Cyber Operations in Ukraine: Emerging Patterns in Cases

Markus Takamaa and Martti Lehto
University of Jyväskylä, Finland

markus.k.t.takamaa@jyu.fi
martti.j.lehto@jyu.fi

Abstract: The Ukrainian state has been a target of cyber-related incidents since the annexation of Crimea in 2014. Cyberattacks have targeted Ukrainian critical infrastructure, government offices, and several public and private organisations. Sometimes, these cyberattacks have caused significant impacts within the nation's borders. Some of the most well-known cyber-incidents in Ukraine include attacks on the Ukrainian electrical grid, which cut out the power supply for hundreds of thousands of people in 2015 and 2016. Attacks have also targeted presidential election systems and financial entities operating in Ukraine. The majority of attacks within Ukraine's borders have been attributed to Russian-affiliated non-state actors and organisations, and the number of attacks correlates with the escalation of the war in 2022. This implies previous cyberattacks potentially belonging to a series of hybrid operations related to the Ukrainian conflict and the general geopolitical situation since the annexation of Crimea. The paper focuses on this context by examining cyber incidents targeting Ukraine since 2014. We study the unifying factors related to Ukrainian cyber incidents, and we will discuss emerging patterns related to the attacks during the last ten years. This study will uncover the general traits of state-affiliated attacks in Ukraine, which will help uncover emerging patterns. Our particular focus will be cyber-attacks, where the target is the Ukrainian state and its critical infrastructure. We will examine methods of attacks, the attack targets, and the impacts, among other things. With the patterns emerging from our study, we can predict future cyber-attacks targeting Ukraine, providing tools for preparing for future incidents. We can use the information to improve national cyber-defences, where the attacks are likely to happen in the future. Studying the Ukrainian cases may also provide additional insights for improving cyber defences in other nation-states within the parts that apply to these nation-states and their geopolitical contexts.

Keywords: Cyber Warfare, Cyber-Attack, Cyber Incident, Ukrainian Conflict, Digital Warfare

1. Introduction

Numerous cyber-attacks have hit Ukraine since the start of the current conflict. During the last ten years, attacks in Ukraine have targeted the electricity grid, electoral systems, and army organisations, to name a few. Cyber-attacks have been used numerous times throughout the years and have affected Ukrainian organisations in various ways and effects. It is also likely the attacks will continue striking the nation in the future as the conflict continues within different parts of Ukraine.

The goal of this paper is to examine these previous cyber-attacks in Ukraine during the last ten years. We discuss the cases starting from the annexation of Crimea and proceed to study the attacks throughout the current conflict. We aim to explore the methods used and determine the general patterns the most notable attacks follow. The goal is to discover the general nature of the attacks to understand how cyber operations are used as a part of warfare during the conflict. By doing this, we hope to provide information for assessing the general methods by which these cyberattacks may also occur in the future. We also aim to highlight the cases that harness the most attention within the publicly available sources and focus on patterns discovered from these cases.

In this paper, we first examine general aspects related to cyber-operations and discuss their use as part of general warfare. After this, we examine the overall situation in Ukraine and the cases of cyberattacks occurring throughout the years. We further explore the details of these attacks and attempt to make new conclusions based on the results discovered. We further evaluate the results and assess the meaning of the potential discoveries emerging from the cases. Based on the results, we come to our conclusions regarding the long-term situation in Ukraine and bring awareness to how cyberattacks are used as a part of inter-state conflicts.

2. Background

In this chapter, we will first examine cyber operations and their general use within Ukraine based on previously harnessed information.

Cyber operations are actions in or through cyberspace aiming to create effects on the target's actions (Laari, 2019). They can come in various forms and have different goals based on their actor's and target's relationship. Generally, Cyber operations can be divided into offensive and defensive operations based on the objectives.

Offensive cyber operations are cyberattacks used to project power by applying force through cyberspace and are generally aggressive in their nature. Defensive ones, in turn, aim to protect one's cyber-physical environment and can be both passive and active in their actions (Theohary, 2021). The active ones consist of direct defensive actions taken to reduce or nullify the effectiveness of cyber threats, and the passive ones focus more on protecting one's own cyber infrastructure from possible threats (Turunen & Kari, 2020). From offensive and defensive cyber operations, this paper examines the nature of offensive ones, focusing on attacks targeting Ukraine.

Cyber operations may be used with various tools and purposes. For example, they can act as a method for conducting the actions of warfare. In this context, their use as part of military operations may be called cyber warfare. Cyber warfare is a broad term and may refer to several nation-state actions aiming to achieve objectives in or through cyberspace (Goel, 2020).

