disable communication of the Ukrainian army. If that had happened, it could have helped to increase the probability of the attackers' military success. Nevertheless, such an outcome was avoided, as per the statement of Ukrainian officials. Consequently, it could be concluded that the cyber-attack was integrated into the war per complementary logic (in addition to other means), resulting in effects and scale only achievable with cyber means.

Cyber Operation 5

Universities websites defaced

On February 25th, 2022, at least 30 Ukrainian university websites were defaced.[210] Wordfence, the company protecting the websites of numerous Ukrainian services, including the ones of universities, provided their analysis of the attack. The company claimed that all 376 academic websites it protected suffered at least 200,000 attacks in the first days of the invasion. In this case, malicious actors from Brazil managed to exploit the vulnerability of the 30 WordPress-based websites which they defaced. The group claiming to be behind the attack is theMxOnday,

which also expressed its allegiance to Russia.[211] In this case, it can be concluded that data was modified to achieve disruptive effects.

This cyber operation occurred on the second day of the invasion, during which Russian forces entered the outskirts of Kyiv and managed to capture Kherson.[212] It can be assumed that this cyber operation was integrated into conflict per complementary logic (in addition to the existing means). That was concluded as the attack was executed by non-state actors who performed defacement attacks (which can only be achieved with cyber action).

Cyber Operation 6

Border control station for entering Romania targeted with malware

On February 26th, 2022, a data wiper attack hit the border control station systems for entering Romania from Ukraine.[213] Technical information on the attack is scarce. The security researcher Chris Kubecka, crossing from Ukraine to Romania during the cyber-attack, said that the border control office confirmed that they were targeted with a data wiper, which was already used to attack the government and financial sector in previous days. Kubecka also stated that due to the attack, she spent (along with other refugees) almost 40 hours waiting on the border for crossing, as the systems were unavailable due to the incident. As a result, the data had to be processed with "pen and paper ". This attack was performed by destroying digital data and has caused disruptive effects, as the governmental systems were not usable. To date, the attribution was not specified.

The 26th, 2022, marked the third day of the invasion. During the 26th, Russia attacked several targets. For instance, they attacked Vasylkiv military Air Base near Kyiv and hit multiple fuel tanks.[214] Similarly, explosions were reported near Kyiv and its second major airport. On the same day, Ukraine closed its borders to Russia and Belarus. By the 26th, 120,000 people had already fled the country, which caused queues at the number of border crossings. Therefore, it appears that the attack on the border control system was planned to support creating chaos and further delay refugee crossing. The attack was possibly integrated per substitution logic. As Russian forces concentrated on three other fronts, east, north, and south, it may be assumed that attackers chose for cyber-attack instead of military action on the western border. Additionally, it could be considered that Russian forces were deterred from attacking the border station with Romania with arms, as Romania is a member of NATO. An imprecise attack could escalate further, resulting in direct conflict with the Alliance.

Cyber Operation 7

Governmental and financial services websites attacked with DDoS attack

On February 28th, 2022, Ukrainian governmental and financial websites were attacked with DDoS attack. The adversaries used the "Zhadnost" botnet with more than 3,000 IP addresses globally.[215] The Security Scorecard research showed that the attack was performed using DNS amplification.[216] In such an attack, the adversary sends thousands of spoofed requests to the Domain Name Server (DNS).[217] The DNS replies to the spoofed IP address belonging to the targeted system. As a result, the victim is overwhelmed with DNS replies. Such a type of attack is often performed by a botnet. The attackers can craft DNS requests to expect large amounts of data in return, congesting the network.[218] The research has shown that the DDoS attack had at least 34 bots, mostly misconfigured MicroTik devices.[219] The SecurityScorecard attributed this disruptive attack with moderate confidence to Russia or Russia-linked actors.

On 28th February, Russia continued attacking the cities of Kyiv and Kharkiv.[220] No other notable events occurred on or the day before and after. Therefore, it appears that this cyber-attack was integrated per complementary logic on a tactical level, as it achieved effects that are not available by other means (e.g., scale).

Cyber Operation 8

A media company in Kyiv attacked with DesertBlade malware

On March 1st, 2022, a major media broadcasting company based in Kyiv got attacked by DesertBlade data wiper.[221] The destructive program was deployed via Group Policy Object (GPO), a mechanism used for centralized management of configurations and deployment of software in an enterprise IT environment.[222] Microsoft reported on the malware and noted that further technical details could not be shared due to an agreement with partners. Microsoft attributed the attack to Russia. Since the wiper was used in the attack, the data was manipulated and destroyed.

On the same day, the television tower in Kyiv was struck with missiles.[223] It can be concluded that this cyber-attack was integrated on a tactical level into the military action per substitution logic (instead of). Since the Russian forces were performing the kinetic attacks on Kyiv media, they could have also executed the physical attack against this cyber-attack media to disrupt the media broadcasting infrastructure. However, the attacker may have chosen to use a cyber-attack instead as it can achieve same the effects as kinetic action. This cyber-attack supported overall warfare and efforts to destabilize Ukraine. In this case, the target was the media, essential services in times of uncertainty when accurate and timely information is crucial. Russia stated on the 1st of March that the (kinetic) incident aimed to thwart "informational" attacks.[224]

Cyber Operation 9

The Webmail server of the Ministry of Defense suffered a DDoS attack

On March 4th, 2022, the Ukrainian Ministry of Defense suffered a DDoS attack on their email servers. To attack the Ukrainian Ministry of Defense web server, malicious actors used Malware-as-a-Service, DanaBot, which has executables that offer DDoS functionality.[225] Based on the information, the webmail was still available at the time of the attack, and there is no additional information on the effects. Additionally, the attribution of the attack is unknown.

On 4th March, Russian forces attacked Zaporizhzhya nuclear power plant and besieged Mariupol and Kharkiv.[226] It could be assumed that this cyber-attack was integrated into conflict per support logic, as the aim was probably to impair the communication of the Ministry of Defense, which is vital in wartime. The possible goal was to increase the probability of success of another course of action (military offensive), by delaying information sharing and communication among military personnel during the armed conflict.

Cyber Operation 10

ISP Triolan experienced an outage due to changed configurations of the network devices (2)

On March 9th, 2022, ISP Triolan experienced another outage. The first cyber-attack is detailed under "Cyber Operation 3" and occurred on 24th February. While technical details are scarce, some sources noted that both attacks were performed similarly: by resetting network devices to factory levels.[227] Due to the attack, Triolan Internet service was down nationally for over 12 hours. It took a day to recover 70% of the attacked nodes in Kyiv, Kharkiv, Dnipro, Poltava, Odesa, Rivne, and Zaporizhzhya.[228] Since the attackers allegedly modified the configurations of network assets, this attack can be classified as data manipulation. It can be concluded that the service was disrupted, as customers could not access the internet. Triolan attributed the attack to Russia.[229]

On March 9th Russian forces bombed a maternity hospital in Mariupol amid the 12 hours pause of hostilities to allow refugees to evacuate.[230] The refugee evacuation from Kyiv suburbs and the town of Bucha failed. The attacks on Kyiv and Kharkiv continued.[231] It appears that this cyber-attack occurred in addition (complementary logic) to conventional military attacks because it had properties typical to cyber-attack, such as large scale and character (reset of devices).

Cyber Operation 11

Organizations targeted with destructive malware CaddyWiper

On March 14th, 2022, ESET researchers noted that they had discovered a new type of data wiper that attacked Ukrainian organizations.[232] The malware was delivered to targeted networks

before the attack, as it was planted in the mechanism for central management of the IT environment (Group Policy) from where it was executed against devices. Once deployed, it deleted files and physical device partitions. The wiper avoided deleting files from the domain controllers (central management and authentication servers) to ensure the attackers could keep access to the environment while executing the attacks. Furthermore, ESET claimed that the malware targeted a limited number of organizations without specifying the sectors. Microsoft attributed the attack to Russia.[233] This type of attack consisted of data manipulation and resulted in its destruction.

On March 14th, Russian forces continued attacking Kyiv and seizing Mariupol.[234] Since the targeted organizations are unknown, it can only be speculated that this attack was integrated per complementary logic due to its properties of scale (multiple targets). The integration could have been characterized under support logic if it was known that the organization was related to the Ukrainian military. For instance, the destructive malware could have deleted key information from the military devices, possibly damaging capabilities and relevant information of Ukrainian forces.

