Politeia : Journal of Public Administration and Political Science and International Relations
E-ISSN : 3031-3929
Volume. 3 Issue 3 July 2025
Page No: 157-172

Analyzing Russia's Hybrid Warfare Strategy through HermeticWiper Against Ukraine: A Cybersecurity and Desecuritization Approach

Muhammad Haekal Zulfian[1], Yanuar Rahmadan[2]
Universitas 17 Agustus 1945 Jakarta, Indonesia
Correspondent: mhdzulfian96@gmail.com

Received : June 05, 2025
Accepted : June 19, 2025
Published : July 30, 2025

Citation: Zulfian, M, H., & Rahmadan, Y. (2021). Analyzing Russia's Hybrid Warfare Strategy through HermeticWiper Against Ukraine: A Cybersecurity and Desecuritization Approach. Politeia : Journal of Public Administration and Political Science and International Relations, 3(3), 157-172.

ABSTRACT: This study examines Russia's deployment of HermeticWiper malware in the early hours preceding the 2022 full-scale invasion of Ukraine as part of a broader hybrid warfare strategy. Unlike conventional cyberattacks focused on espionage or financial gain, HermeticWiper was designed to irreversibly destroy digital infrastructure, disrupting governance, finance, and communication sectors. Using a qualitative case study method with secondary data from technical reports, academic literature, and verified media, the study finds that the malware was strategically aligned with military objectives. Despite the destructive intent, Ukraine demonstrated significant cyber resilience through formal institutional responses and collaborations with Microsoft, ESET, and its volunteer-based IT Army. The study applies the National Cybersecurity Strategy framework and Desecuritization Theory to highlight how Ukraine addressed the threat without escalating the conflict. These findings illustrate a paradigmatic shift in modern warfare, where digital domains play a central role in national defense.

Keywords: HermeticWiper, Hybrid Warfare, Cyber Resilience, Ukraine, Cybersecurity Strategy, Desecuritization

INTRODUCTION

The development of the times from year to year continues to change and it also affects the trend of war that occurs to date (Samad, 2022). In the digital era, technological advancements have fundamentally reshaped the dynamics of international conflict. Warfare is no longer confined to traditional battlefields but extends into cyberspace, where attacks can target state institutions, financial systems, and civilian infrastructure. A key example is the Russia-Ukraine conflict, which has demonstrated the increasing integration of cyber operations into military strategy. With the global focus on physical conflict increasing, Russia's coordinated cyberattacksespecially the use of HermeticWiper reflect a shift similar to modern warfare. . Unlike typical malware aimed at data theft or economic sabotage, HermeticWiper was a destructive cyberweapon designed to cause irreversible damage to Ukraine's critical infrastructure. The timing of this cyberattack, which

occurred just hours before Russia's full-scale invasion on February 24, 2022, suggests a high level of synchronization between cyber and kinetic operations.

However,Existing literature tends to emphasize the broader consequences of cyber warfare or the role of non-state actors, with limited analysis of how cyber tools operate in the context of hybrid warfare and how target states react without escalating the conflict.. This study fills that gap by examining HermeticWiper not only as a digital attack but also as a strategic element of Russia's hybrid warfare and Ukraine's institutional and collaborative responses as acts of desecuritization. (Aris Hardinanto, 2024). The digital era is a condition where human life is carried out with digital technology. as a development of the communication technology revolution, while cyber warfare is a condition of conflict using the development of information and communication technology. Cyber war is a social phenomenon in international relations that has become a serious problem for nations in the world in building international stability (AM, 2021). The use of technology in the international sphere has developed at the level of rapid progress which makes every information play an important role in the government system. Each country no longer makes technological sophistication a means of clarifying developed countries, but as part of controlling relations between countries, including conflicts and wars that have substantially shifted to a more modern way. In this case, technology and information have indirectly created a new era of warfare. As a result, wars that occur no longer only use military force, but every country is now able to create threats and chaos for the sovereignty of other countries through sabotage and information espionage, especially in terms of defense and security (Karisma, 2023).

In recent years, cyber threats have emerged as a new dimension in cyberspace or digital space. Cyberspace includes attacks and operations conducted through computers, networks and information systems. These actions, such as hacking, cyberattacks, and data manipulation, can compromise the information infrastructure, security, and stability of a country or organization (Khoirunnisa Khoirunnisa, 2025).

