Jurnal Perencanaan Pembangunan:
The Indonesian Journal of Development Planning
Volume VIII No. 1 - June 2023/Page: 118 - 131
https://doi.org/10.36574/jpp.v8i1.470
Article

The Role of Russian Cyber Operations in The Russian–Ukraine War in Achieving Russia's Strategic Objectives

Firdini[1], Jeffri Urbanus Panggabean[2], and Syaiful Anwar[3]

Corresponding author. Email: firdiney@gmail.com

Submitted: 2023-04-08 | Accepted: 2024-05-28 | Published: 10th June 2024

Abstract

Experts predict that there will be a cyber war when Russia invades Ukraine. Russia is expected to use offensive cyberattacks to create surprise and undermine Ukraine's defenses and morale. Cyberattacks are seen as sufficient to achieve Russia's goals without the need for conventional military force. Cyber operations are predicted to provide strategic advantages for Russia, both as a complement to military power and as an independent instrument. This study seeks to assess the impact of cyber operations that accompanied Russia's invasion in the Russia-Ukraine conflict, considering the circumstances and conditions of the situation. The research approach is a qualitative analysis of literature about the Russia-Ukraine conflict. The results show no evidence to support that Russia's cyber operations measurably affect the course of the conflict, provide tactical advantages, or observable strategic value. Cyber operations tend to produce effects that are immeasurable and difficult to control fully. Cyber operations are not a replacement for military force but can complement military operations. They can be effective for data gathering or disruptive operations, especially in gray zone conflicts. Proper planning, preparation, and resource allocation are necessary for successful cyber operations.

Keywords: cyber-attacks; cyber operations; cyber war; hybrid warfare; Russia–Ukraine war.

[1] Kementerian PPN/Bappenas
[2] Universitas Pertahanan Republik Indonesia
[3] Universitas Pertahanan Republik Indonesia

I. Introduction

The process of globalization has led to complex, contemporary, and global changes in national and international security environments. One notable change is the increasing reliance on information and communication technology, which has diminished the relevance of traditional notions of physical borders and emphasized the importance of cyberspace as a global domain for understanding contemporary security (Strucl, 2022). The present security scenario is marked by growing intricacy and instability caused by swift technological advancements and threats from opponents. However, significant changes in the behavior of state and non-state actors in the cyber realm have not been matched by similar changes in security literature (Harknett & Smeets, 2020). Therefore, it is necessary to focus more on developing ideas and strategies related to military cyber operations and measures for countering cyber threats (Brantly & Smeets, 2020).

The current focus of attention is on cyber operations, particularly cyber-attacks carried out by Russia in the context of the Russia-Ukraine conflict as a tool to achieve its political goals. Russia has used cyber-attacks on several occasions, both as part of military actions and to disrupt societies, as seen in the 2016 US presidential election. Additionally, in response to certain incidents, Russia has utilized cyber-attacks as a means of intimidation against governments. For example, in April when Finland extended an invitation for Ukrainian President Volodymyr Zelensky to speak in parliament, Russia launched cyber-attacks as a show of force. This situation highlights the complexity and importance of cyber operations in the global geopolitical context.

The cyber-attacks used by Russia in the Russia-Ukraine conflict serve as an example of how Russia leverages cyber operations in armed and hybrid warfare against the West, aiming to avoid direct military responses. The invasion of Ukraine provides an opportunity to test theories on how cyber-attacks can be used in conventional warfare. Some predictions suggest that a cyber war may ensue, where Russia would initiate attacks with offensive cyber capabilities to create surprise and weaken Ukraine's defenses and morale. Some experts suggest that Russia might not need to use military force to achieve its goals, as cyber-attacks can provide significant strategic advantages. These attacks can be used either as a complement to military power or as a standalone instrument. Understanding the effectiveness of cyber operations accompanying Russia's invasion in achieving Russia's strategic objectives becomes crucial in the context of the situation and conditions in the Russia-Ukraine conflict.

II. Method

The objective of this study is to assess the effectiveness of cyber operations accompanying Russia's invasion in the Ukrainian conflict from 2014-2017 and early 2022 in achieving Russia's strategic goals. The research method used in this study is qualitative research, which is appropriate for examining natural phenomena (Sugiyono, 2005). The qualitative approach allows for a deeper understanding of the substance of the events under investigation (Sofaer, 1999). The research is conducted through the analysis of documents from previous studies, including journals, articles, and reports related to the Russia-Ukraine War, hybrid warfare, cyber warfare, cyber operations, and cyber-attacks. Technical documents, such as reports analyzing the results of cyber-attack monitoring activities

published as a result of government and private sector collaborations, are also used to obtain more detailed and up-to-date technical data and information about the situation in the field.