Cyber warfare can be defined as the use of armed attacks in or through cyberspace to impose a nation-state's political will onto another nation-state (Applegate, 2015). These involve non-kinetic attacks on information data and its collection process aimed at damaging, disrupting or destroying the target's decision-making processes or normal operations. Cyber warfare encompasses using all the digital tools available to paralyse or destroy the other party's ICT-technology-based systems while keeping one's systems operational. (Lehto & Henselmann, 2020). Often, cyber warfare has been categorised as part of hybrid warfare, which refers to using all non-kinetic forms of combat alongside the traditional forms of warfare. These other forms of hybrid warfare can also include, for example, information operations and energy blockades alongside cyber-attacks (Boyte, 2017).

Cyber warfare has been used extensively as part of the ongoing conflict in Ukraine, and they show how cyber-attacks can be used to conduct inter-state conflicts. Some commonly known cases include cyberattacks targeting Ukrainian electrical infrastructure in 2015 and 2016, each paralysing the electrical distribution within different parts of Ukraine (Kostyk & Zhukov, 2019). Cyberattacks targeting Ukraine also intensified during the escalation of the conflict in 2022, when the number of foreign troops increased significantly within the country. Since then, online activities towards Ukraine have been aimed at destroying, disrupting or infiltrating the various governmental bodies and critical infrastructure organisations (Microsoft, 2022).

Between January 2022 and September 2023, the CyberPeace Institute documented a total of 174 incidents against different entities in Ukraine. In this timeframe, their study indicated that DDoS attacks consisted of almost 71,3% of the observed attacks. The public administration was also seen as the most targeted sector between July and September 2022 (Cyber Peace Institute, 2023a). In the analysis made by CSIS (Centre for Strategic & International Studies) in 2022, almost 60 percent of the targets of the cyber-attacks were private non-state actors, just over 30 percent were government nonmilitary actors, and just over 10 percent were government military actors (Mueller et al., 2023).

The operations of 2022 in Ukraine correspond to the principles of the Russian so-called Gerasimov doctrine[1], according to which:

- Reduction of the state's military-economic potential by destroying critically important facilities of their military and civilian infrastructure in a short time.
- Warfare simultaneously in all physical environments and the information space.
- The use of asymmetric and indirect operations.
- Command-and-control of forces and assets in a unified information space.

In exchange for the Western concept of hybrid warfare, Russia has developed its own concept: New Generation Warfare (Russian. Война нового поколения). As part of the doctrine, continuous cyber operations are conducted below the threshold of war beyond the reach of attribution. (Kari, 2019, 54)

Russian doctrines include the concept of information warfare, which consists of two elements:

1. Information Technology-based – The target is critical infrastructure.

[1] Gerasimov Doctrine based on General Valery Gerasimov's annual speech and presentation at the Russian Military Academy of Science in March 2013 and interpretations of some Russian analysts.

2. Information Psychology-based – The target in the human mind, the moral and mental world of man, socio-political and psychological orientation, or decision-maker's ability to make decisions.

From a Western point of view, Russia has combined cyber operations and information operations into a single entity, where the goal of the information war is:

- Generating losses on information systems, processes, resources, and critical or other structures.
- Paralysis of political, economic, and social systems.
- Massive psychological surgery to unbalance society and the state.

(Kari, 2016)

As we can notice from the previous information, most of the recent discussion of the situation in Ukraine has focused on the events during and after the escalation of the conflict in 2022, leaving the previous events with less attention. Therefore, to understand the situation regarding the overall progression of the conflict, there is a need to examine and bring awareness of the long-term patterns since the annexation of the Crimean Peninsula by Russia. This study aims to focus on this timeframe in Ukraine since 2014.

However, it should be noted that attributing the cyber-attacks to any nation-state actors has often been challenging in the past. This is due to the natural anonymity as a core part of the internet, which enables state actors to perform their online actions often unnoticed (Goel, 2020). Proper attribution of cyber-attacks is considered to be important in justifying countermeasures against the correct nation-state perpetrator of the attacks (Goel, 2020). Still though, the international law regarding the attribution of cyberattacks has remained undefined for the moment (Banks, 2021). However, the technical tools for attribution have improved in recent years, making states declare the potential actors behind the attack more often (Goel, 2020; Banks, 2021).

3. Research and Methods

Next, we will further examine the use of cyber operations during the current Ukrainian conflict. In our examination, we will attempt to find answers to the following questions:

Q1: Can we uncover patterns from cyber incidents targeting Ukraine since 2014?