Cyber Operation 12

Organization targeted with malicious data wiper Junkmail

On March 16th, 2022, Mandiant reported that Junkmail wiper targeted Ukrainian organization. The security company noted that malware was configured to be executed via a scheduled task three hours before president Zelensky was scheduled to deliver a speech to the U.S. Congress.[235] In its address, Zelensky called for a humanitarian no-fly zone over Ukraine.[236] On the same day, Russia bombed a theatre in the encircled city of Mariupol, in which Ukrainians took shelter, and heavy fighting continued in the vicinity of Kyiv. The attack has been attributed to Russia. However, no further technical details on this data manipulation attack are available, and it was not made public which organization suffered the data destruction. Therefore, it is not feasible to assume the logic of integration.

Cyber Operation 13

Media companies targeted with web defacement attack

On March 17th, 2022, mass media companies in Ukraine were targeted with web defacement attacks. The Ukrainian Security Service reported that banned symbols used by occupiers (Russia) were placed on the media websites, disrupting the regular news broadcasting operations.[237] The additional technical details were not made available to the public. The attack was attributed to Russia. On the same day, Russia struck a theatre in the besieged city of Mariupol, where hundreds of people were sheltering.[238] But, it does not appear that this cyber-

attack supported military action. It was most likely incorporated in conflict per complementary logic, especially considering that web defacement effects cannot be achieved with other means.

Cyber Operation 14

Private companies targeted with destructive malware DoubleZero

On March 22nd, 2022, The Computer Emergency Response Team of Ukraine released an advisory on DoubleZero, another data wiper found in Ukraine.[239] DoubleZero is a .NET program that overwrites files on devices with zero blocks. Then it destroys the Windows registry, a hierarchical database that stores low-level settings from the operating system and applications.[240] After the files have been wiped, the devices shut down. The attack was attributed to Russia.[241] The reports did not expressly state what organizations were targeted with the destructive malware. On March 22nd, Ukrainian forces started with a counterattack on Kyiv's north and west and regained control of Makariv, a town near Kyiv.[242] Since there is a lack of information on the type of organizations which suffered the attack, it could be concluded that this attack was probably integrated with complementary logic, due to its effects and scale.

1.2 Summary of cyber operations assessment

Cyber Op. ID	Date	Short Description	Cyber Operation Type	Cyber Operation Effect	Logic of Integration	Military Action	Targeted Sector	Attribution	Sources
1	24/02/2022	DDoS against a Kyiv-based media	DoS	Disrupt	Substitute	Start of invasion and missiles attacks on Kyiv.	Commercial Facilities	Russia	162, 163, 164
2	24/02/2022	Governmental network devices targeted with destructive malware IsaacWiper	Data Manipulation	Destroy	Complement	Start of invasion and multiple military attacks on various cities.	Government Facilities	Russia	193, 194, 195, 196, 197
3	24/02/2022	ISP Triolan experienced an outage due to changed configurations of the network devices (1)	Data Manipulation	Disrupt	Complement	Start of invasion and attack on Kyiv and Kharkiv.	Communications	Unknown	198, 199, 200, 201
4	24/02/2022	ISP ViaSat experienced an outage after AcidRain data wiper attack	Data Manipulation	Disrupt	Complement	Start of invasion and multiple military attacks on various cities.	Communications	Russia	202, 203, 204, 205, 206, 207, 208, 209
5	25/02/2022	University websites defaced	Data Manipulation	Disrupt	Complement	Start of invasion and multiple military attacks on various cities.	Government Facilities	theMxOnday (Brazil)	210, 211, 212
6	26/02/2022	Border control station for entering Romania targeted with data wiper	Data Manipulation	Disrupt	Substitute	Attacks on multiple cities and military facilities, refugees fleeing Ukraine.	Government Facilities	Unknown	213, 214
7	28/02/2022	Governmental and financial services websites attacked with DDoS attack	DoS	Disrupt	Complement	Attacks on Kyiv and Kharkiv.	Government Facilities, Financial Services	Russia or affiliated actors	215, 216, 217, 218, 219, 220

Cyber Op. ID	Date	Short Description	Cyber Operation Type	Cyber Operation Effect	Logic of Integration	Military Action	Targeted Sector	Attribution	Sources
8	01/03/ 2022	Media company in Kyiv attacked with DesertBlade malware	Data Manipulation	Destroy	Substitute	Missiles attack on Kyiv television tower.	Commercial Facilities	Russia	221, 222, 223, 224
9	04/03/ 2022	Webmail server of Ministry of Defense suffered DDoS attack	DoS	Disrupt	Support	Russian forces attacked Zaporizhzhya nuclear power plant, and besieged Mariupol and Kharkiv.	Government Facilities	Unknown	225, 226
10	09/03/ 2022	ISP Triolan experienced an outage due to changed configurations of the network devices (2)	Data Manipulation	Disrupt	Complement	The attacks on Kyiv and Kharkiv continued. Mariupol maternity hospital bombed.	Communications	Russia	227, 228, 229, 230, 231
11	14/03/ 2022	Organizations targeted with destructive malware CaddyWiper	Data Manipulation	Destroy	Complement	Attack on Kyiv and siege of Mariupol.	Unknown	Russia	232, 233, 234
12	16/03/ 2022	Organization targeted with malicious data wiper Junkmaiil	Data Manipulation	Destroy	Lack of Information	President Zelensky speech in front of the US Congress, calling for a no-fly zone. Attacks on cities including Kyiv.	Unknown	Russia	235, 236
13	17/03/ 2022	Media companies targeted with web defacement attack	Data Manipulation	Disrupt	Complement	Russia attacked a theatre in Mariupol in which hundreds found shelter.	Commercial Facilities	Russia	237, 238
14	17/03/ 2022	Private companies targeted with destructive malware DoubleZero	Data Manipulation	Destroy	Complement	Ukrainian forces started a counteroffensive.	Unknown	Russia	239, 240, 241, 242