III. Result and Discussion

The results of the study indicate that the notion of cyber operations as a high-level destructive tool is not entirely accurate. Instead, they produce low-intensity effects due to practical limitations such as speeds that are judged too slow, strengths deemed too weak, or vulnerabilities that are volatile, reducing their effectiveness as an attack tool in military operations. Even in a hybrid operating setting, cyber operations have only limited strategic value. Therefore, cyber operations are not effective enough in achieving the expected strategic goals. Cyber operations have not been able to replace the use of military force or significantly increase military effectiveness. Military force remains the primary instrument used by Russia in attempting to force Ukraine to comply with its demands, especially in situations of increasing escalation.

The study also found that cyber operations have not been able to replace the use of military force or significantly increase military effectiveness. Military force remains the primary instrument used in attempting to force compliance with demands. However, cyber operations are useful for data/intelligence gathering or disruptive operations, especially when time and severity of effect are not important to the success of the operation.

The success of cyber operations depends on planning, preparation, and sufficient resource allocation, especially in terms of time. Collaboration with foreign cyber defense teams has the potential to be a game-changer in increasing cyber strength in a relatively shorter time. Cyber operations are relevant mainly in gray zone conflicts, through gradually and cumulatively felt attacks, rather than sudden massive attacks.

3.1. Russian Cyber-attack Against Ukraine

So far, there is no universally agreed definition of a cyber-attack. In simple terms, a cyber-attack can be defined as an intentional effort to enter a computer system with malicious intent. Cyber-attacks are carried out by exploiting vulnerabilities in computer systems and data networks, or by tricking users to gain illegal access, with the aim of stealing, destroying, or manipulating data and systems. There are many motives behind cyber-attacks, ranging from sabotage and espionage to theft, fraud, 'hacktivism', etc. Attacks generally take one of three forms: 1) Attacks on confidentiality, which aim to gain access to restricted information; 2) Attacks on integrity, which alter, manipulate, or jeopardize computer data and systems; and 3) Attacks on availability, which impede or restrict legitimate owners' access to their data.

Russian groups, including those linked to the Russian government, are suspected of being involved in cyber-attacks on other countries' infrastructure over the past 20 years. Examples include a series of cyber-attacks targeted at Estonia's parliament, banks, and TV stations in 2007, allegedly in response to a dispute over a Soviet war grave. In 2006 and 2007, Russia's intelligence agency was accused of hacking into the US Democratic National Committee's email system as part of efforts to influence the US presidential election that occurred in the year 2016. In 2015, a Russian group was suspected of being responsible for attacks on Ukraine's power grid. In 2017, the NotPetya malware, allegedly developed by Russian intelligence, spread to A.P. Møller - Maersk's systems, one of the world's largest

container shipping companies, resulting in losses of up to $300 million for Maersk. In 2020, the SolarWinds cyber-attack targeted SolarWinds' Orion software product used by companies to manage IT resources. The attack went undetected for months, allowing hackers to spy on SolarWinds customers and install malware on their systems. Targets included cyber security firms, US government institutions, and Microsoft (Hakmeh, Naylor, & Wallace)

During the conflict between Russia and Ukraine, there was a drastic increase in cyber-attacks. A day before the military invasion, operators linked to the Russian Military Intelligence Agency (GRU) conducted a harmful cyber operation on numerous systems in Ukraine, including those in the government, IT, energy, and financial sectors. The objective of the attack was to destroy, disrupt, or infiltrate critical infrastructure and government networks, which were also targeted by ground and missile attacks by Russian military forces. According to Russian Ministry of Defense documents, to the Russian military, information warfare involves a conflict in the information domain to harm important information systems, disrupt political, economic, and social systems, and use psychological manipulation to create instability and influence a country's decisions in favor of the enemy. (Conceptual Views of the Armed Forces of the Russian Federation's Action in Information Space, 2011). This is reinforced by the statement of the former Chief of Staff of the Russian Armed Forces, who expressed his view that winning in information warfare is sometimes more important than winning in classic warfare with the use of weapons. This is characterized by effects that draw attention and paralyze the entire authority of the enemy state. Therefore, in modern warfare, operations to weaken the military, and economic potential, lower the morale of forces, and discredit the leadership of the state, including the military, have become an integral part of war strategy (Novosti, 2017).

