Available online at: http://jurnal.utu.ac.id/jppolicy

Jurnal Public Policy

| ISSN (Print) 2477-5738 | ISSN (Online) 2502-0528 |

Cyber Warfare Strategies in the Russia-Ukraine Conflict (2021-2022): Implications for National Security and Modern Warfare

Khoirunnisa, Cristy Sugiati

Universitas 17 Agustus 1945 Jakarta. Jl Sunter Permai Raya, Jakarta 1435. Indonesia

ARTICLE INFORMATION

Received: October 23, 2023
Revised: December 14, 2023
Available online: April 28, 2024

KEYWORDS

Cyber warfare; Russia-Ukraine conflict; Distributed Denial of Service (DDoS) attacks; National security; Cyber security.

CORRESPONDENCE

Name: Khoirunnisa
Email: khoirunnisa@uta45jakarta.ac.id

ABSTRACT

This study examines the cyber warfare strategies employed during the 2021-2022 conflict between Russia and Ukraine, focusing on how technological developments in information and communication have influenced this aspect of modern warfare. The conflict escalated as Russia viewed Ukraine's desire to join NATO as a significant threat, leading to a mix of military and non-military strategies, including extensive cyber attacks. Using a descriptive qualitative method, this research analyzes the cyber warfare strategies through the lens of state security, national interest, and cyber security theories. The findings highlight that both Russia and Ukraine utilized Distributed Denial of Service (DDoS) attacks and hacker groups to damage and disable governmental systems, aiming to disrupt communication and weaken the opponent with minimal costs. Russia's advanced cyber capabilities made Ukraine a vulnerable target, resulting in widespread cyber assaults impacting both civilian and governmental infrastructures. The study concludes that cyber warfare has emerged as a pivotal strategy in modern conflicts, with effects comparable to traditional military tactics. The Russia-Ukraine conflict underscores how cyber strategies can be used to achieve national interests and demonstrates the growing importance of cyber security in contemporary warfare. This conflict also serves as a warning to other nations regarding the vulnerabilities in their cyber defenses.

INTRODUCTION

This research aims to provide a comprehensive overview and explanation of cyber warfare strategies within the context of the Russia-Ukraine conflict from 2021 to 2022. The emergence of cyber warfare is relatively new in the long history of military strategies and defense security. Over the past decade, cyber warfare has garnered increasing attention as a novel aspect of international relations (Jennex, 2007). Unlike conventional warfare, which typically involves direct confrontation between military forces and physical weaponry, cyber warfare leverages technology to invade and disrupt a nation's systems without the need for a traditional military presence (Rid, 2012; Welch & Feeney, 2014). According to Relia (2016), cyber warfare uses technology to cause damage comparable to that of conventional warfare, requiring fewer resources but achieving a similarly devastating impact.

The evolution of conflict strategies has influenced the dynamics of global conflict, prompting a shift towards new forms of warfare (Kelly, 2019). These new strategies, including cyber warfare, provide a fresh perspective on how wars are fought. Instead of relying solely on military power and weaponry, cyber strategies allow states to wage war through technological means, minimizing the need for physical forces. States can attack their targets using various cyber tools, such as data manipulation, hacking, and malware, to compromise governmental and institutional systems (Thornton, 2020). As Pool (2013), points out, cyber warfare involves using malware, viruses, worms, and other forms of attacks on software and hardware connected to government systems to achieve political and military objectives.

The concept of cyber warfare aligns with Sun Tzu's principle in The Art of War, where he states, "The supreme art of war is to subdue the enemy without fighting" Niagahoster, (2021). This quote underscores the modern warfare approach, in which nations no longer need to engage in direct military confrontation to defeat their enemies. Instead, using sophisticated skills and technological capabilities, a state can inflict significant damage, effectively "winning" the war. This form of warfare leaves the enemy in a weakened state, requiring substantial time and resources to recover.

The advent of globalization has contributed to the rise of technological, informational, and communicative advances, which, in turn, have shaped modern warfare. Globalization, while fostering interconnectedness, has also amplified ethnic conflicts and weakened state sovereignty, allowing both internal and external political actors to influence national security. As described by Kirshner (2006), globalization has reduced states' capacity to maintain control over their national security, thus altering the nature of conflicts. These conflicts are no longer solely conventional but increasingly non-conventional, with cyber warfare being a prominent example.

The rapid pace of technological development, particularly in the realm of communication, has broken down conventional borders, pushing states to adapt to the digital age. This has had profound effects on how nations perceive and execute warfare. As national security becomes intertwined with digital infrastructures, cyber warfare has emerged as a key area of concern for many countries. Non-conventional wars, particularly cyber warfare, threaten national security by attacking critical infrastructure and systems rather than engaging in traditional military battles.

Over the past decade, cyber warfare has evolved into a critical point of tension in international relations, with nations increasingly recognizing the strategic advantages and risks posed by cyber conflicts. For countries that do not fully comprehend or

https://doi.org/10.35308/jpp.v10i2.9026

prepare for these developments, reliance solely on conventional military strategies may leave them vulnerable to adversaries employing more advanced, non-conventional cyber strategies.