Q2; If patterns are uncovered, what kind of patterns are these?

We examine the notable cases during the last ten years in Ukraine, of which we can collect information from public sources. These sources can be journal articles, reports, and other publications for example. We collect information from these sources and examine the details of the previous incidents. We use comparison on the collected information on the cases and examine the potential emerging patterns and trends from the incidents overall. In our study, we especially focus on incidents that have affected normal operations within the Ukrainian state. We collect information from the cases' details, such as the attack methods, the targets, and the overall impacts of the events. Based on the discovered data, we will also subjectively evaluate these incidents' potential goals and objectives.

The cases selected for our study examination are based on the availability of the information. We will start conducting the study by searching for mentions of previous cyberattacks in Ukraine and attempt to find more details by examining more data on each case from the public sources available. We then insert the gathered information on the cases in a table, which helps examine the overall patterns of the observed cases. If only limited information is available on the case, we will leave these unexamined within our study. By collecting all this data, our qualitative study aims to provide the first glimpse into the nature of cyber-attacks in Ukraine in the last ten years. By this, we hope to provide new information on the trends and patterns emerging in these cases.

Due to the issues caused by the attribution problem for evaluating the culprit of these attacks from public sources, we will leave the most likely actors of the incidents unexamined within the scope of our study. It should be noted that within the West, Russia and Russian state-affiliated groups have often been said to have performed previous attacks, especially the cases regarding Ukraine. Also, we will leave espionage and influence operations unexamined within the Ukrainian cyber environment in our study and focus on other cyber incidents affecting normal operations within Ukraine. Further, since the study is based on publicly available sources, those potential cases yet to be brought to public attention are unincluded within the study data.

Our objective in studying previous cyber-attacks is to examine the long-term threats targeting Ukraine in or through cyberspace. By this study, we hope to discover the long-term trends in the nation-state level. The discoveries may be used to forecast the potential attack mechanisms and targets in the future, which can be used to harden the protection of the potential targets' cyber environment before any possible offensive cyber operations occur. The discovered data could be used to pre-emptively improve the security of the it-systems in other nation-states, considering the parts of their practical and geopolitical contexts where they are similar or equal regarding Ukraine now or in the future. In addition, we aim to highlight the cases which are brought to attention in the publicly available sources and have the most visibility within them.

Next, we will examine the cases in detail and evaluate the data available from public sources.

4. Cases Examined in the Study

The following table shows the most important and well-known cyberattacks on Ukraine, which also have publicly available information.

Table 1:

Event	Date	Attack method	Target	Impact	Potential objectives
DDoS attack before the referendum on the status of Crimea (Przetacznik & Tarpova, 2022; Weedon, 2018)	March, 2014	DDoS	Official government and media websites	Sites unavailable for up to multiple hours	Disruption of online services
An attempt to delete the results of the presidential election of 2014 (Weedon, 2015)	May, 2014	Malware	Ukraine's Central Election Commission	Impacts prevented by Ukraine's Security Service (SBU)	Election interference
DDoS attack on Election counting systems (Clayton, 2014)	May, 2014	DDoS	Ukraine's election counting systems	Election counting blocked for 2 hours, delaying the final results of the vote	Election interference
BlackEnergy (Izycki & Vianna, 2021)	December, 2015	Trojan	Ukrainian electricity distribution network	Disruption of energy services for hundreds of thousands of people for 1-6 hours	Disruption of energy services
2016 attack on the Ukrainian power grid (Simons, Danyk & Maliarchuk, 2020)	December, 2016	Malware	Ukrenergo's (Ukraine's national grid operator) network	Disruption of energy services around Kyiv for around an hour	Disruption of energy services
NotPetya (Izycki & Vianna, 2021)	June, 2017	Wiper -attack disguised as ransomware	Various critical infrastructure organizations and companies	destruction of data of close to 10 percent of computers in Ukraine and impacts on various companies globally	Destruction of computers, disruption of normal operations
WhisperGate -attack (Microsoft Digital Security Unit, 2022; Dutta, 2022)	January, 2022	Wiper attack disguised as ransomware	Ukrainian government and IT organizations	destruction of computers	Destruction of data and disabling of normal operations
Attack on the KA-SAT-satellite network (Przetacznik & Tarpova, 2022; Cyber Peace Institute, 2022)	February, 2022	Wiper attack	modems used to communicate with the KA-SAT-satellite network	Communication outages for several thousand people up to two weeks	Disruption of communication services