Table 5 - Summary of cyber operations assessment

References

[1] Natalia Zinets and Aleksandar Vasovic, "Missiles rain down around Ukraine," Reuters, February 24, 2022, Accessed February 22, 2023, https://www.reuters.com/world/europe/putin-orders-military-operations-ukraine-demands-kyiv-forces-surrender-2022-02-24/.
[2] "Ukraine war: Three dead as maternity hospital hit by Russian air strike," BBC, March 10, 2022, Accessed February 22, 2023, https://www.bbc.com/news/world-europe-60675599.
[3] "Ukraine: Timeline of Cyberattacks," CyberPeace Institute, June 8, 2022, Accessed January 21, 2022, https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks.; Cynthia Brumfield, "Russia-linked cyberattacks on Ukraine: A timeline," August 24, 2022, Accessed February 17, 2023, https://www.csoonline.com/article/3647072/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html.
[4] Joe Tidy, "Ukraine crisis: 'Wiper' discovered in latest cyber-attacks," BBC, February 24, 2022, Accessed February 22, 2023, https://www.bbc.com/news/technology-60500618.; Alicia Hope, "Major Ukrainian Internet Provider Triolan Suffers Severe Cyber Attacks and Infrastructure Destruction During Russian Invasion," CPO Magazine, March 16, 2022, Accessed February 22, 2023, https://www.cpomagazine.com/cyber-security/major-ukrainian-internet-provider-triolan-suffers-severe-cyber-attacks-and-infrastructure-destruction-during-russian-invasion/.
[5] Kyle Alspach,"Ukraine border control hit with wiper cyberattack, slowing refugee crossing," Venture Beat, February 27, 2022, Accessed February 22, 2023, https://venturebeat.com/security/ukraine-border-control-hit-with-wiper-cyberattack-slowing-refugee-crossing/.
[6] Shmuel Even and David Siman-Tov, "Cyber Warfare: Concepts and Strategic Trends," Institute for National Security Studies, May 2012, https://www.files.ethz.ch/isn/152953/inss%20memorandum_may2012_nr117.pdf. 9.
[7] Ibid. 30.
[8] Max Smeets, "No Shortcuts - Why States Struggle To Develop a Military Cyber-Force," Hurst, 2022, 1.
[9] "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit," CCDCOE, Accessed January 21, 2023, https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/.
[10] Ibid.
[11] Thomas Rid, "Cyber War Will Not Take Place," Oxford University Press, 2013, The Argument - xiv.
[12] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, "Cyber Persistence Theory - Redefining National Security in Cyberspace," Oxford University Press, 2022, 7.
[13] John Arquilla and Davir Ronfeldt, "In Athena's Camp: Preparing for Conflict in the Information Age: Cyberwar is Coming!," RAND Corporation, 1997, 27, 30-31.
[14] Thomas Rid, "Cyber War Will Not Take Place," Oxford University Press, 2013, The Argument xiv-xv, 37, 42-43.
[15] Eric Gratzke, "The Myth of Cyberwar," MIT Press, International Security, Volume 38, Number 2, Fall 2013, pp. 41-73 (Article), 43, 49, 57-58, 72.
[16] David J. Betz and Tim Stevens, "Cyberspace and the State", Routledge, 2011, 91.
[17] Martin C. Libicki, "Why Cyber War Will Not and Should Not Have Its Grand Strategist," Air University Press Strategic studies quarterly: SSQ, 2014, Vol.8 (1), p.23-39, 2014, https://www.jstor.org/stable/26270603, 16.
[18] Jeff Erickson, "The Possibility Of A Cyber Pearl Harbor Remains Real, Says Former CIA Director," March 19, 2019, Accessed January 31, 2023, https://www.forbes.com/sites/oracle/2019/03/13/the-possibility-of-a-cyber-pearl-harbor-remains-real-says-former-cia-director/.
[19] Adam Stone, "How Leon Panetta's 'Cyber Pearl Harbor' warning shaped Cyber Command," C4ISRNET, July 30, 2019, Accessed February 1, 2023, https://www.c4isrnet.com/opinion/2019/07/30/how-leon-panettas-cyber-pearl-harbor-warning-shaped-cyber-command/.
[20] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, "Cyber Persistence Theory - Redefining National Security in Cyberspace," Oxford University Press, 2022, 4.
[21] Nathan Gardels, "Mike McConnell: An American Spymaster on Cyberwar," Huff Post, August 8, 2009, Accessed February 1, 2022, https://www.huffpost.com/entry/mike-mcconnell-an-america_b_227944.
[22] Jane Perlez, "U.S. and China Put Focus on Cybersecurity," April 20, 2013, Accessed February 3, 2023, https://www.nytimes.com/2013/04/23/world/asia/united-states-and-china-hold-military-talks-with-cybersecurity-a-focus.html.
[23] Martin C. Libicki, "Why Cyber War Will Not and Should Not Have Its Grand Strategist," Air University Press Strategic studies quarterly: SSQ, 2014, Vol.8 (1), p.23-39, 2014, https://www.jstor.org/stable/26270603, 14.
[24] Nadya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?," Journal of Conflict Resolution, 2013, 63(2), 317–347. https://doi.org/10.1177/0022002717737138, 6.
[25] Monica Kaminska, James Shires, and Max Smeets, "Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far)," July 2022, https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf.
[26] Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK, 8.
[27] "Cyberspace," NIST, Accessed March 10, 2023, https://csrc.nist.gov/glossary/term/cyberspace.

[28] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, "Cyber Persistence Theory - Redefining National Security in Cyberspace," Oxford University Press, 2022, 34.
[29] For example, weaknesses in systems can be exploited to cause destruction of data, causing financial and other damage.
[30] Florian J. Egloff and James Shires, "Offensive Cyber Capabilities and State Violence: Three Logics of Integration," Journal of Global Security Studies, Volume 7, Issue 1, March 2022, https://doi.org/10.1093/jogss/ogab028, 1.
[31] "Cyberspace Operations, " NIST, Accessed October 23, 2022, https://csrc.nist.gov/glossary/term/cyberspace_operations#:~:text=Definition(s)%3A,objectives%20in%20or%20through%20cyberspace.
[32] "Defense Primer: Cyberspace Operations," Congressional Research Service, December 9, 2022, Accessed January 13, 2023, https://sgp.fas.org/crs/natsec/IF10537.pdf.
[33] Bruce Schneier, "Computer Network Exploitation vs. Computer Network Attack," Schneier on Security, March 10, 2014, Accessed October 23, 2022, https://www.schneier.com/blog/archives/2014/03/computer_networ.html.
[34] Eric D. Knapp and Joel Thomas Langill, "Industrial Network Security (Second Edition)," Syngress, 2015, 191.
[35] Michael B Kelley, "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought," Business Insider, November 13, 2013, Accessed December 7, 2022, https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?international=true&r=US&IR=T.
[36] "What Is Stuxnet?," Malwarebytes, Accessed November 30, 2022, https://www.malwarebytes.com/stuxnet.
[37] Yoram Dinstein and Willy Arne Dahl, "Oslo Manual on Select Topics of the Law of Armed Conflict", Springer, 2020, https://doi.org/10.1007/978-3-030-39169-0_2, 20.
[38] "Titan Rain," Council on Foreign Relations, August 2005, Accessed November 30, 2022, https://www.cfr.org/cyber-operations/titan-rain.
[39] Quentin E. Hodgson, Yuliya Shokh, and Jonathan Balk, "Many Hands in the Cookie Jar," RAND Corporation, 2022, https://www.rand.org/pubs/research_reports/RRA1190-1.html, 25.
[40] Richard J. Harknett and Max Smeets, "Cyber campaigns and strategic outcomes," Journal of Strategic Studies, 45:4, 534-567, https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1732354, 9.; "Defense Primer: Cyberspace Operations", Congressional Research Service, December 9, 2022, Accessed January 13, 2023, https://sgp.fas.org/crs/natsec/IF10537.pdf.
[41] "Defensive Cyber Operations," ENSCO, Accessed January 14, 2022, https://www.ensco.com/cyber/defensive-cyber-operations.
[42] "Defensive Cyberspace Operations," Marine Corps Forces Reserve, Accessed January 14, 2022, https://www.marforres.marines.mil/Units/Force-Headquarters-Group/DCO-IDM/.
[43] "Defend Forward and Persistent Engagement," U.S. Cyber Command, October 25, 2022, Accessed January 14, 2023, https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/.
[44] Josephine Wolff, "How do we know when cyber defenses are working?," Brookings, October 5, 2022, Accessed February 18, 2023, https://www.brookings.edu/techstream/how-do-we-know-when-cyber-defenses-are-working/.
[45] "DoD Joint Terminology for Cyberspace Operations," Department of Defense, November 2020, Accessed February 18, 2023, https://publicintelligence.net/dod-joint-cyber-terms/.
[46] Li Yuchong and Liu Qinghui, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, Volume 7, November 2021, Pages 8176-8186, September 3, 2021, Accessed February 18, 2023, https://www.sciencedirect.com/science/article/pii/S2352484721007289.
[47] Max Smeets, "No Shortcuts - Why States Struggle To Develop a Military Cyber-Force," Hurst, 2022, 1, 15-16.
[48] "Understanding Denial-of-Service Attacks," CISA, October 28, 2022, Accessed February 17, 2023, https://www.cisa.gov/uscert/ncas/tips/ST04-015.
[49] Ibid.
[50] "Understanding Denial-of-Service Attacks," CISA, October 28, 2022, Accessed February 17, 2023, https://www.cisa.gov/uscert/ncas/tips/ST04-015.
[51] "What is denial of service attack (DoS)," Palo Alto, Accessed February 17, 2023, https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos#:~:text=A%20Denial%2Dof%2DService%20(,information%20that%20triggers%20a%20crash.
[52] Nick Lewis, "How to stop a DDoS after initiation," Computer Weekly, March 23, 2011, Accessed February 17, 2023, https://www.computerweekly.com/tip/How-to-stop-a-DDoS-attack-after-initiation.
53 Rain Ottis, "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective," Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, 2008, Reading: Academic Publishing Limited, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf, pp 163-168.
[54] "Hybrid Threats: 2007 Cyber Attacks on Estonia," NATO StratCom Centre of Excellence, NATO StratCom, Accessed December 4, 2022, https://www.stratcomcoe.org/hybrid-threats-2007-cyber-attacks-estonia, 3.
[55] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," The Guardian, May 17, 2007, Accessed December 4, 2022, https://www.theguardian.com/world/2007/may/17/topstories3.russia.
[56] Max Smeets, "No Shortcuts - Why States Struggle To Develop a Military Cyber-Force," Hurst, 2022, 16.
[57] "CIA Triad,", Fortinet, https://www.fortinet.com/resources/cyberglossary/cia-triad.