Cyber warfare is defined as the use of technology to steal or destroy a target nation's information to advance national interests. Similarly, cyber warfare as actions taken by a state to infiltrate another nation's computer networks with the intent of causing damage. Richard Clarke echoes this definition, emphasizing that the goal of cyber warfare is to breach another nation's computer systems to achieve destruction. Unlike conventional warfare, where physical territory is contested, the battlefield in cyber warfare is the digital domain, targeting cyber systems and infrastructures crucial to national stability.

Cyber warfare differs from cybercrime, which refers to illegal activities targeting individuals or groups to inflict harm or cause financial and emotional distress using the internet or modern communication tools (Maskun., 2013). Cybercrime includes traditional crimes such as fraud, theft, defamation, and others, but conducted through digital means. In contrast, cyber warfare operates on a much larger scale, often directed by state actors or state-backed hacker groups, aiming to disrupt national security systems.

The tensions between Russia and Ukraine have deep historical roots, with significant conflicts dating back to 1991 when Ukraine declared independence from the Soviet Union. Although Russia initially recognized Ukraine's independence, tensions soon arose, particularly with Ukraine's desire to join NATO. Ukraine's plan to align with NATO was perceived as a direct threat to Russia's territorial and national security. In 2014, tensions escalated into a military conflict over the Crimean Peninsula, resulting in the deployment of Russian military forces into Ukrainian territory (Oktarianisa, 2022). This military conflict set the stage for further hostilities, culminating in a series of military and cyber engagements between the two nations.

The 2021-2022 conflict marked a turning point in the relationship between Russia and Ukraine. Fueled by Ukraine's renewed interest in joining NATO under President Volodymyr Zelenskyy, Russia responded by rejecting Ukraine's aspirations and deploying both military and non-military strategies, including cyber warfare. The conflict garnered significant international attention as it unfolded, involving military incursions alongside extensive cyber attacks aimed at Ukrainian infrastructure. Russia's cyber attacks in this conflict primarily targeted Ukraine's governmental systems and critical infrastructure, using sophisticated strategies like Distributed Denial of Service (DDoS) attacks and hacking campaigns.

During the conflict, Russia reportedly carried out cyber operations that deleted data from Ukrainian systems, including a significant cyber attack known as WhisperGate in early 2022. These attacks damaged important Ukrainian websites, disrupting communication and governance functions. In many ways, the cyber attacks carried out by Russia in this period achieved the same goals as conventional military tactics: disrupting national stability, weakening the enemy, and asserting dominance.

According to data from the Center for Strategic and International Studies (CSIS), Ukraine experienced 27 major cyber attacks between 2014 and 2022, targeting a range of sectors, including banking, energy, and transportation. The most notable attack occurred in 2017 when the NotPetya ransomware crippled several key Ukrainian institutions, including banks and airports. The economic and infrastructural damage from this attack was estimated to be in the hundreds of millions of dollars (Chrisnandi, 2019). These attacks illustrate how cyber warfare has become a prominent feature of the Russia-Ukraine conflict.

The theoretical framework of this study relies on state security and national interest theories, as well as concepts from cyber security. The theories of military strategy articulated by Clausewitz (2021) emphasize that conflict strategies can be divided into two fundamental techniques: the tactical execution of war and the broader strategy that combines military efforts to achieve overarching goals. Clausewitz's theory highlights the importance of intelligence, quality of forces, psychological factors, and weaponry, all of which are applicable to both conventional and cyber warfare. In cyber warfare, nations leverage their technological intelligence to outmaneuver opponents, often achieving strategic goals with minimal physical confrontation or resource expenditure.

The research gap addressed by this study lies in the limited exploration of cyber warfare strategies within the Russia-Ukraine conflict. While prior studies have examined the broader geopolitical implications of the conflict, few have focused specifically on the cyber dimensions and their role in shaping the conflict's outcome. Additionally, this research integrates the concept of cyber security, particularly the CIA Triad (Confidentiality, Integrity, and Availability), which forms the foundation of national cyber defense strategies (Whitman & Mattord, 2021). The primary research question of this study is: "How have cyber warfare strategies influenced the Russia-Ukraine conflict from 2021 to 2022, and what are the broader implications for national security and modern warfare?"

METHOD

This study employs a qualitative descriptive method to analyze cyber warfare strategies in the Russia-Ukraine conflict during the 2021-2022 period. This method was chosen because it allows for an in-depth exploration of complex phenomena related to the use of technology in modern warfare. The approach enables researchers to examine how both countries utilize cyberattacks, such as Distributed Denial of Service (DDoS) and hacker attacks, as part of efforts to undermine the opponent's critical infrastructure. The research data will be collected from secondary sources, including reports from international organizations, academic journals, news, and official documents related to cybersecurity.

The collected data will be analyzed using a thematic approach, where the researcher identifies key themes that emerge concerning the strategies and impacts of cyberattacks during the conflict. The analysis will focus on the techniques used in cyberattacks, their effects on government systems and civilian infrastructure, and how both countries responded to these threats. Additionally, this study will explore the role of state-sponsored hacker groups in extending the reach and effectiveness of cyberattacks.