On February 24th, 2022, Russian tanks crossed the border into Ukraine, but in reality, cyber-attacks on Ukraine's critical infrastructure had been carried out a few days earlier. Since the beginning of the war, Russia has launched nearly 800 cyber-attacks on Ukraine, some of which have caused significant economic losses and most of which have had psychological effects, according to the European Cyber Conflict Research Initiative (Kaminska, Shires, & Smeets, 2022). A report was published by Microsoft's Digital Security Unit on April 27, 2022, which analyzed and recorded the cyber-attacks carried out by Russia against Ukraine during the early months of the war. The report concluded that Russia's Military Intelligence Agency, the GRU (Glavnoye Razvedyvatelnoye Upravlenie), the Foreign Intelligence Agency, the SVR (Sluzhba Vneshney Razvedki), and the Federal Security Service, the FSB (Federal'naya Sluzhba Bezopasnosti), launched destructive attacks and espionage operations. Additionally, Russian military forces also attacked Ukraine through land, air, and sea. The aim of the cyber-attacks launched by Russia's military intelligence agencies was to disrupt or harm the functioning of Ukraine's government and military, and to erode public trust. As the conflict escalated, the frequency and intensity of the cyber-attacks also increased, with 15 attacks in December 2021 and a significant rise to 125 attacks in March 2022.

Russia initiated the destructive attacks by releasing the WhisperGate wiper to delete hard drives and make computers unbootable on several government and private IT systems when discussions among Russia, Ukraine, NATO, and EU countries were unsuccessful in reaching an agreement on January 13, 2022. In response, Russia launched attacks on services on the Ukrainian government website. Prior to the commencement of the war on February

23, 2022, a group within the Russian Military Intelligence Agency, known as the GRU, which engages in threatening activities known as Iridium released another harmful computer program named FoxBlade on multiple networks of the Ukrainian government and military all at once (Orenstein, 2022). Microsoft detected a link between particular military operations and cyber-attacks during the conflict between Russia and Ukraine. The attacks were concentrated in Kyiv and Donbas and targeted nuclear power companies, particularly when Russia took control of the biggest nuclear power station in Zaporizhia, Ukraine. During the course of the war, the frequency of cyber-attacks escalated, increasingly damaging, and more closely coordinated with the actions of the military. Microsoft's observation showed that Russia deployed several destructive malwares, including WhisperGate, FoxBlade, DesertBlade, CaddyWiper, FiberLake, SonicVote, and Industroyer2, to overwrite data and render computers unable to boot or to target industrial technology for physical effects (Microsoft, 2022). Table 1 shows various data-wiping malware used in Russia's cyber-attacks against Ukraine.

Table 1. Data Wipers Used in Russian Cyber-attacks Against Ukraine

Malware	*MBR*	*GPT*	*Files*	*Associated Ransomware*	*Target OS*	*Languages*
WhisperGate	Y	N	Y	Y	Windows	C++ (Stage 1)
			Y	Y	Windows	.NET (Stage 2, 3)
HermeticWiper	N**	N**	Y	N	Windows	C, Assembly
IsaacWiper	Y	N**	N	N	Windows	C, C++, Assembly
DesertBlade	?	?	Y	N	Windows	Golang
*ACIDRAIN**	N/A	N/A	Y	N	Linux (MIPS)	C
CaddyWiper	Y	N	Y	N	Windows	C
DoubleZero	N**	N**	Y	N	Windows	.NET
AwfulShred	Y	Y	Y	N	Linux	Bash
SoloShred	Y	Y	Y	N	Solaris	Bash

Source: Insikt Group, 2022

According to the report from the European Cyber Conflict Research Initiative, experts have analyzed Russia's approach to the Ukrainian conflict and concluded that Russia's cyber-attacks since the beginning of the conflict have been relatively unsophisticated. They merely rehashed old malware in some cases. This suggests that if Russia possessed more potent attack capabilities, it would have utilized them right from the start of the invasion. This implies that Russia may not have any backup cyber capabilities. Nonetheless, this does not necessarily mean that Russia will not execute more harmful cyber-attacks in the future. (Antoniuk, 2022).

3.2. Characteristics Of Russian Cyber Operations

The current focus of academic and political discussions is on Russia's hybrid operations involving information and cyber operations, known as the "gray zone" war. The three main features of Russia's hybrid operations that have been identified are: conserving the use of military force, being conducted continuously, and focusing on the population. In practice, Russia's hybrid strategy had three key strategic objectives, namely 1. Taking

control of land without relying on traditional military methods; 2. Generating a pretext for overt conventional military action; and 3. Using mixed measures to influence a state's politics (Chivvis, 2017).