[58] Drew Todd, "Top 10 Data Breaches of All Time," September 14, 2022, Accessed February 17, 2023, https://www.secureworld.io/industry-news/top-10-data-breaches-of-all-time.
[59] "Chinese Military Hackers Charged in Equifax Breach," FBI, February 10, 2020, Accessed February 18, 2023, https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020.
[60] "CIA Triad,", Fortinet, https://www.fortinet.com/resources/cyberglossary/cia-triad.
[61] David Maynor, Matt Olney and Yves Younan, "The MeDoc Connection," Talos, July 5, 2017, Accessed December 14, 2022, https://blog.talosintelligence.com/the-medoc-connection/.
[62] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, August 22, 2018, Accessed December 14, 2022, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[63] "Statement from the Press Secretary," Trump White House Archive, February 15, 2018, Accessed December 14, 2022, https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.
[64] Polina Ivanova, "Kremlin Rejects US Accusation That It Was behind Massive 'NotPetya' Cyber Attack, Blames 'Russophobia'," Business Insider, February 16, 2018, Accessed December 14, 2022, https://www.businessinsider.com/kremlin-rejects-us-accusation-that-it-was-behind-notpetya-cyber-attack-2018-2?international=true&r=US&IR=T.
[65] "CIA Triad," Fortinet, Accessed February 17, 2023, https://www.fortinet.com/resources/cyberglossary/cia-triad.
[66] "Website Defacement Attack," Imperva, Accessed February 17, 2023, https://www.imperva.com/learn/application-security/website-defacement-attack/.
[67] Catalin Cimpanu, "Hackers deface Ukrainian government websites," January 14, 2022, Accessed February 17, 2023, https://therecord.media/hackers-deface-ukrainian-government-websites/.
[68] Max Smeets, "No Shortcuts - Why States Struggle To Develop a Military Cyber-Force," Hurst, 2022, 16.
[69] Ibid.
[70] "Compromise of a Power Grid in Eastern Ukraine," Council on Foreign Relations, December 2015, Accessed December 7, 2022, https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine.
[71] Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," E-ISAC ICS SANS, March 2016, https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf, 4,7-16.
[72] Alan Haji, "Industroyer – Crash Override (2016)," CCDCOE, Accessed March 11, 2023, https://cyberlaw.ccdcoe.org/wiki/Industroyer_%E2%80%93_Crash_Override_(2016).
[73] Jai Vijayan, "First Malware Designed Solely for Electric Grids Caused 2016 Ukraine Outage," Dark Reading, June 12, 2017, Accessed March 9, 2023, https://www.darkreading.com/threat-intelligence/first-malware-designed-solely-for-electric-grids-caused-2016-ukraine-outage.
[74] Tom Uren, Bart Hogeveen, and Fergus Hanson, "Defining Offensive Cyber Capabilities," Australian Strategic Policy Institute, July 4, 2018, Accessed 4 December 2022, https://www.aspi.org.au/report/defining-offensive-cyber-capabilities.
[75] John Reed, "The Five Deadly Ds of the Air Force's Cyber Arsenal," Foreign Policy, April 12, 2013, Accessed October 23, 2022, https://foreignpolicy.com/2013/04/12/the-five-deadly-ds-of-the-air-forces-cyber-arsenal/.
[76] Max Smeets, "No Shortcuts - Why States Struggle To Develop a Military Cyber-Force, " Hurst, 2022, 1, 15-16.; Smeets also mentions espionage. However, in his view, espionage is separated from cyber-attacks. Since this thesis focuses on the offensive cyber capabilities that can directly participate in the kinetic conflict, espionage is outscoped; "Computer Network Attack," NIST, Accessed February 18, 2023, https://csrc.nist.gov/glossary/term/computer_network_attack.
[77] Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/.
[78] Maathuis, C., W. Pieters , and J. van den Berg, "Developing a Cyber Operations Computational Ontology," Journal of Information Warfare, 2018, Vol.17 (3), 2018, pp.32-49, https://repository.tudelft.nl/islandora/object/uuid:b9aedb25-255a-4882-942e-8c697b14a563?collection=research, 4.
[79] Ibid, 6.
[80] Trey Herr and Drew Herrick, "Military Cyber Operations: A Primer," The American Foreign Policy Council, January 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2725275, 2, 5-7.
[81] Ibid, 5.
[82] Oliver Fitton, "Cyber Operations and Gray Zones: Challenges for NATO," Connections Vol. 15, No. 2 (Spring 2016), Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, pp.109-119, https://www.jstor.org/stable/26326443#metadata_info_tab_contents, 3-4.
[83] Brandon Valeriano and Ryan C. Maness, "Cyber War versus Cyber Realities: Cyber Conflict in the International System," Oxford University Press, 2015, https://academic.oup.com/book/25308, 3.
[84] Nye, Joseph S. 2011a. "Nuclear Lessons for Cyber Security?", Strategic Studies Quarterly, Vol. 5, No. 4 (Winter 2011), pp. 18-38 (21 pages), 21.
[85] Brandon Valeriano and Ryan C. Maness, "Cyber War versus Cyber Realities: Cyber Conflict in the International System," Oxford University Press, 2015, https://academic.oup.com/book/25308, 3.; Thomas Rid, "Cyber War Will Not Take Place," Oxford University Press, 2013, The Argument - xiv.
[86] Ibid. 34.
[87] Ibid. 25, 62, 116.