Event	Date	Attack method	Target	Impact	Potential objectives
DDoS attacks on government websites and Ukrainian bank systems (Regional Cyber Defence Centre, 2023)	February, 2022	DDoS	Web resources of Ukrainian banks and state institutions	Disruption of the availability of web services	Disruption of services
HermeticWiper -attack (Grossman et al., 2023; Lehto, 2022)	February, 2022	Wiper-attack	300 systems, such as dozens of financial, government, energy, information technology, and agricultural organizations	destruction of computers	Destruction of data, disruption of normal operations
Attack on Ukrainian state organization (Cyber Peace Institute, 2023b)	April, 2023	Wiper and BASH script attack	Ukrainian state organisations	Destruction and disabling of computers	Destruction of data and disabling of normal operations
Wiper attack on Ukraine's largest telecom operator, Kyivstar (Antoniuk, 2023; Antoniuk, 2024)	December, 2023	wiper-attack	Telecommunications in Ukraine	Disruption of telecommunication services for days	Disruption of telecommunication services

5. Results

The examination of the cases suggests that the cases available from public sources follow general patterns in Ukraine. In these cases, the most common attack tools have been various forms of malware and DDoS attacks. From the malware types, wiper attacks are most mentioned in the cases. These are malware, whose primary purpose is to wipe out the contents of the infected computer's hard drive, which disables the ability to turn on the computer, making it inoperable. Based on these cases, the goal of the considerable number of examined cases has been to make the infected systems inoperable, thus disrupting the daily operations dependent on these systems. Some cases also seem to have aimed to temporarily slow down the normal operations in Ukraine by using DDoS as a method of attack.

In addition, most target organisations can be considered part of the critical infrastructure in Ukraine, while governmental organisations have also been targeted in some cases. The number of cyber-attacks targeting Ukraine seems to be also correlating with the significant events of the conflict, such as the occupation of Crimea and the escalation of the conflict at the start of 2022. Based on this, there is a clear link between the events of the conflict and the timing of cyber-attacks targeting Ukraine.

6. Conclusions and Discussion

The results examine the various cases targeting Ukraine. Most of these cases seem to be aimed at causing damage to the information systems, preventing everyday actions dependent on these systems, and bringing extra expenses to Ukrainian organisations with repair costs and lost work hours. Many of the attacks seem to have aimed to maximise their impact on Ukrainian society by causing as much of the effects within the nation as possible. NotPetya and Hermaticwiper -cases have been especially aimed at affecting Ukrainian society broadly. This would indicate that the main objective of these cyber operations is to undermine the functioning of Ukrainian society. Based on this, the attack targets, and the observed correlation between cyber-attacks and significant events of the conflict, most of the observed cases follow similar patterns with Russian information warfare strategies and doctrines throughout the years.

It should be noted, however, that the limitations of the study leave some nation-state activities online outside the scope of this study. These activities include espionage and operations targeting the public perception, which have been observed to be very common. More studies can be done to examine these other kinds of online operations in the Ukraine context further.

In addition, since most of the cases observed have had significant impacts on Ukrainian society, these effects might explain their visibility within the publicly available information. This visibility could impact the nature of cases and their patterns observed in the study. The cases with more minor effects may be left with less attention on the public material, making these more challenging to observe throughout the years. Further studies may be conducted to examine the potential correlation between the effects of the attacks and their public visibility.

Overall, the results indicate that offensive cyber operations are aimed at weakening the ability to operate in Ukraine. The results could be used to anticipate techniques, timing, and targets of cyberattacks if future conflicts arise within societies that have integrated IT technology-based solutions into their regular operating capabilities. In these scenarios, utilising technology may become a significant supporting tool for the toolbox of warfare.

References

Antoniuk, S. (2023) "*Ukraine's largest telecom operator shut down after cyberattack",* The Record. December 12th, 2023. Viewed 15.01.2024. https://therecord.media/kyivstar-cyberattack-telecom-shutdown-ukraine

Antoniuk, S. (2024) "*Russian hackers infiltrated Ukrainian telecom giant month before cyberattack",* The Record. January 4th, 2024. Viewed 15.01.2024. https://therecord.media/russians-infiltrated-kyivstar-months-before

Applegate, S. (2015) "Cyber Conflict: Disruption and Exploitation in the Digital age"*,* in Lemieux, F. (eds.), *Current and emerging trends in cyber operations: Policy, Strategy and Practice*. Basigstoke: Palgrave Macmillan. pp. 19-36.

Banks, W. (2021) "Cyber Attribution and State Responsibility", *International Law Studies*, Vol 91, pp 1040-1072.