The Russian approach to cyber warfare has several key characteristics. Firstly, Russian cyber operations tend to be highly strategic, with a focus on achieving specific political objectives rather than simply causing damage. This is often achieved through the use of sophisticated propaganda and disinformation campaigns that seek to manipulate public opinion and sow discord within target countries. Secondly, Russian cyber operations often involve the use of third-party proxies and "patriotic hackers" who are not directly affiliated with the Russian government but share its goals and ideology. This allows the Russian government to maintain plausible deniability and avoid direct retaliation. Thirdly, Russian cyber operations are characterized by a high degree of coordination between different elements of the government, including the military, intelligence agencies, and civilian hackers. This enables Russia to deploy a wide range of cyber capabilities, from relatively unsophisticated attacks carried out by non-state actors to highly advanced cyber espionage and sabotage operations. Finally, Russian cyber operations tend to be highly adaptable and responsive to changing circumstances. This enables Russia to quickly adjust its tactics and techniques in response to new threats or opportunities and to exploit weaknesses in target countries' cyber defenses (Connel and Vogler, 2017).

Three viewpoints exist on the significance and effectiveness of cyber operations in warfare. First, cyber operations are very important in conventional military conflicts, however, studies indicate that there are restrictions to the effectiveness of cyber operations as a method of demonstrating strength. The second perspective sees cyber operations as a complement to military power, damaging devices, causing disruption to systems that control and direct military operations, spreading disinformation, and undermining enemy morale. The third perspective shows that cyber operations are relevant in gray-zone conflicts, using separate tools of influence and power to impact and undermine adversaries through attacks on vital infrastructure systems, disrupting the economy, and operations to influence or manipulate public opinion and decision-making processes. Thus, cyber operations are anticipated to substitute the use of force in attaining comparable goals without resorting to war, by means of incremental and accumulating attacks, eroding enemy strength in several operations, rather than sudden massive attacks (Maschmeyer & Kostyuk, 2022).

3.3. Russian Cyber Operations Phase I (2014 – 2017) and Phase II (Early 2022)

The massive buildup of Russian military forces along the Ukrainian border has raised concerns of the biggest military confrontation starting from the end of World War II, including predictions of a potential cyber war. These forecasts suggest that Russia anticipates substantial strategic benefits from cyber operations, either as a complement to the use of military power or as a stand-alone instrument.

During the period of 2014-2017, Russia launched five (5) cyber-attacks against Ukraine, including Election Interference (2014), Electricity Grid Sabotage (2015 and 2016), Economic Disruption NotPetya (2017), and Economic Disruption BadRabbit (2017). In the next phase, cyber-attacks remained a tool for Russia at the beginning of 2022, when attempts at diplomacy were unsuccessful in easing tensions around Russia's military buildup on the Ukrainian border. Russian malicious actors conducted more frequent and severe attacks with wiper malware against various Ukrainian agencies. This suggests that Russia's actions in

Ukraine had reached a destructive phase that had the potential to escalate even further. At the beginning of January, the malicious actor group DEV-0586 released WhisperGate malware, which had the ability to locate and remove certain file extensions and manipulate the Master Boot Record (MBR) to make the targeted computer useless. A small number of government systems and the IT industry were impacted by this destructive malware and destroyed Ukrainian government websites in February. On the night of the Russian invasion, the cyber-attacks became more intense, as IRIDIUM deployed the Foxblade6 malware (also known as HermeticWiper) to destroy approximately 300 systems across more than 12 organizations in Ukraine's government, IT, energy, agriculture, and financial sectors. The distribution of FoxBlade malware was customized for particular environments, unlike the NotPetya worm within the targeted organization's domain (Microsoft, 2022b). These attacks had the potential to escalate the conflict even further. Figure 1 illustrates the correlation between political-military events and the cyber-attacks that occurred.

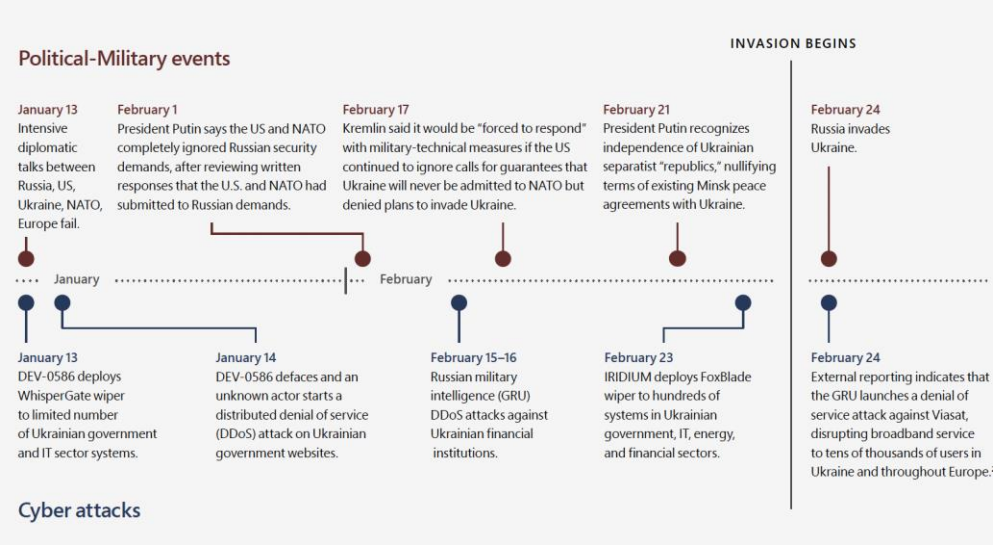

Figure 1. Timeline of the Relationship between Political-Military Events and Russian Cyber-attacks