[88] Richard J. Harknett and Max Smeets, "Cyber campaigns and strategic outcomes," March 4, 2020, Journal of Strategic Studies, 45:4, 534-567, https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1732354, 2-3.
[89] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, "Cyber Persistence Theory - Redefining National Security in Cyberspace," Oxford University Press, 2022, 7.
[90] "Joint Communications to the European Parliament and the Council – EU Policy on Cyber Defence," European Commission, November 11, 2022, Accessed March 12, 2023, https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf, 2.
[91] Florian J. Egloff, and James Shires, "Offensive Cyber Capabilities and State Violence: Three Logics of Integration," Journal of Global Security Studies, Volume 7, Issue 1, March 2022, https://doi.org/10.1093/jogss/ogab028, 6-11.
[92] Ibid. 8, 14.
[93] Ibid, 7.
[94] Florian J. Egloff, and James Shires, "Offensive Cyber Capabilities and State Violence: Three Logics of Integration," Journal of Global Security Studies, Volume 7, Issue 1, March 2022, https://doi.org/10.1093/jogss/ogab028, 6-11.
[95] David A. Dulghum and Douglas Barrie, "Israel used electronic attack in air strike against Syrian mystery target," ABC News, October 8, 2007, Accessed January 15, 2023, https://abcnews.go.com/Technology/story?id=3702807&page=1.
[96] "Georgia-Russia conflict (2008)," CCDCOE, September 17, 2022, Accessed January 15, 2023, https://cyberlaw.ccdcoe.org/wiki/Georgia-Russia_conflict_(2008).
[97] Max Smeets, "No Shortcuts - Why States Struggle To Develop a Military Cyber-Force," Hurst, 2022, 6-8.
[98] Thomas Rid, "Cyber War Will Not Take Place," Oxford University Press, 2013, 36.
[99] Lennart Maschmeyer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations," International Security 2021; 46 (2): 53, 55, 5, 14-15.
[100] David J. Betz and Tim Stevens, "Cyberspace and the State," Routledge, 2011, 98.
[101] Monica Kaminska, "Restraint under Conditions of Uncertainty: Why the United States Tolerates Cyberattacks," Oxford University Press - Journal of Cybersecurity, Volume 7, Issue 1, 2021, March 9, 2021, https://academic.oup.com/cybersecurity/article/7/1/tyab008/6162971, 2.
[102] Florian J. Egloff and Max Smeets, "Publicly attributing cyber-attacks: a framework," Journal of Strategic Studies, March 10, 2021, https://www.tandfonline.com/doi/full/10.1080/01402390.2021.1895117, 7, 33.
[103] David J. Betz and Tim Stevens, "Cyberspace and the State," Routledge, 2011, 89-90.
[104] Lucas Kello, "The Virtual Weapon and International Order," Yale University Press, 2018, 78.
[105] Brandon Valeriano and Ryan C. Maness, "Cyber War versus Cyber Realities: Cyber Conflict in the International System," Oxford University Press, 2015, https://academic.oup.com/book/25308, 2.
[106] "Ukraine", CIA Factbook, Accessed December 14, 2022, https://www.cia.gov/the-world-factbook/countries/ukraine/#people-and-society.
[107] Jeffrey Mankoff, "Russia's War in Ukraine: Identity, History, and Conflict," Center for Strategic and International Studies, April 22, 2022, https://www.csis.org/analysis/russias-war-ukraine-identity-history-and-conflict, 5.
[108] Orysia Lutsevych and Jon Wallace, "Ukraine-Russia Relations," Chatham House, March 24, 2022, Accessed December 6, 2022, https://www.chathamhouse.org/2021/11/ukraine-russia-relations.
[109] "Ukraine - Economic Difficulties," Britannica, Accessed December 6, 2022, https://www.britannica.com/place/Ukraine/Economic-difficulties.
[110] Jonathan Masters, "Ukraine: Conflict at the Crossroads of Europe and Russia," Council on Foreign Affairs, October 11, 2022, Accessed December 6, 2022, https://www.cfr.org/backgrounder/ukraine-conflict-crossroads-europe-and-russia.
[111] Ibid.
[112] Matthew Mpoke Bigg, "A History of the Tensions between Ukraine and Russia," New York Times, March 26, 2022, Accessed December 6, 2022, https://www.nytimes.com/2022/03/26/world/europe/ukraine-russia-tensions-timeline.html.
[113] Vladimir Putin, "Message from the President of the Russian Federation," Kremlin, March 18, 2014, Accessed December 6, 2022, http://en.kremlin.ru/events/president/news/66181.
[114] Orysia Lutsevych and Jon Wallace, "Ukraine-Russia Relations," Chatham House, March 24, 2022, Accessed December 6, 2022, https://www.chathamhouse.org/2021/11/ukraine-russia-relations.
[115] Jonathan Masters, "Ukraine: Conflict at the Crossroads of Europe and Russia," Council on Foreign Affairs, October 11, 2022, Accessed December 6, 2022, https://www.cfr.org/backgrounder/ukraine-conflict-crossroads-europe-and-russia.
[116] Meijun Li, "How Did We Get Here? Russia, Crimea, and the West," Pacific Council, November 14, 2018, Accessed December 6, 2022, https://www.pacificcouncil.org/newsroom/how-did-we-get-here-russia-crimea-and-west.
[117] Georgi Gotev, "Putin's World: Selected Quotes from a Disturbing Speech," Euractiv, February 22, 2022, Accessed December 6, 2022, https://www.euractiv.com/section/global-europe/news/putins-world-selected-quotes-from-a-disturbing-speech/.
[118] Orysia Lutsevych and Jon Wallace, "Ukraine-Russia Relations," Chatham House, March 24, 2022, Accessed December 6, 2022, https://www.chathamhouse.org/2021/11/ukraine-russia-relations.

[119] Roman Olearchynk and Ben Hall, "Zelensky forced to 'face reality' over peace process with Russia," Financial Times, May 3, 2021, Accessed December 14, 2022, https://www.ft.com/content/b8e7489d-bfa9-4a1f-aa1e-ba441bb0d354.
[120] Matthew Mpoke Bigg, "A History of the Tensions between Ukraine and Russia," New York Times, March 26, 2022, Accessed December 6, 2022, https://www.nytimes.com/2022/03/26/world/europe/ukraine-russia-tensions-timeline.html.
[121] "Ukraine conflict: Russian forces attack from three sides," BBC, February 24, 2022, Accessed December 15, 2022, https://www.bbc.com/news/world-europe-60503037.
[122] "February 24, 2022 Russia-Ukraine news", CNN, February 25, 2022, Accessed December 15, 2022, https://edition.cnn.com/europe/live-news/ukraine-russia-news-02-24-22-intl/index.html.
[123] "Ukraine conflict: Russian forces attack from three sides," BBC, February 24, 2022, Accessed December 15, 2022, https://www.bbc.com/news/world-europe-60503037.
[124] "Six months on, the Russia-Ukraine war mapped out," Al Jazeera, August 23, 2022, Accessed December 16, 2022, https://www.aljazeera.com/news/longform/2022/8/23/russia-ukraine-war-after-six-months-explained-in-maps.
[125] Adam Taylor, "Mariupol siege endgame means very different things for Kyiv and Moscow," The Washington Post, May 6, 2022, Accessed December 16, 2022, https://www.washingtonpost.com/world/2022/05/06/seige-mariupol-azovstal-last-stand-russia/.
[126] "Russia says Azovstal siege is over, in full control of Mariupol," Al Jazeera, May 21, 2022, Accessed December 16, 2022, https://www.aljazeera.com/news/2022/5/21/russia-azovstal-siege-over-full-control-ukraines-mariupol.
[127] Matthew Mpoke Bigg, "Russia invaded Ukraine more than 200 days ago. Here is one key development from every month of the war," The New York Times, September 13, 2022, Accessed December 16, 2022, https://www.nytimes.com/article/ukraine-russia-war-timeline.html.
[128] "Putin declares four areas of Ukraine as Russian," BBC, September 30, 2022, Accessed December 12, 2022, https://www.bbc.com/news/live/world-63077272/page/4.
[129] Hannah Ritchie, Tim Lister and Josh Pennington, "Massive blast cripples parts of Crimea-Russia bridge, in blow to Putin's war effort," CNN, October 8, 2022, Accessed December 17, 2022, https://edition.cnn.com/2022/10/08/europe/crimea-bridge-explosion-intl-hnk/index.html.
[130] Jaroslav Lukiv, "Ukraine war: Power and water supply hit across Ukraine in 'massive' Russian missile strikes," BBC, October 31, 2022, Accessed December 17, 2022, https://www.bbc.com/news/world-europe-63454230
[131] Jonathan Landay and Tom Balmforth, "Ukraine forces advance on two fronts, cross Russian lines in the south,", Reuters, October 3, 2022, Accessed December 17, 2022, https://www.reuters.com/world/europe/ukraine-celebrates-capturing-key-town-putin-ally-mulls-possible-nuclear-response-2022-10-02/.
[132] Harry Taylor, Ben Quinn, and Samantha Lock, "Russia-Ukraine war: Zelenskiy says Kherson 'never gave up' as Ukrainian troops reach city centre – as it happened," Guardian, November 11, 2022, Accessed December 17, 2022, https://amp.theguardian.com/world/live/2022/nov/11/russia-ukraine-war-live-news-kyivs-forces-close-in-on-kherson-reclaim-dozens-of-towns-in-south.
[133] "Ukraine updates: Kyiv, other cities hit by missiles," Deutsche Welle, November 11, 2022, Accessed December 17, 2022, https://www.dw.com/en/ukraine-updates-kyiv-other-cities-hit-by-missiles/a-63760677.; "Russia Fires 'Massive' Missile Barrage at Ukraine Grid," The Defense Post, December 16, 2022, Accessed December 17, 2022, https://www.thedefensepost.com/2022/12/16/russia-fires-missile-barrage-ukraine/.
[134] Josh Pennington, Julia Kesaieva, Tim Lister, and Mariya Knight," Ukraine launches missile attack on Russian-occupied Melitopol, explosions reported in Donetsk and Crimea," CNN; December 11, 2022, Accessed December 17, 2022, https://edition.cnn.com/2022/12/11/europe/ukraine-crimea-melitopol-odesa-intl-hnk/index.html.
[135] Stefan Ellerbeck, "Russia's invasion of Ukraine: 1-year timeline," World Economic Forum, February 23, 2023, Accessed March 9, 2023, https://www.weforum.org/agenda/2023/02/ukraine-war-timeline-one-year/.
[136] "Ukraine," CIA Factbook, Accessed December 14, 2022, https://www.cia.gov/the-world-factbook/countries/ukraine/#people-and-society.
[137] Ibid.
[138] "Estimated direct losses from damages to physical infrastructure from the Russian invasion in Ukraine as of September 2022, by type," Statista, December 12, 2022, Accessed December 17, 2022, https://www.statista.com/statistics/1303344/ukraine-infrastructure-war-damage/.
[139] Jakub Przetacznik and Simona Tarpova," Russia's war on Ukraine: Timeline of cyber-attacks," June 2022, European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf, 1-3.
[140] Ibid.
[141] See details on those attacks in section: Offensive cyber operations types and effects.
[142] See details on those attacks in section: Offensive cyber operations types and effects.
[143] Catalin Cimpanu, "Ukraine reports cyber-attack on government document management system," ZDNet, February 24, 2021, Accessed February 17, 2023, https://www.zdnet.com/article/ukraine-reports-cyber-attack-on-government-document-management-system/.
[144] Catalin Cimpanu, "Hackers deface Ukrainian government websites," January 14, 2022, Accessed February 17, 2023, https://therecord.media/hackers-deface-ukrainian-government-websites/.