To ensure validity and reliability, the data used will be validated through triangulation by comparing various sources of information. Through this analysis, the research aims to provide a clearer understanding of the strategic role of cyber warfare in the Russia-Ukraine conflict and its implications for national and global security. This study is expected to highlight how cyber warfare has become a crucial element in modern warfare and a challenge to the digital security of nations worldwide.

RESULTS AND DISCUSSION

Conventional and Unconventional Warfare

Conventional warfare refers to a form of warfare that involves direct physical combat between the armed forces of two or more countries, using military force and weapons in accordance with established rules. This conflict usually takes place on a clearly defined battlefield, where the strategies and tactics used are well established. Conventional warfare can include various forms, such as regional wars involving several countries in a specific geographic area—such as World Wars I and II—and terrorist warfare, which, although often associated with unconventional tactics, can trigger conventional military responses from countries to address terrorist threats. In addition, intelligence warfare involves military operations to gather information or destroy enemy intelligence networks.

The Rational Choice Theory (RCT) approach in security analysis assumes that actors in war, whether states, individuals, or companies, act rationally to maximize their benefits. Boudon (2003), explains that RCT allows for an understanding of strategic decisions in conventional warfare by considering the rational interests of these actors. Indrawan (2016), adds that conventional warfare involves military forces and weapons with the aim of achieving maximum benefits according to existing rules, describing the conflict as a form of direct warfare that is well-structured and organized.

Unconventional warfare includes forms of warfare that do not follow traditional or conventional rules, often involving more complex and diverse tactics. In unconventional warfare, methods such as cyber-attacks or unstructured strategies become more dominant. Examples include asymmetric warfare, where the parties involved have a large difference in military strength; the weaker party uses unconventional tactics to fight a larger force, such as in a conflict between guerrilla fighters and regular armies. Hybrid warfare combines conventional and unconventional warfare techniques, including information warfare, to create confusion and weaken the enemy through various methods, both on the physical battlefield and in propaganda.

Network Centric Warfare (NCW) focuses on the advantages of information and communication technology to increase the effectiveness of military operations, prioritizing the use of technology for better coordination and combat power. Meanwhile, cyber warfare involves the use of information technology to attack and damage enemy information systems and infrastructure, with the aim of destroying data, disrupting command and control systems, and creating economic and political instability. The cyber warfare is increasingly significant, showing a broad impact on national security that covers various aspects of life.

Russia and Ukraine Cyber War Conflict

The Russian-Ukrainian dispute has been going on since 1991 when Leonid Kravchuk declared Ukraine's independence from the Soviet Union. The problem was due to differences in political priorities during the Ukrainian presidency in 1991, and separatist groups also emerged in the Luhansk and Donetsk regions. Then, in 1992, NATO began to consider reuniting the Eastern European and Asian allies, and since then, Ukraine has officially wanted to join NATO even though it has not done so. After that, in 1999, Leonid Kutsma, who was seen from the communist side, was seen as a strong president and able to represent the people. Viktor Yanukovych was nominated for president in 2004. Still, the election process was complicated and resulted in the emergence of a social movement known as the Orange Revolution, which confirmed the legitimacy of Yanukovych's election. In 2005, Viktor Yushchenko was elected president of Ukraine. He was pro-European and pro-Western, and he believed that Ukraine would leave the Russian border region to be closer to NATO and the European Union. Viktor Yanukovych was elected president of Ukraine in 2010 after NATO contacted the country in 2008 to join as an ally in the post-Cold War era, and Russia complied with the request. At the beginning of the negotiations, Ukraine and Russia managed to reach an understanding regarding the price of gas that was too high for the Russian fleet to invest in the Ukrainian Black Sea port area. Not only that, Ukraine also received benefits offered by Russia because it had previously experienced a crisis due to the transfer of gas from the Russian Gazprom company to Ukraine for several months.

Business and social cooperation between Ukraine and the European Union continued under Yanukovych's leadership. This issue had an impact on strengthening economic relations between Russia and Ukraine in 2013. In 2014, Viktor Yanukovych resigned from his position as president of Ukraine because of the Maidan rebellion; the reason why this revolutionary generation began was that Yanukovych was ordered to overthrow the Association Agreement; then, in 2014, Russia launched an invasion of Crimea after a referendum was held on March 16. Russia, Ukraine, Israel, and France began to heat up because of this to produce a ceasefire agreement in these areas. The Minsk agreement in the Donbas conflict of 2016-2017 has continued. In 2014, Ukraine experienced a relatively sizeable cyber attack by Russia, and many aspects of Ukrainian statehood were detrimental; relations between countries did not improve only because of this; Russia quite often launched small and large-scale cyber attacks on Ukraine at that time (Jaswal, 2015).