Source: (Microsoft, 2022b)

3.4. Cyber Operations in Achieving Russia's Strategic Objectives

After the invasion occurred, the initial prediction about a cyber war did not happen. Concerns about cyber warfare are related to two interconnected issues. First, the excessive use of the term "cyber war" to refer to all politically motivated cyber operations. This causes every incident to be interpreted as a sign of widespread vulnerability in modern society and as a harbinger of doom. With this perspective, it could be said that a cyber war has already occurred. The second problem is the lack of consensus on the definition of cyber war, which is usually defined as a cyber-attack those damages critical civilian infrastructure. By referring to societal vulnerabilities and concluding that doom is likely to happen, according to this view, a cyber war is yet to occur.

During the Hybrid War period of 2014-2017, Russia launched five (5) cyber-attacks against Ukraine, including election interference (2014), sabotage of electricity grids (2015

and 2016), economic disruption of NotPetya (2017), and economic disruption of BadRabbit (2017). However, impact analysis shows that cyber operations only caused temporary disruptions and no significant economic or psychological impact, and only affected a small number of targets whose data could later be recovered. From a strategic value standpoint, the NotPetya operation was an exception as it caused 65 countries have experienced notable economic harm, including Russia, due to its difficulty in being controlled and its long-term impact on public infrastructure and business as well as data destruction.

Based on the conflict in Ukraine, Russia's eight-year-long cyber operations did not achieve the desired results. Analysis of the period of battle between 2014 and 2016 showed that there was no significant connection between military operations and cyber operations, and the cyber operations did not reciprocate. This indication suggests that cyber operations did not have a clear impact on armed conflicts, and digital operations occurred independently of events on the ground. It also shows that cyber operations were not used as an effective complement to the Russian armed forces. In the initial military confrontation where both parties heavily employed minor cyber operations, cyber operations had no significant effect on either side. Therefore, the use of cyber operations in armed conflicts still cannot be considered an effective tool in achieving significant strategic value.

The history of utilizing cyber operations as an individual tactic in the Ukrainian gray zone conflict illustrates that cyber operations are not effective in achieving Russia's strategic goals. Examination of the five significant cyber operations backed by Russia demonstrates that the majority of operations did not make a measurable contribution to Russia's strategic goals. The primary disadvantages of conducting cyber operations are the potential loss of control over the propagation of consequences, inadvertent outcomes, and additional expenses. Evidence from the Russia-Ukraine conflict shows that the perspective of cyber operations as a substitute for or complement to force has become irrelevant. Cyber operations are more relevant as a standalone alternative with lower intensity in the use of force.

Cyber operations rely on subversive mechanisms that exploit vulnerabilities in the enemy's system to be used against them. Although it has great strategic value, the effectiveness of cyber operations is constrained by an operational trilemma that involves balancing speed, intensity of impact, and degree of control. This trilemma limits the strategic value of cyber operations because they often run too slow, too weak, and too fluctuating to make a measurable contribution towards strategic objectives. The function that restricts this trilemma is apparent in the five cyber operations supported by Russia against Ukraine as shown in Table 2.

The historical performance of cyber operations as a solitary tactic in the Ukrainian gray zone conflict has not yielded the desired results. Russian cyber operations tend to be slow, weak, or fluctuating in achieving Russia's strategic goals. Cyber operations rely on subversive mechanisms that present operational challenges, including a trilemma that involves balancing speed, impact intensity, and control over outcomes. The effectiveness of one variable can be achieved by sacrificing the remaining variables. The trilemma can be clearly seen in all Russian cyber operations against Ukraine, which are distinguished by operations that are either too slow, too feeble, or too inconsistent to generate strategic significance. An exception is given to the NotPetya malware that caused significant economic losses but also demonstrated the limitations of cyber operations when malware spreads beyond control. These limitations make cyber operations less relevant as a substitute

or complement to force, but can still be used as a standalone alternative with lower intensity. Russia's cyber operations in Ukraine are considered to have failed to provide measurable contributions to Russia's strategic goals and have damaged public support for this policy.