[145] Jakub Przetacznik and Simona Tarpova, "Russia's war on Ukraine: Timeline of cyber-attacks," June 2022, European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf, 2.
[146] Ibid.
[147] Lauren Feiner, "Cyberattack hits Ukrainian banks and government websites," CNBC, February 23, 2022, Accessed February 17, 2023, https://www.cnbc.com/2022/02/23/cyberattack-hits-ukrainian-banks-and-government-websites.html.
[148] Jakub Przetacznik and Simona Tarpova, "Russia's war on Ukraine: Timeline of cyber-attacks," June 2022, European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf, 2.
[149] Sergiu Gatlan, "ViaSat shares details on KA-SAT satellite service cyberattack," Bleeping Computer, March 30, 2022, Accessed February 17, 2022, https://www.bleepingcomputer.com/news/security/ViaSat-shares-details-on-ka-sat-satellite-service-cyberattack/.
[150] Jakub Przetacznik and Simona Tarpova, "Russia's war on Ukraine: Timeline of cyber-attacks," June 2022, European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf, 3
[151] Chris Vallance, "Ukraine war: Major Internet provider suffers cyber-attack," BBC, March 28, 2022, Accessed February 17, 2023, https://www.bbc.com/news/60854881.
[152] Jakub Przetacznik and Simona Tarpova, "Russia's war on Ukraine: Timeline of cyber-attacks," June 2022, European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf, 2.
[153] James Pearson, "Ukraine says it thwarted Russian cyberattack on electricity grid," Reuters, April 12, 2022, Accessed February 18, 2023, https://www.reuters.com/world/europe/russian-hackers-tried-sabotage-ukrainian-power-grid-officials-researchers-2022-04-12/.
[154] "Russian hackers coordinated latest missile strikes on Odesa," Ukrinform, Accessed February 18, 2023, https://www.ukrinform.net/rubric-ato/3477610-russian-hackers-coordinated-latest-missile-strikes-on-odesa.html.
[155] "Quarterly Analysis Report Q3 July to September 2022: Cyber Dimensions of the Armed Conflict in Ukraine," CyberPeace Institute, December 16, 2022, Accessed February 18, 2023, https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q3%20Report.pdf, 4.
[156] "Cyber Dimensions of the Armed Conflict in Ukraine," CyberPeace Institute, February 1, 2023, Accessed February 18, 2023, https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q4%20Report.pdf, 4.
[157] Ravie Lakshmanan, "Ukraine Hit with New Golang-based 'SwiftSlicer' Wiper Malware in Latest Cyber Attack," The Hacker News, January 28, 2023, Accessed February 18, 2023, https://thehackernews.com/2023/01/ukraine-hit-with-new-golang-based.html.; Carly Page, "Russian 'WhisperGate' hackers are using new data-stealing malware to target Ukraine," February 8, 2023, Accessed February 18, 2023, https://techcrunch.com/2023/02/08/whispergate-hackers-data-stealing-malware-ukraine/.
[158] See sections: 2.2. Offensive cyber operation types and effects and 2.4 Logic of integration of offensive cyber operations into the military structures.
[159] "Cambridge Dictionary", https://dictionary.cambridge.org/dictionary/english/.
[160] "Critical Infrastructure Sectors," CISA, Accessed February 25, 2023, https://www.cisa.gov/critical-infrastructure-sectors.
[161] "An introduction to the cyber threat environment," Canadian Centre for Cyber Security, Accessed March 10, 2023, https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment.
[162] Oliver Darcy, "'We want to get the news out': How Ukraine's journalists are covering the invasion of their country," CNN, February 25, 2022, Accessed February 18, 2023, https://edition.cnn.com/2022/02/25/media/kyiv-post-ukraine-journalists/index.html.
[163] Kyiv Post, Twitter, February 24, 2022, Accessed February 18, 2023, https://twitter.com/KyivPost/status/1496775905192161280?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1496775905192161280%7Ctwgr%5E%7Ctwcon%5Es1_c10&ref_url=https%3A%2F%2Fwww.news18.com%2Fnews%2Ftech%2Fukrainian-publication-kyiv-post-says-website-hacked-amid-russian-cyberattacks-heres-whats-happening-4809248.html.
[164] "February 24, 2022 Russia-Ukraine news," CNN, February 24, 2022, February 18, 2023, https://edition.cnn.com/europe/live-news/ukraine-russia-news-02-24-22-intl/index.html.
[165] "Ukraine: Timeline of Cyberattacks," CyberPeace Institute, June 8, 2022, Accessed January 22, 2022, https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks; Natalia Zinets and Aleksandar Vasovic, "Missiles rain down around Ukraine," Reuters, February 25, 2022, Accessed January 22, 2023, https://www.reuters.com/world/europe/putin-orders-military-operations-ukraine-demands-kyiv-forces-surrender-2022-02-24/.
[166] Jonathan Greig, "ViaSat confirms report of wiper malware used in Ukraine cyberattack," Recorded Future, April 1, 2022, Accessed January 22, 2023, https://therecord.media/ViaSat-confirms-report-of-wiper-malware-used-in-ukraine-cyberattack/.
[167] "Cyber Operations," Council of Foreign Relations, https://www.cfr.org/cyber-operations/.