In 2022, the Russian and Ukrainian war is still ongoing; the invasion carried out by Russia against Ukraine has been going on for quite a long time, and several diplomatic initiatives are being carried out, including a meeting in mid-January 2022 between the United States, NATO, and Russia for security and cooperation purposes in Europe. At this meeting, Russia submitted a proposal for a security guarantee to prevent Ukraine from joining NATO, but NATO and the United States rejected the proposal submitted; this meeting did not produce any results, and Russia did not want to withdraw its troops from the borders of Ukraine. In February 2022, Russia wanted to move its citizens from the border area, but according to NATO, there is still no objective evidence that Russia will continue to withdraw its troops. It is known that NATO is currently considering plans to use more aircraft, such as ships and fighter jets, to help with security and defense in Eastern Europe (Iswardhana, 2022).

Based on the discussion above, the theory of strategy and state security is critical in defending its territory. Russia sees that if Ukraine joins NATO, Russia will experience a threat because, geographically, Ukraine is a country that has the largest supply of wheat and grain in the world. Russia feels that the territory of Ukraine is part of Russia, and both countries have different perspectives on the geographical location of their territory. Hence, the invasion conflict becomes the path taken in the struggle for territory. Ukraine intensely feels the threat to state security, the pressure that Russia continues to give in military and non-military wars.

The situation is getting worse. Vladimir Putin, as president of Russia, has warned of the dangers of planning a war against Ukraine and has outlined a plan to deal with the cyber crisis

https://doi.org/10.35308/jpp.v10i2.9026

where Russia will use information technology, internet infrastructure, and mobile phones to disrupt the Ukrainian government's information system.

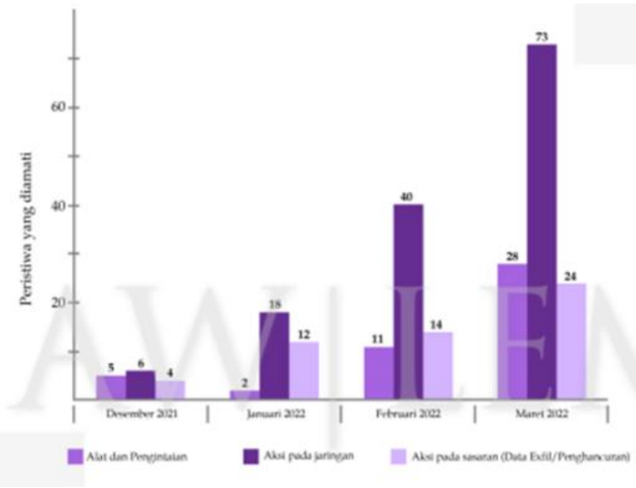

Figure 1. Russian Cyber Operations in Ukraine (December-March 2022)

The data above shows that in the conflict between Russia and Ukraine, cyber operations were carried out by Russia and increased from the end of 2021 to March 2022. The table shows that there were cyber attacks by Russia starting from tools and reconnaissance, network actions, and data destruction. This means that Russia has carried out many cyber attacks on networks against Ukraine in a short period, and there was an increase in March 2022. Despite having a border with Ukraine, Russia continues to dominate the region during the invasion with the aim of developing cyber operations to multiply the effectiveness of more conventional armed forces components. In terms of international competition, Russia is a heavyweight country or a country with the most advanced cyber capabilities. Discussing technology, Russia is indeed not as advanced as the United States, but in terms of cyber capabilities, Russia is a threat to other countries or is its ally. As for other countries with the most significant cyber capabilities, namely (including the US, China, Iran, Central and East Korea, West England, Israel, and Japan), Russia is the country with the most advanced cyber capabilities. Russia has been involved in cyber warfare with neighboring countries in Southeastern Europe, notably Estonia in 2007 and Georgia in 2008 (Kansas: School of Advanced Military Studies US Army Command and General Staff College FortLeavenworth, 2009).

War Strategy Used in the Russia-Ukraine Conflict

a. Formation of Hacker Groups

Russia

Russian hacking groups carried out cyberattacks on Ukrainian military and civilian Facebook accounts to undermine their combat capabilities and prevent access to information. The activity of these groups, which are linked to the Russian and Belarusian governments, reportedly increased shortly before the attacks. The group's strategy was to pose as journalists for independent news sites to encourage positive discussion about Russia, and hackers attempted to hack several Ukrainian military Facebook accounts in a coordinated campaign to remove criticism of Russia from social media. Mark Zuckerberg's Meta company explained that a group of people known as "Ghostwriters" were connected to Belarus by people online. Moreover, it said that this group has succeeded in several cases; the group posted videos calling on the military to surrender as if these posts came from legitimate account owners. Then, in February 2022, on the same day that Russia began its invasion of Ukraine, there were news reports in Polish and English about Ukrainian state troops that had left without warning and its leaders leaving the country. The fake reports went into detail about the topic of enemy accounts being compromised by social media. Mark Zuckerberg's company claims that around 200 accounts operated by Russians often post fake reports. This strategy is known as mass reporting, which is usually used by people who choose to hack social media accounts. The founder of the Ukrainian organization Digital Security Lab claims that the Russian invasion caused a significant threat to social media accounts through widespread public opinion (Krisdamarjati, 2022).