Table 2. Russian Cyber Operations Against Ukraine 2014-2017

Operation	Description	Impact	Strategic Value
Election Interference (2014)	Attempted to disrupt Ukraine's Central Election Commission system but missed contingencies that allowed for quick system recovery.	Temporary disruption of the Central Election Commission system, had no impact on the election or vote counting.	Ignored
Electric Grid Sabotage (2015)	Disrupted power supply in Eastern Ukraine. Victims were able to switch to manual control and neutralize it.	Temporary power outage (6 hours), no measurable economic or psychological impact	Ignored
Electric Grid Sabotage (2016	Disrupted power supply, but victims quickly switched to manual control. Also attempted physical damage to substations, but failed due to basic errors	Temporary power outage (75 minutes), no measurable economic or psychological impact.	Ignored
NotPetya Economic Disruption (2017)	A self-propagating malware that disabled systems by encrypting data, affecting critical economic and infrastructure disruption. Spread out of control.	Temporary disruption of public and business infrastructure, long-lasting data destruction, significant economic damage in 65 countries (including Russia itself).	Uncertain
BadRabbit Economic Disruption (2017)	A manually installed malware that disabled systems by encrypting data. Designed to control the spread, affecting a small number of targets.	Minimal and temporary disruptive impact on a small number of targets, data can be recovered.	Ignored

Source: (Maschmeyer, 2021)

In the 2022 phase, Russia failed to achieve its goals through cyber operations in the previous phase. The expectation that the cyber conflict would change when the notion of a transition from low-intensity hybrid warfare to high-intensity conventional warfare during the conflict is still hypothetical and encounters practical impediments. If Russia expects different results, significant planning, preparation, and resources are needed, particularly in terms of time (Maschmeyer & Cavelty, 2022). The cyber operations carried out in Phase 2 also failed to provide the expected strategic value, as shown in Table 3. A series of Russian cyber operations in this phase appeared to be rushed, reckless, and a complete failure. In practice, cyber operations have failed in the Russia-Ukraine conflict. Research conducted by Maschmeyer (2021) indicates that cyber operations remain insignificant in the field of combat, although Russia conducted autonomous operations to debilitate Ukraine, such as meddling in elections, sabotaging essential infrastructure, and causing economic turmoil, these efforts mostly failed to assist Russia in accomplishing its strategic objectives against Ukraine.

Table 3. Strategic Value of Cyber Operations in 2022

Name/Effect	Strategic Value
Jan 2022 Website Defacements	
Multiple UKR government websites temporarily defaced with threatening message, no reported impact on systems.	Negligible
Jan - April 2022 *Disk Wiper*	
Multiple disk wipers (data-deleting malware) infected Ukrainian systems, small to modest scale, no evidence of significant impact.	Negligible
Feb 2022 DDoS Attacks	
Distributed Denial of Service Attacks (DDoS) temporarily overloaded websites of UKR government agencies and some banks, causing nuisance but no lasting impact or damage.	Negligible
Feb 2022 Viasat Sabotage	
Viasat Satellite Communication Service (used by UKR military) disrupted at the time Russian invasion started. No impact on UKR military communications but collateral damage across Europe.	Negligible
April 2022 Power Grid Sabotage	
Attempt to disrupt power supply in Ukraine, detected and deleted before any effect achieved.	None

Source: (Maschmeyer & Cavelty, 2022)

Russia's cyber operations have been limited by various factors, including inadequate cyber capability, weak non-cyber institutions, and strong defense measures by Ukraine and its allies. Cyber operations need to be conducted at a pace that Russia appears incapable of sustaining for more than a few weeks. Russia has worsened its capacity problem by conducting global cyber activities and failing to employ cyber criminals as an auxiliary force against Ukraine. Furthermore, Russian military leaders seem unable to plan and execute war in a precise, intelligence-driven manner that is most effective for cyber operations. On the other hand, Ukraine has a resilient digital infrastructure and has received significant cyber assistance from capable governments and companies. Even if some factors were reversed, the military effectiveness of Russian cyber operations is unlikely to improve significantly (Bateman, 2022).

The operational trilemma proved to be true for Russia's cyber operations in the Russia-Ukraine conflict. The majority of Russia's cyber operations depended on simple and rapid, yet weak impacts, such as erasing data, demolishing websites, and launching DDoS attacks. More intricate assaults usually result in failure or loss of control. Attempts to disrupt electricity with the same malware used in 2016 failed completely. The attempt to interfere with the Viasat satellite communication network, with the aim of severing Ukrainian military communication, did not result in any significant outcomes. Instead, the disruption spread uncontrollably, causing significant additional damage to other European service customers, encompassing numerous wind turbines located in Germany. Generally speaking, there is no indication that Russia's cyber operations in the conflict measurably affected its course, provided observable tactical advantages, or produced strategic value.