[168] "CyberPeace Institute, " https://cyberpeaceinstitute.org/.
[169] "CERT-UA, " https://cert.gov.ua/articles.
[170] "CERT-UA has processed over 2,000 cyberattacks against Ukraine year to date," State Service of special communication and information protection of Ukraine, December 30, 2022, Accessed January 17, 2023, https://cip.gov.ua/en/news/cert-ua-vid-pochatku-roku-opracyuvala-bilshe-dvokh-tisyach-kiberatak-na-ukrayinu.
[171] Lennart Maschmeyer, Ronald J. Deibert and Jon R. Lindsay, "A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society," Journal of Information Technology & Politics, 2020, 18:1, 1-20, https://www.tandfonline.com/doi/full/10.1080/19331681.2020.1776658, 1, 13, 16.
[172] Max Smeets, "No Shortcuts - Why States Struggle To Develop a Military Cyber-Force," Hurst, 2022, 32.
[173] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, "Cyber Persistence Theory - Redefining National Security in Cyberspace," Oxford University Press, 2022, 114.
[174] Ibid.
[175] Max Smeets, "No Shortcuts - Why States Struggle To Develop a Military Cyber-Force," Hurst, 2022, 52-55.
[176] Tim Lister, "Here's what we know about how Russia's invasion of Ukraine unfolded," CNN, February 24, 2022, Accessed February 24, 2023, https://edition.cnn.com/2022/02/24/europe/ukraine-russia-attack-timeline-intl/index.html.
[177] Adam Stone, "How Leon Panetta's 'Cyber Pearl Harbor' warning shaped Cyber Command," C4ISRNET, July 30, 2019, Accessed February 1, 2023, https://www.c4isrnet.com/opinion/2019/07/30/how-leon-panettas-cyber-pearl-harbor-warning-shaped-cyber-command/.
[178] Nathan Gardels, "Mike McConnell: An American Spymaster on Cyberwar," Huff Post, August 8, 2009, Accessed 1 February 2022, https://www.huffpost.com/entry/mike-mcconnell-an-america_b_227944.
[179] Thomas Rid, "Cyber War Will Not Take Place," Oxford University Press, 2013, The Argument xiv-xv, 37, 42-43.
[180] Eric Gratzke, "The Myth of Cyberwar," MIT Press, International Security, Volume 38, Number 2, Fall 2013, pp. 41-73 (Article), 43, 49, 57-58, 72.
[181] Max Smeets, "No Shortcuts - Why States Struggle To Develop a Military Cyber-Force," Hurst, 2022, 6-8.
[182] Florian J. Egloff and James Shires, "Offensive Cyber Capabilities and State Violence: Three Logics of Integration," Journal of Global Security Studies, Volume 7, Issue 1, March 2022, https://doi.org/10.1093/jogss/ogab028, 7.; Thomas Rid, "Cyber War Will Not Take Place," Oxford University Press, 2013, The Argument xiv-xv, 37, 42-43.
[183] See Chapter 3, 3.2 The 2022 War in Ukraine for chronological overview of military activities.
[184] John Psaropoulos, "Timeline: Six months of Russia's war in Ukraine," Al Jazeera, August 22, 2022, March 5, 2023, https://www.aljazeera.com/news/2022/8/24/timeline-six-months-of-russias-war-in-ukraine.
[185] Ibid.
[186] Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," Carnegie Endowment for International Peace, December 16, 2022, https://carnegieendowment.org/files/Bateman_Cyber-FINAL21.pdf, p 2-3.
[187] "Ghostwriter / UNC1151 Adopts Microbackdoor Variants in Cyber Operations Against Ukraine," Cluster25 Threat Intel Team, March 8, 2022, Accessed March 6, 2023, https://blog.cluster25.duskrise.com/2022/03/08/ghostwriter-unc1151-adopts-microbackdoor-variants-in-cyber-operations-against-targets-in-ukraine.; Ravie Lakshmanan, "Ukrainian CERT Warns Citizens of Phishing Attacks Using Compromised Accounts," March 7, 2022, Accessed March 6, 2023, https://thehackernews.com/2022/03/ukrainian-cert-warns-citizens-of.html?&web_view=true.; Shane Huntley, "An update on the threat landscape," March 7, 2022, Accessed March 6, 2023, https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/.
[188] Nadiya Kostyuk and Eric Gartzke, "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine," Texas National Security Review, Vol 5, Iss 3, Summer 2022, 112-126, https://tnsr.org/2022/06/why-cyber-dogs-have-yet-to-bark-loudly-in-russias-invasion-of-ukraine/#_ftn13.
[189] Marcus Willett, "The Cyber Dimension of the Russia–Ukraine War," Xcina Consulting, October 2022, Accessed March 6, 2023, https://xcinaconsulting.com/blog/the-cyber-dimension-of-the-russia-ukraine-war/.
[190] Ibid.
[191] "Lessons from Russia's cyber-war in Ukraine," The Economist, November 30, 2022, Accessed March 6, 2023, https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russias-cyber-war-in-ukraine.
[192] "Ukrainian IT Army," Council on Foreign Relations, Accessed March 11, 2023, https://www.cfr.org/cyber-operations/ukrainian-it-army.
[193] "IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine," ESET Research, March 1, 2022, Accessed February 22, 2023, https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/.
[194] DLL represents a shared library in Microsoft Windows operating systems, in which code can be used by more than one program at a time. See "What is a DLL," Microsoft, December 4, 2022, Accessed February 24, 2023, https://learn.microsoft.com/en-us/troubleshoot/windows-client/deployment/dynamic-link-library.; Ryan Estes, "A Technical Analysis of IsaacWiper," Secplicity, February 10, 2023, Accessed February 24, 2023, https://www.secplicity.org/2023/02/10/a-technical-analysis-of-isaacwiper/.
[195] "An overview of Russia's cyberattack activity in Ukraine ," Microsoft, Accessed February 24, 2023, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd, 3.

[196] Tim Lister, "Here's what we know about how Russia's invasion of Ukraine unfolded," CNN, February 24, 2022, Accessed February 24, 2023, https://edition.cnn.com/2022/02/24/europe/ukraine-russia-attack-timeline-intl/index.html.
[197] "Russian forces launch full-scale invasion of Ukraine," Al Jazeera, February 24, 2022, Accessed February 24, 2023, https://www.aljazeera.com/news/2022/2/24/putin-orders-military-operations-in-eastern-ukraine-as-un-meets.; "Ukraine fighting to stop 'a new iron curtain' after the Russian invasion," The Guardian, February 24, 2022, Accessed February 24, 2023, https://www.theguardian.com/world/2022/feb/24/russia-attacks-ukraine-news-vladimir-putin-zelenskiy-russian-invasion.
[198] Thomas Brewster, "As Russia Invaded, Hackers Broke Into A Ukrainian Internet Provider. Then Did It Again As Bombs Rained Down," Forbes, March 10, 2022, Accessed February 24, 2023, https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/.; Daryna Antonyuk, "On the day of the invasion, hackers disabled a satellite that distributes the Internet in Europe and Ukraine. Now they found a Russian trace in the attack," Forbes Ukraine, April 4, 2022, Accessed February 25, 2023, https://forbes.ua/ru/innovations/u-den-vtorgnennya-khakeri-viveli-z-ladu-suputnik-shcho-rozdae-internet-u-evropi-ta-ukraini-teper-v-atatsi-znayshli-rosiyskiy-slid-04042022-5275.
[199] "Internet disruptions registered as Russia moves in on Ukraine," NetBlocks, February 24, 2022, Accessed February 23, 2023, https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K.
[200] "Internet problems: Triolan reports connection failures in Kharkiv and Kyiv," Focus, February 24, 2022, Accessed February 24, 2023, https://focus.ua/uk/digital/507700-problemy-s-internetom-triolan-soobshchaet-o-sboyah-soedineniya-v-harkove-i-kieve.
[201] Thomas Brewster, "Bombs and hackers do not give life to Ukrainian Internet providers. How "invisible heroes" risk their lives to keep Ukraine online," Forbes Ukraine, March 17, 2022, Accessed February 25, 2023, https://forbes.ua/ru/company/bombi-i-khakeri-ne-dayut-zhittya-ukrainskim-internet-provayderam-nevidimi-geroi-rizikuyut-svoim-zhittyam-shchob-ikhnya-kraina-i-dali-bula-onlayn-16032022-4714.
[202] Nicolò Boschetti, Nathaniel Gordon, Gregory Falco, "Space Cybersecurity Lessons Learned from The ViaSat Cyberattack," 2022, https://www.researchgate.net/publication/363558808_Space_Cybersecurity_Lessons_Learned_from_The_ViaSat_Cyberattack/link/632285a770cc936cd30bbf07/download, 3.
[203] Ibid.
[204] Matt Burgess, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine," Wired, March 23, 2022, Accessed February 24, 2023, https://www.wired.co.uk/article/viasat-internet-hack-ukraine-russia.
[205] Ibid.
[206] Raphael Satter, "Satellite outage caused 'huge loss in communications' at war's outset -Ukrainian official," Reuters, March 15, 2022, Accessed February 24, 2023, https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/.
[207] Kim Zetter, "Viasat Hack "Did Not" Have Huge Impact on Ukrainian Military Communications, Official Says," Zero Day, September 14, 2022, Accessed February 24, 2023, https://zetter.substack.com/p/viasat-hack-did-not-have-huge-impact.
[208] Carly Page, "US, UK and EU blame Russia for 'unacceptable' Viasat cyberattack," Techcrunch, May 10, 2022, Accessed February 24, 2023, https://techcrunch.com/2022/05/10/russia-viasat-cyberattack/.
[209] "February 24, 2022 Russia-Ukraine news," CNN, February 25, 2022, Accessed February 27, 2023, https://edition.cnn.com/europe/live-news/ukraine-russia-news-02-24-22-intl/index.html.
[210] Mark Maunder, "Ukraine Universities Hacked As Russian Invasion Started," Wordfence, March 1, 2022, Accessed February 24, 2023, https://www.wordfence.com/blog/2022/03/ukraine-universities-hacked-by-brazilian-via-finland-as-russian-invasion-started/.
[211] Ibid.
[212] Mason Clark, George Barros, and Kateryna Stepanenko, "Russia-Ukraine Warning Update, February 25 2022," Institute for the War Studies," February 25, 2022, Accessed March 1, 2023, https://www.understandingwar.org/backgrounder/russia-ukraine-warning-update-russian-offensive-campaign-assessment-february-25-2022.
[213] Kyle Alspach, "Ukraine border control hit with wiper cyberattack, slowing refugee crossing," VentureBeat, February 27, 2022, Accessed February 24, 2023, https://venturebeat.com/security/ukraine-border-control-hit-with-wiper-cyberattack-slowing-refugee-crossing/.
[214] "February 26, 2022 Russia-Ukraine news," CNN, March 6, 2022, Accessed February 27, 2023, https://edition.cnn.com/europe/live-news/ukraine-russia-news-02-26-22-intl/index.html.
[215] ""Zhadnost" Botnet DDoS Attacks," CyberPeace Institute, February 28, 2022, Accessed February 24, 2023, https://cyberpeaceinstitute.org/cyberattacks/zhadnost-botnet-ddos-attacks/.
[216] Ryan Slaney, "Zhadnost 'stamps' out Ukrainian National Postal Service's website," Security Scorecard, April 29, 2022, Accessed February 24, 2023, https://securityscorecard.com/blog/zhadnost-stamps-out-ukrainian-national-postal-services-website/.
[217] DNS is a service which provides name resolution between hostnames and IP addresses. "The Continuing Denial of Service Threat Posed by DNS Recursion (v2.0)," US-CERT, Accessed February 24, 2023, https://www.cisa.gov/sites/default/files/publications/DNS-recursion033006.pdf.