Boyte, K. (2017) "A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine", *International Journal of Cyber Warfare and Terrorism*, Vol 7, No. 2 pp 54-69.

Clayton, M. (2014) "*Ukraine election narrowly avoided 'wanton destruction' from hackers",* The Christian Science Monitor. June 17th, 2014. Viewed 15.01.2024. https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers

Cyber Peace Institute (2022) *Case Study: Viasat, June 2022*, Cyber Peace Institute. Viewed 22.01.2024. https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

Cyber Peace Institute (2023a) *Cyber Dimensions of the Armed Conflict in Ukraine: Quarterly Analysis report Q3 July to September 2023*, Cyber Peace Institute.

Cyber Peace Institute (2023b) *Cyber Dimensions of the Armed Conflict in Ukraine: Quarterly Analysis report Q2 April to June 2023*, Cyber Peace Institute.

Dutta, S. "Cyber Operations Associated with the Ukraine-Russia Conflict: An Open-Source Assessment*",* in Chauhan, P., Lahiri, D. and Kumar, R. (eds.), *Maritime perspectives 2022: Non-traditional Dimensions of Maritime Security,* New Delhi: National Maritime Foundation. pp 346-361

Goel, S. (2020) "How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race", *Connections*, Winter, Vol 19, No. 1, pp. 87-95.

Grossmann, T., Kaminska, M., Shires, J., and Smeets, M. (2023) The Cyber Dimensions of the Russia-Ukraine war, ECCRI workshop report. The European Cyber Conflict Research Initiative.

Izycki, E. and Vianna, E. (2021) "Critical Infrastructure: A Battlefield for Cyber Warfare?", *Proceedings of the 16th International Conference on Cyber Warfare and Security, ICCWS 2021,* 25 – 26 February 2021*.* Online*.* pp. 454–464.

Kari M. (2016) "Cyber fortress under siege - The cyber threat to Russia according to Russian public documents", JYU MSc thesis, University of Jyväskylä 2016

Kari M. (2019) "Russian Strategic Culture in Cyberspace: Theory of Strategic Culture – a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats", JYU academic dissertation 122, University of Jyväskylä

Kostyk, N. and Zhukov, Y. (2019) "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?", *Journal of Conflict Resolution,* Vol 63, No. 2, pp 317–347.

Laari, T. (2019*) #Kyberpuolustus, Kyberkäsikirja puolustusvoimien henkilöstölle*, Helsinki: National Defense University.

Lehto, M. (2020) "Cyber warfare: The new game changer in the battlespace*"*, *Cyberwatch magazine*, 2022(2), pp 21-26.

Lehto, M. and Hanselmann, G. (2020) "Non-kinetic warfare – The new game changer in the battle space", *15 th International Conference on Cyber Warfare and Security*, 12-13 March 2020, Old Dominion University, Norfolk, Virginia, USA, pp 316-25.

Microsoft (2022) *Special report: Ukraine – an overview of Russia's cyberattack activity in Ukraine*. Digital Security Unit. 27th April, 2022

Microsoft Digital Security Unit (2022) "*destructive malware targeting Ukrainian organizations,* Microsoft. January 15th, 2021. Viewed 17.01.2024. https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

Mueller, G., Jensen, B., Valeriano, B., Maness, R, and Macias J. (2023) *Cyber Operations during the Russo-Ukrainian War from Strange Patterns to Alternative Futures*, CSIS report July 2023. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

Regional cyber defence centre (2023) *Report on Cyber Lessons Learned during the War in Ukraine,* Vilnius: Regional cyber defence centre.

Przetacznik, J. & Tarpova, S. (2022) *Russia's war in Ukraine: Timeline of Cyber-attacks,* Brieffing of the European Parliament, June 2022. European Parliamentary Research Service.

Simons, G., Danyk, Y. and Maliarchuk, T. (2020) "Hybrid war and cyber-attacks: creating legal and operational dilemmas", *Global change, peace & security,* Vol 32, No. 3, pp 337–342.

Theohary, C. (2021) *Defensive primer: Cyberspace operations*, Congressional Research Service report, 1 December.

Turunen, M. and Kari, M. (2020) "Cyber deterrence and Russia's active cyber defensive", *Proceedings of the 19 the European Conference on Cyber Warfare and Security*, 25-26 June 2020, Online, pp 526-532.

Weedon, J. (2015) "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine*",* From Kenneth Geers (Ed.), "*Cyber War in Perspective: Russian Aggression against Ukraine*", Tallinn: NATO CCD COE Publications.