Russia has permission from the Conti group to launch attacks on its citizens. This group has a command channel connected to the Russian government. The Heimdal Security page states that the Russia-based Conti Ransomware uses the name Wizard Spider. Because of its ability to quickly copy data and enter other systems, these intruders are known as destructive actors. In addition, Alphabet Inc's Google detected Russian hackers known to law enforcement, including FancyBear, playing a role in phishing campaigns, espionage, and other attacks targeting Ukraine and its allies (Giovani, 2022; Natisha, 2022). The hacking group built by Russia has caused anxiety among Ukrainian civilians; the information and public opinion that is widely disseminated will cause significant threats to social media accounts; the strategy carried out by Russia aims to bring the thoughts of the Ukrainian people to the opposite direction and make the Ukrainian army feel threatened.

Ukraine

The Ukrainian IT Army is a group of hackers who have been active since the beginning of the conflict between Russia and Ukraine to help Russian rebels. Prior to this, the first stage of the Ukrainian IT Army's attacks managed to turn off the website of a significant alcohol distribution, the Moscow Stock Exchange, and several Russian banks. Media and government websites that have suffered from hacking include the All-Russia State Television, Radio Broadcasting Company (VGTRK), and the live-streaming platform Smotrim. The incident was when Russian President Vladimir Putin delivered his speech via live streaming before the Russian parliamentary assembly. At the same time, journalists in various locations complained that they could not access the broadcast at various points. In addition, around 308,000 people have joined a Telegram group known as the "Ukrainian IT Army." The group focuses on disrupting Russian websites, preventing disinformation, and getting accurate information to Russian citizens. One tactic used by the group is attacks that try to make targeted websites inaccessible by flooding them with online traffic (Valqa, 2022). Based on the theory of state strategy and security in viewing the cyber conflict between Russia and Ukraine, the roles played by both countries are the same: both want to maintain a state security sovereignty with techniques or strategies taken through hacker groups formed to disrupt information traffic and create anxiety for soldiers and civilians for both countries. These Cyber Attacks sometimes not only reduce the function of the organization in question but also try to disrupt citizens' access to critical information and public services and aim to reduce public trust.

https://doi.org/10.35308/jpp.v10i2.9026

b. *Distributed denial of service*

Distributed denial-of-service (DDoS) attacks target websites and servers by disrupting network services. DDoS attacks attempt to exhaust application resources. The perpetrators behind these attacks flood sites with false information, making the website's functionality poor or inaccessible. These attacks are usually aimed at attacking technology and information systems belonging to infrastructure. Attacks are carried out by sending Distributed Denial of Service (DDoS), which aims to hinder the work of a service on a large scale (Golose, 2015). The danger of DDoS attacks is one of the most serious in recent cyber events. Compared to the first year of 2021, the number of DDoS attacks in 2022 increased by 25%, making it much more frequent. The events mentioned above also state that the specific duration of DDoS attacks is long, especially those aimed at state resources and banks. DDoS attacks themselves are designed to damage network resources used by businesses and organizations, as well as government systems, so that they cannot function properly. This attack virus will disrupt the operation of the internet network by distributing large amounts of data to each web system so that the website or web system is disrupted and even the information distributed is incorrect and makes it difficult for the government service system to disseminate information to the public (Microsoft.com, 2022). This attack is dangerous if the system being attacked is a system in the government or financial sector; if this service is not available, it will have a broad impact on the life of the country. The first year of 2022 saw an increase on February 13 in response to the crisis in Ukraine. These activities are carried out on a smaller or larger scale.

Russia

Russia's strategy in the cyberattack on Ukraine is using DDoS, with the Distributed-Denial-of-Service (DDoS) attack that began by making Ukrainian government websites inaccessible, then spreading to the entire internet infrastructure around the world. A DDoS attack takes down a website by overwhelming its systems. Around 70 websites in Ukraine were targeted. After the DDoS attack, two banks and the Ukrainian Ministry of Defense were inaccessible, leaving them unable to access their websites and online banking services. The cyber incident came after Russia announced that it was preparing to launch exercises near a point of contact with Ukraine. The goal of a DDoS attack, also known as a distributed denial-of-service attack, is to disrupt the usual internet connectivity of a targeted server, service, or internet backbone.

DDoS attacks are practical by using multiple computer systems that have been configured to act as the source of the attack before it has time to spread. Other computers and types of power grids, such as IoT networks, can be compromised by the exploited machines. IoT, often known as the Internet of Things, is a concept or software program that allows a physical object to send or receive data over a network without using a computer or human. Four hours later, the site was still inaccessible. At the same time, two banks also experienced cyber attacks that disrupted ATM services offline and made it difficult for customers to withdraw or transfer funds online (Wibowo, 2022). The cyber attack has an impact on a threat to Ukraine's national security, and Russia's actions aim to disrupt Ukraine's internal communications so that concerns and anxieties can occur in Ukraine. This attack makes the security issue increasingly complex. However, over time, non-military aspects can now also be classified as an agenda that focuses on security issues.