[218] "DNS amplification attack," Cloudflare, Accessed February 24, 2023, https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/.
[219] Ryan Slaney, "Zhadnost 'stamps' out Ukrainian National Postal Service's website," Security Scorecard, April 29, 2022, Accessed February 24, 2023, https://securityscorecard.com/blog/zhadnost-stamps-out-ukrainian-national-postal-services-website/.
[219] "February 28, 2022, Russia-Ukraine news," CNN, March 1, 2022, Accessed February 27, 2023, https://edition.cnn.com/europe/live-news/ukraine-russia-news-02-28-22-intl/index.html.
[220] "February 28, 2022, Russia-Ukraine news," CNN, March 1, 2022, Accessed February 27, 2023, https://edition.cnn.com/europe/live-news/ukraine-russia-news-02-28-22-intl/index.html.
[221] "An overview of Russia's cyberattack activity in Ukraine," Microsoft, Accessed February 24, 2023, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.
[222] "Cyber threat activity in Ukraine: analysis and resources," Microsoft, February 28, 2022, Accessed February 24, 2023, https://msrc.microsoft.com/blog/2022/02/analysis-resources-cyber-threat-activity-ukraine/.
[223] Katya Soldak, "Tuesday, March 1. Russia's War On Ukraine: News And Information From Ukraine," March 1, 2022, Accessed February 28, 2023, https://www.forbes.com/sites/katyasoldak/2022/03/01/tuesday-march-1-russias-war-on-ukraine-news-and-information-from-ukraine/.
[224] "Russian Defense Ministry warns about strikes being prepared on military sites in Kiev," Tass, March 1 2022, Accessed March 1, 2023, https://web.archive.org/web/20220301133913/https://tass.com/defense/1414199.
[225] "DanaBot malware leveraged in DDoS attack targeted at the Ukrainian Ministry of Defense," Broadcom, March 4, 2022, Accessed February 24, 2023, https://www.broadcom.com/support/security-center/protection-bulletin#blt9ce9c846352bf024_en-us.
[226] "March 4, 2022 Russia-Ukraine news," CNN, March 5, 2022, Accessed March 1, 2023, https://edition.cnn.com/europe/live-news/ukraine-russia-putin-news-03-04-22/index.html.
[227] Thomas Brewster, "As Russia Invaded, Hackers Broke Into A Ukrainian Internet Provider. Then Did It Again As Bombs Rained Down," Forbes, March 10, 2022, Accessed February 24, 2023, https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/.; Daryna Antonyuk, "On the day of the invasion, hackers disabled a satellite that distributes the Internet in Europe and Ukraine. Now they found a Russian trace in the attack," Forbes Ukraine, April 4, 2022, Accessed February 25, 2023, https://forbes.ua/ru/innovations/u-den-vtorgnennya-khakeri-viveli-z-ladu-suputnik-shcho-rozdae-internet-u-evropi-ta-ukraini-teper-v-atatsi-znayshli-rosiyskiy-slid-04042022-5275.
[228] Thomas Brewster, "As Russia Invaded, Hackers Broke Into A Ukrainian Internet Provider. Then Did It Again As Bombs Rained Down," Forbes, March 10, 2022, Accessed February 24, 2023, https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/.
[229] Sebastian Moss, "Ukraine's Ukrtelecom goes down nationwide for 40m, ISP Triolan outage caused by cyber attack," Datacenter Dynamics, March 10, 2022, Accessed February 25, 2023, https://www.datacenterdynamics.com/en/news/ukraine-ukrtelecom-goes-down-nationwide-for-40m-isp-triolan-outage-caused-cyber-attack/.
[230] "March 9, 2022 Russia-Ukraine news," CNN, March 10, 2022, Accessed March 1, 2023, https://edition.cnn.com/europe/live-news/ukraine-russia-putin-news-03-09-22/index.html.
[231] Ruslan Trad, "Russia-Ukraine war military dispatch: March 9, 2022," Al Jazeera, March 9, 2022, Accessed March 1, 2023, https://www.aljazeera.com/news/2022/3/9/russia-ukraine-war-military-dispatch-march-9-2022.
[232] "CaddyWiper" Tweet, ESET Research, March 14, 2022, Accessed February 25, 2023, https://twitter.com/ESETresearch/status/1503436423818534915.
[233] Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK, 6.
[234] "March 14, 2022 Russia-Ukraine news," CNN, March 5, 2022, Accessed March 1, 2023, https://edition.cnn.com/europe/live-news/ukraine-russia-putin-news-03-14-22/index.html.
[235] Alden Wahlstorm at al., "The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine," Mandiant, May 19, 2022, Accessed February 25, 2023, https://www.mandiant.com/resources/blog/information-operations-surrounding-ukraine.
[236] "March 16, 2022, Russia-Ukraine news," CNN, March 17, 2022, Accessed March 4, 2023, https://edition.cnn.com/europe/live-news/ukraine-russia-putin-news-03-16-22/index.html.
[237] "The SBU reported a massive hacker attack on the websites of popular online publications in Ukraine," Slovo i Dilo, March 17, 2022, Accessed February 25, 2023, https://www.slovoidilo.ua/2022/03/17/novyna/suspilstvo/sbu-povidomyla-pro-masovu-xakersku-ataku-sajty-populyarnyx-onlajn-vydan-ukrayini.
[238] "March 16, 2022 Russia-Ukraine news," CNN, March 16, 2022, Accessed March 1, 2023, https://edition.cnn.com/europe/live-news/ukraine-russia-putin-news-03-16-22/index.html.
[239] "Cyber-attack on Ukrainian enterprises using the DoubleZero destructor program (CERT-UA#4243)", CERT-UA, March 22, 2022, Accessed February 25, 2023, https://cert.gov.ua/article/38088.
[240] "What Is the Windows Registry and How Does It Work?", Avast, Accessed February 25, 2023, https://www.avast.com/c-windows-registryhttps://www.avast.com/c-windows-registry.

[241] "An overview of Russia's cyberattack activity in Ukraine," Microsoft, Accessed February 25, 2023, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd, 3.
[242] "March 22, 2022 Russia-Ukraine news," CNN, March 22, 2022, Accessed March 1, 2023, https://edition.cnn.com/europe/live-news/ukraine-russia-putin-news-03-22-22/index.html.