The operational trilemma hinders the success of Russia's cyber operations in the ongoing Russia-Ukraine conflict. The trilemma refers to the tradeoff between speed,

intensity, and control over the effects of cyber operations. Russia's cyber operations in Ukraine have been hampered by this trilemma, leading to slow, weak, and unreliable attacks that failed to yield significant strategic value. Moreover, the statement emphasizes that underestimating and overestimating Ukraine's defense capabilities played a crucial role in the success of Russian cyber operations. In some instances, Russia underestimated Ukraine's ability to defend against cyber-attacks, leading to a lack of preparation and weak execution of its operations. Conversely, overestimating Ukraine's capabilities led to unnecessarily complex and risky attacks, resulting in a loss of control and unintended consequences. Recent cyber-attacks launched by Russia against Ukraine have targeted government agencies, military facilities, and critical infrastructure by using phishing emails, malware, and distributed denial-of-service (DDoS) attacks. However, while the attacks have caused some disruption, they have not had a significant impact on Ukraine's ability to function. It is also important to note that Ukraine has become adept at defending against cyber-attacks since it became a target of Russian cyber aggression in 2014.

Collaboration between the public and private sectors to address cyber threats is highly beneficial. This includes sharing information about threats and attacks and working together to develop and implement effective cybersecurity strategies (Chivvis, 2017). The United States and other allies have assisted Ukraine in strengthening its cybersecurity defenses, which may have played a crucial role in thwarting Russia's cyber operations (McLauglin, 2023). Ukraine's collaboration with foreign cyber defense teams has helped it improve its defenses and respond more effectively to Russian cyber threats. Due to the operational trilemma and an inaccurate assessment of Ukraine's defense capabilities, Russia's cyber operations have been less effective in the ongoing conflict. Collaborating with foreign cyber defense teams has been a significant factor in mitigating the impact of these operations.

Preparing for dealing with large-scale cyber threats involves investing in cybersecurity and being ready to respond to cyber-attacks. Ukraine's experience demonstrates that having strong cybersecurity defenses is crucial in minimizing the impact of cyber-attacks. Organizations should expect the possibility of a cyber-attack and have a response plan in place. This includes having a team to handle the response, backup systems, and data to aid in restoring operations post-attack. To have a clear direction on how to respond to significant cyber-attacks, a comprehensive cybersecurity strategy that encompasses not just technical measures but also policies, procedures, and personnel training is necessary.

IV. Conclusion and Recommendation

4.1. Conclusion

In conclusion, the study reveals that the expectation that cyber operations can provide high-level destructive effects in the cyber realm is not entirely accurate. Cyber operations tend to produce low-intensity effects due to practical limitations such as slow speeds, weak strengths, and volatile vulnerabilities. Even in a hybrid operating setting, cyber operations have limited strategic value and cannot replace military force or significantly increase military effectiveness. However, cyber operations can be useful for data/intelligence gathering or disruptive operations when time and severity of effect are not critical to the success of the operation. The success of cyber operations depends on proper planning, preparation, and sufficient resource allocation, especially in terms of time. Collaboration with

foreign cyber defense teams can enhance cyber strength relatively quickly. Furthermore, the study highlights that cyber operations are relevant mainly in gray zone conflicts, where gradually and cumulatively felt attacks can be effective, rather than sudden massive attacks. However, there is no evidence to suggest that Russia's cyber operations in the Russia-Ukraine conflict had a measurable effect on the course of the conflict or provided observable tactical or strategic value. Cyber operations tend to produce unmeasurable effects that are challenging to control entirely. In summary, while cyber operations have limitations and cannot replace military forces, they still have a role to play in military operations as a complementary tool. Successful cyber operations require proper planning, preparation, and resource allocation. In certain situations, cyber operations can be effective for data gathering or disruptive operations, mainly in gray zone conflicts.

4.2. Recommendation

Based on the conclusion of the study, the following recommendations can be formulated. First, enhance collaboration. Given the limitations of cyber operations and the potential benefits of collaboration, countries should consider collaborating with foreign cyber defense teams to increase their cyber strength. Collaboration can help to enhance resource sharing, skill-building, and speed up the development of new cyber capabilities. Second, invest in planning and preparation. Successful cyber operations require proper planning, preparation, and sufficient resource allocation, especially in terms of time. Military organizations should invest more in training and equipping cyber defense teams to develop more advanced capabilities and to ensure that they are prepared to deal with the latest threats. Third, focus on gray zone conflicts. Cyber operations can be more effective in gray zone conflicts, where gradually and cumulatively felt attacks can be effective, rather than sudden massive attacks. Military organizations should focus on developing cyber capabilities that are relevant to gray zone conflicts to increase their strategic value. Fourth, monitor and evaluate the effectiveness of cyber operations. Given the difficulties in measuring the effectiveness of cyber operations, military organizations should develop ways to monitor and evaluate the impact of their cyber operations. This will help to identify areas of improvement and enhance the effectiveness of future cyber operations. In summary, by enhancing collaboration, investing in planning and preparation, focusing on gray zone conflicts, and monitoring and evaluating the effectiveness of cyber operations, military organizations can improve their cyber capabilities and make the most of the potential benefits of cyber operations.