Ukraine

However, Ukraine's strategy also threatens Russia with a related cyberattack known as DDoS. Sites such as Mil.ru and Kremlin.ru, which are on the backbone of the Russian Internet, have experienced a lack of service or content on the backbone. In addition, every Internet block that hosts Kremlin.ru or Putin's Presidential Palace website has been taken down due to a DDoS (distributed denial of service) attack launched by Ukrainian hackers. In addition to the presidential palace website, government-related sites, and Russian state-affiliated media have also experienced system errors. This has caused problems with telephone and internet networks. In addition, Ukraine's strategy to disrupt Russia is to develop an IT sector focused on hacking, and more than 250,000 Ukrainian community members have joined it. One of the goals of this initiative is to disrupt Russian government websites. Volunteer groups use software that allows mobile phone and computer owners to participate in various Russian services to carry out denial of service. Hackers have also created bots on the Telegram messaging platform with the ability to block information. The bot-master is the main computer or controller that controls other computers because it has been infected with malicious code in the form of viruses so that it cannot be accessed by the public. In addition, Ukrainian hacker troops in their system services also offer the ability to reach people to people in Russia with phone calls, emails, and text messages, as well as send videos and pictures of dead soldiers from the invasion troops from a virtual call center. Some of them created websites where Russian citizens could see photos of other Russian citizens who were captured to see their own sons. The software dubbed "Liberator" allows anyone with a digital connection to become part of a DDoS network or botnet (Oktarianisa, 2022).

Based on the explanation above, Russia is a country that has great potential in terms of cyber warfare. The strategies owned by Russia and Ukraine in this conflict both have a role to be able to defend their respective countries, and the strategies taken by both countries choose to carry out attacks by taking into account all attacks carried out, strategies to make the system error and damage data and use the method of sending videos and photos by utilizing websites to threaten Russian and Ukrainian citizens in terms of defending their countries from threats from other countries. The concept of Cyber Security in the conflict that occurred in these two countries both strive to ensure the achievement and maintenance of the concept of state telecommunications system security and ensure the security of user assets can be protected, but Russia and Ukraine chose to attack each other in Cyberspace, the aim is to protect all state assets from every attack, and maintain the integrity of information spread in society in war conditions (Suryokusumo, 2016). The availability of human resources owned by Russia is more dominant in forming a hacker force to fight Ukraine, and the availability of technological tools owned by Russia has an impact on the smoothness of cyber attacks on Ukraine, as well as an activity with the intention of protecting computer system devices and network devices and state-owned data from various types of cyber attacks is the concept of cyber security in maintaining state security from cyber attacks that is what is done by Russia and Ukraine.

https://doi.org/10.35308/jpp.v10i2.9026

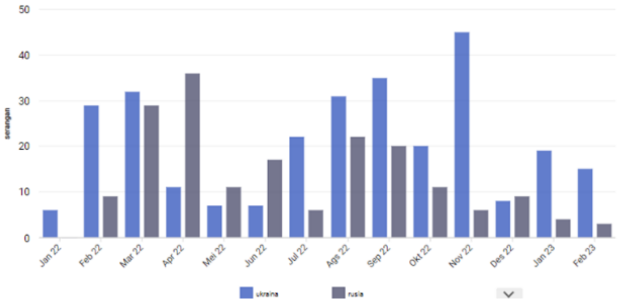

Figure 2. Number of Cyber Attacks Received Russia and Ukraine (2022-2023)

Source: CyberPeace Institute

It can be analyzed from the data above that the total attacks received by Ukraine reached 280 attacks throughout January 2022-February 2023. In the same period, Russia was recorded as receiving 183 attacks, and the attacks received by Ukraine were in the form of DDoS, malware, phishing, hack and leak, wiper, and ransomware. The attacks launched against Ukraine were caught by several names, such as Anonymous Russia, Russian Hackers Team, Clowns, NoName057, People's CyberArmy, XakNet, and many more. The threats were dominated by disruption, but there were other attacks, such as data leaks and as many as two incidents. However, at that time, incidents had decreased by 45.8% compared to the previous quarter. One of the significant attacks occurred on November 8, 2022, namely pro-Ukrainian perpetrators suspected of carrying out hacking and data leak operations against Russian social media video services. At least four files containing two million lines of cellphone data and citizen device information were published through an open site that the public could access. Another cyberattack was the defacement of 7 Russian district administration sites. Ukrainian IT forces broadcast the New Year's address of Ukrainian President Volodymyr Zelenskyy on the website on December 31, 2022 (Erlina, 2023).

Effectiveness of Russia's Cyber Warfare Strategies in the Russia-Ukraine Conflict

This study reveals that Russia's cyber warfare strategies during the 2021-2022 conflict with Ukraine were highly effective in causing significant disruptions to Ukraine's critical infrastructure. Distributed Denial of Service (DDoS) attacks, government system hacks, and data infiltrations were integral parts of Russia's comprehensive strategy to undermine Ukraine's capacity to respond to both military and economic threats.