References

Antoniuk, Daryna. (2022). Lessons learned from Russia's cyber-attacks targeting Ukraine. Available from https://therecord.media/report-lessons-learned-from-russias- [Accessed March 24, 2023]

Bateman, Jon. (2022). Russia's wartime cyber operations in ukraine: military impacts, influences, and implications. Available form https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-

in-ukraine-military-impacts-influences-and-implications-pub-88657 [Accessed April 8, 2023]

Brantly, A., and Smeets, M., (2020). Military cyber operations. In A. McD Sookermany. Handbook of Military Sciences (pp 1-13). Available from https://link.springer.com/referencework/10.1007/978-3-030-02866-4 [Accessed March 25, 2023]

Chivvis, C. S. (2017). Understanding Russian hybrid warfare and what can be done about it. Santa Monica: RAND.10.7249/CT46. Available from https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_C [Accessed March 22, 2023]

Conceptual Views of the Armed Forces of the Russian Federation's Action in Information Space. (2011). Available from https://nsarchive.gwu.edu/document/17098-russian-government-conceptual-views-regarding [Accessed March 24, 2023]

Connel, Michael, and Sarah Vogler. (2017). Russia's Approach to Cyber Warfare. Available from https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf [Accessed April 7, 2023]

Hakmeh, Joyce, Ester Naylor, and Jon Wallace (2022). What is cyber-attack? Available from https://www.chathamhouse.org/2022/02/what-cyber- [Accessed March 22, 2023]

Harknett, J. R., and Max Smeets. (2020). Cyber campaigns and strategic outcomes. Journal of Strategic Studies, pp 1-34. Available from https://www.matthewmonte.net/wp-content/uploads/2022/05/Cyber-campaigns-and-strategic-outcomes.pdf [Accessed March 25, 2023]

Insikt Group. (2022). Overview of the 9 distinct data wipers used in the ukraine war. Available from https://www.recordedfuture.com/overview-9-district-data-wipers- [Accessed March 23, 2023]

Kaminska, Monica, James Shires & Max Smeets. (2022). Cyber operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far). Available from https://eccri.eu/wpcontent/uploads/2022/07/ECCRI_WorkshopReport_Version-24 [Accessed March 24, 2023]

Maschmeyer, Lennart. (2021). The subversive trilemma: why cyber operations fall short of expectations. Available from International Security 46:(2) (2021):51–90.

Maschmeyer, Lennart & Myriam Dunn Cavelty. (2022). Goodbye cyberwar: Ukraine as reality check. Available from https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP10-3_2022-EN.pdf [Accessed March 24, 2023]

Maschmeyer, Lennart & Nadiya Kostyuk. (2022). There is no cyber shock and awe: plausible threats in the ukrainian conflict. War on the Rocks. Available from https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible- [Accessed March 23, 2023]

McLaughlin, Jenna. (2023). Russia bombards Ukraine with cyber-attacks, but the impact appears limited. https://www.npr.org/2023/02/23/1159039051/russia-bombards-

ukraine-with-cyber-attacks-but-the-impact-appears-limited [Accessed April 7, 2023]

Microsoft. (2022a). An overview of russia's cyber-attack activity in ukraine. Available from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd 3 [Accesed March 23, 2023]

Microsoft. (2022b). Destructive malware targeting Ukrainian organizations. Available from https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware- 25 [Accessed March 25, 2023]

Orenstein, Mitchell. (2022). Russia's use of cyber-attacks: lessons from the second ukraine war – analysis. Available from https://www.eurasiareview.com/08062022- [Accessed March 23, 2023]

Ria Novosti. (2017). Shoigu spoke about the tasks of the information operations troops. Available from https://ria.ru/20170222/1488617708.html [Accessed March 24, 2023]

Sofaer, S. (1999). Qualitative methods: what are they and why use them? Health Services Research 34:4 Part II. Available from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1089055/ [Accessed Oktober 22, 2022]

Štrucl, Damjan. (2022). Russian aggression on ukraine: cyber operations and the influence of cyberspace on modern warfare. Contemporary Military Challenges/Sodobni Vojaški Izzivi, vol.24, no.2, 2022, pp.103-123.

Sugiyono. (2005). Memahami Penelitian Kualitatif. Bandung: Alfabeta.