One of the most significant cyberattacks, WhisperGate, launched in early 2022, targeted and destroyed data on various Ukrainian government websites. This attack not only compromised data integrity but also disrupted communication channels and hampered Ukraine's government responses during the conflict escalation. WhisperGate's impact extended beyond mere technical dysfunction, delivering a psychological blow by exposing the vulnerability of Ukraine's systems to cyber threats. According to analysis, the damage caused by WhisperGate was comparable to a physical attack on critical infrastructure, but with far fewer risks for Russia.

In addition, Russia employed state-sponsored hacking groups such as Fancy Bear and Sandworm to enhance the scope and effectiveness of their attacks. These groups did not merely carry out cyberattacks but acted as strategic instruments designed to weaken critical sectors, such as banking, energy, and transportation infrastructure. The scope of these attacks extended beyond government agencies to include private sector entities, illustrating that cyber warfare serves not only to weaken a nation's military capabilities but also its economic and social structures. The effectiveness of these strategies is evident in the significant disruptions caused across various sectors in Ukraine. The financial system, in particular, faced repeated assaults, with the NotPetya ransomware in previous years setting a precedent for broader tactics. This attack crippled Ukraine's financial institutions, creating economic chaos and eroding public trust in the government's ability to protect vital data and resources.

In the face of intense cyberattacks, Ukraine sought to bolster its cyber defenses through international cooperation and domestic efforts. Despite Ukraine's technological inferiority compared to Russia, support from international partners such as NATO and the European Union helped mitigate the impact of some attacks. Ukraine also strengthened its cyber defenses by implementing rapid mitigation measures, including enhancing data encryption, patching system vulnerabilities, and improving incident response times. However, these efforts were not entirely successful in neutralizing the ongoing cyber threats from Russia. One of the biggest challenges for Ukraine was the asymmetric nature of cyber warfare, where Russia, with its more advanced technological capabilities, was able to launch attacks that were harder to detect and defend against. Ukraine's reliance on vulnerable digital infrastructure, particularly in its communication and governance systems, became a key weakness exploited by Russia.

The implications of these findings extend beyond Ukraine's national security and raise broader concerns for global security. Cyber warfare has demonstrated its potential to disrupt global stability, as attacks on one nation can have far-reaching consequences for regional security and economic systems. Cybersecurity is now central to national defense strategies, not only for countries directly involved in conflicts like Ukraine but for all nations increasingly aware of their vulnerability to cyberattacks in the digital age. The Russia-Ukraine conflict serves as a crucial lesson that modern warfare is no longer confined to physical battlefields, but increasingly takes place in the digital realm. Cyberattacks can disable critical infrastructure, paralyze government functions, and weaken a nation's economy without the need for traditional military forces. The involvement of non-state actors, such as state-backed hacker groups, further expands the scope of the threat, making it more difficult to detect and prevent.

As nations become more reliant on digital infrastructure, the findings of this study highlight the urgent need for stronger cybersecurity defense strategies and international collaboration to address cyber threats. Moreover, the study suggests that countries must adapt their defense strategies to respond to the evolving threats posed by cyber warfare. Without adequate preparation, cyberattacks like those executed by Russia against Ukraine could be replicated elsewhere, posing significant risks to global security. This conflict serves as a stark warning to the international community that cyber warfare has become one of the most efficient and destructive forms of warfare in the modern era, and nations that fail to recognize this threat are at great risk.

CONCLUSION

This study concludes that cyber warfare strategies play a crucial role in modern conflicts, as demonstrated by the 2021-2022 conflict between Russia and Ukraine. In this conflict, advancements in information and communication technology were employed to implement non-military strategies such as Distributed Denial of Service (DDoS) attacks and the formation of hacker groups, effectively damaging government systems and national infrastructure. Russia's superior cyber capabilities made Ukraine an easy target for attacks that disrupted communication and weakened the opponent at a low cost, yet with significant impact, comparable to traditional military strategies. The conflict highlights how cyber strategies can be used to achieve national interests more efficiently and underscores the importance of cyber security in safeguarding national security in the modern era. Furthermore, this study serves as a warning to other nations about the vulnerabilities in their cyber defenses, given the significant potential of cyber attacks in future conflicts.

This research has several limitations, including the restriction in generalizing the findings due to the descriptive and qualitative approach used, and the reliance on open-source data and media reports, which may introduce information bias. Additionally, the study does not delve into the technical aspects of the cyber attacks, leaving a limited understanding of how these attacks were designed and executed. Further research is needed to address these limitations and explore the evolution of cyber warfare strategies in greater depth.

REFERENCES

Boudon, R. (2003). *Beyond rational choice theory. Annual review of sociology, 29(1), 1-21.*

Chrisnandi, Y. (2019). *Dari Kyiv Menulis Indonesia.*

Clausewitz, Von C. (2021). *On War (Vom Kriege). e-artnow.*

Erlina, E. (2023). *Setahun Perang, Serangan Siber yang Diterima Ukraina Lebih Banyak Ketimbang Rusia*. https://databoks.katadata.co.id/datapublish/2023/02/24/setahun-perang-serangan-siber-yang-diterima-ukraina-lebih-banyak-ketimbang-rusia

Giovani. (2022). *Grup Ransomware Conti Siap Serang Balik Musuh yang Lakukan Serangan Siber ke Rusia*. Liputan6.Com.

Golose, P. R. (2015). *Invasi terorisme ke cyberspace.*

Indrawan, J. (2016). *Studi Strategis dan Keamanan*. Depok: nadi pustaka.

Iswardhana, M. R. (2022). Sejarah Invasi Rusia di Ukraina Dalam Kaca Mata Geopolitik. *Isu-Isu Kontemporer Internasional Konflik Rusia - Ukraina: Realisme Politik.* http://eprints.uty.ac.id/11192/

Jaswal, V. S. (2015). *.Kejahatan Cyber dan Teknologi Informasi.*

Jennex, M. E. (2007). Cyber war defense: Systems development with integrated security. In *Cyber Warfare and Cyber Terrorism* (pp. 241–253). IGI Global. https://doi.org/10.4018/978-1-59140-991-5.ch029

Kelly, M. (2019). Language and new forms of warfare. In *The Palgrave Handbook of Languages and Conflict* (pp. 481–498). Springer International Publishing. https://doi.org/10.1007/978-3-030-04825-9_22

Kirshner, J. (2006). Globalization and national security. In *Globalization and National Security*. https://doi.org/10.4324/9780203943762

Krisdamarjati, Y. A. (2022). *Media Sosial, Medan Propaganda Ukraina-Rusia*. Kompas. https://www.kompas.id/baca/linimasa/2022/03/09/media-sosial-medan-propaganda-ukraina-rusia-1

Maskun. (2013). *Kejahatan Siber-Cyber Crime-Suatu Pengantar*. Kencana Prenada Media Group.

Microsoft.com. (2022). *Serangan DDoS ditentukan*. https://www.microsoft.com/id-id/security/business/security-101/what-is-a-ddos-attack

Natisha. (2022). *Kelompok ransomware Conti akan serang musuh Rusia*. Antara News. https://kalbar.antaranews.com/berita/505929/kelompok-ransomware-conti-akan-serang-musuh-rusia

Niagahoster. (2021). Cyber Security: Panduan Lengkap dan Penerapannya. In *Cyber Security: Panduan Lengkap dan Penerapannya* (p. 1). https://www.niagahoster.co.id/blog/cyber-security-adalah/

Oktarianisa, S. (2022). *Kronologi dan Latar Belakang Konflik Rusia dan Ukraina*. CNBC Indonesia. https://www.cnbcindonesia.com/news/20220304134216-4-320044/kronologi-dan-latar-belakang-konflik-rusia-dan-ukraina/1

Pool, P. (2013). *War of the Cyber World: The Law of Cyber Warfare*. International Lawyer. http://anu.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwXV07CgJRDHxYayPoLZ6Yj4mpxcUD7AXy9hm7rbw_ZkUQLRNShmEGZphSCA_H-ocJaEHNyDoKTmcmF_ek-hIttxr80w2z_uLVsC2r-7wr43AdL7f66QeoDzGo1sxl0vBYhJZjGDF2npS9Q2AzVAlQ6QR5lkQgB7b80XZS7qCwLxtfbOTz8x036y82GC5k%5Cnwww

Relia, S. (2016). *Cyber warfare: its implications on national security. Vij Books India Pvt Ltd.*

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Suryokusumo, S. (2016). *Konsep sistem pertahanan nonmiliter: suatu sistem pertahanan komplemen sistem pertahanan militer dalam pertahanan rakyat semesta*. https://books.google.co.id/books?hl=en&lr=&id=94BMDAAAQBAJ&oi=fnd&pg=PA9&dq=jurnal+tentang+pertahanan+nirmiliter&ots=fk3gRgH5p0&sig=kw6k72Sf4QZbD3CRQPRZwYMv6XM&redir_esc=y#v=onepage&q&f=false

Thornton, Rod. (2020). Fourth Generation: A 'new' form of 'warfare'? In *Global Insurgency and the Future of Armed Conflict* (pp. 97–104). Routledge. https://doi.org/10.4324/9780203089279-18

Valqa, A. (2022). *Serangan Rusia ke Ukraina Picu Perang Hacker Pertama di Dunia*. https://www.dexpert.co.id/serangan-rusia-ke-ukraina-picu-perang-hacker-pertama-di-dunia

Welch, E. W., & Feeney, M. K. (2014). Technology in government: How organizational culture mediates information and communication technology outcomes. *Government Information Quarterly*, *31*(4), 506–512. https://doi.org/10.1016/j.giq.2014.07.006

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security. Cengage learning.*

Wibowo, W. (2022). *2 Bank dan Kementerian Pertahanan Ukraina Lumpuh Terkena Serangan Siber DDoS Artikel ini telah diterbitkan di halaman SINDOnews.com pada oleh dengan judul "2 Bank dan Kementerian Pertahanan Ukraina Lumpuh Terkena Serangan Siber DDoS"*. Sindonews.Com. https://tekno.sindonews.com/read/687343/207/2-bank-dan-kementerian-pertahanan-ukraina-lumpuh-terkena-serangan-siber-ddos-1644969771

https://doi.org/10.35308/jpp.v10i2.9026