Cyber warfare can involve organizations, companies, and the military in destroying or attacking the computer systems of other countries or other parties, as Russia integrates cyber warfare as a broader military and security strategy to make cyberspace a 'battlefield'. As the preparation of the strategy launched by Russia, where IO information operations and asymmetrical military Russian tactics are used to disrupt the government of other countries, organize anti-government in their own country, deceive opponents, influence public opinion, and reduce an interest from other countries to fight it (Junior & D, 2024). Since the overthrow of Viktor Yanukovych's leadership by pro-Western Ukrainians, until the change of new leadership, relations between Russia and Ukraine began to experience ups and downs(Setiyono, 2024). The cyberattack carried out by Russian hacker groups in Ukraine is one form of attack that is related to the international armed conflict between Russia and Ukraine (Sya'roni, 2019).

One example is the cyberattacks carried out by Russia against Ukraine, which have increased in recent years. The year 2022 became one of the periods that marked the escalation of cyber conflict between Russia and Ukraine, with the emergence of a fairly complex attack, namely the use of HermeticWiper malware. HermeticWiper is known as a ransomware malware designed to

permanently damage and delete data on the target computer system. This attack shows the existence of a cyber warfare strategy from Russia that is not only a physical attack on the battlefield, but also a digital attack targeting Ukraine's critical infrastructure, Disk wiper is one type of malware that is often used to attack Ukraine. The implementation and quality of such wipers vary, and may require different developers. The day before the Russian troop invasion of Ukraine on February 24, a new data wiper was discovered that was used to attack a number of Ukrainian entities. The malware was named "HermeticWiper" after a digital certificate stolen from a company called Hermetica Digital Ltd.

The wiper is remarkable for its ability to bypass Windows security features and gain write access to many low-level data structures on the disk. In addition, the attackers wanted to fragment the files on the disk and overwrite them making recovery impossible. On February 23, 2022, just one day before the start of Russia's full military invasion of Ukraine, a destructive cyber campaign was launched using the *HermeticWiper* malware. This attack targeted a number of Ukrainian governmental and private sector organizations, with the primary goal of destroying data and crippling information technology systems. Different from typical cyberattacks aimed at data theft or economic gain, *HermeticWiper* exhibits the characteristics of a cyberweapon designed to create massive chaos and operational instability.

The operational method of cyber warfare weapons is generally carried out through the spread of malicious computer viruses, known as "Malware", which includes computer viruses with many forms of malicious devices including worms, computers, trojan horses, and other software. The attack is a continuation of the pattern of cyber aggression that has been going on for a long time, as seen in the *NotPetya* case in 2017, which was also accused of being carried out by Russian state actors. In the context of modern warfare, cyberattacks have evolved into an integral part of military and political strategy, with cyberspace becoming a battlefield of equal importance to land, sea and air. On June 27, 2017, the first NotPetya attack was launched by Russia against Ukraine, which began with an attack on a major Ukrainian bank that reported an infection of its network. The following day it was reported that NotPetya also affected Kiev's Borispol airport and energy companies Kyivernergo and Ukrenergo. 21 NotPetya malware has the goal of destroying files (Afiah, 2021). For Ukraine, the constant cyber threats from Russia are proof that the conflict is no longer limited to the physical realm, but also targets the economic foundations and digital infrastructure of the country.

The immediate impact of these attacks was a significant disruption to the information technology infrastructure in Ukraine. Many institutions were unable to access their critical data, resulting in delays in public services and difficulties in administrative decision-making. This was exacerbated by the concurrent military invasion, making the HermeticWiper attack part of a hybrid warfare strategy, combining military force and digital attacks to maximize the disruptive effect on the opposing country. The objective of this research is to analyze the deployment of HermeticWiper malware by Russia as part of its hybrid warfare strategy against Ukraine, and to examine Ukraine's institutional and collaborative responses within the frameworks of the National Cybersecurity Strategy and Desecuritization Theory. This journal discusses how the characteristics and patterns of *HermeticWiper* attacks carried out by Russia against Ukraine's digital infrastructure ? and how the influence of HermeticWiper attacks on the de-escalation process of the Russia-Ukraine conflict ?.

The concept of CyberSecurity is then developed where according to Saco and Deibert the threat of cybersecurity has also violated national boundaries so that it threatens internationally. This is due to the increasingly high interaction of people through cyberspace due to technological advances and the information age. In contrast, Deibert's opinion explains that cybersecurity is based on four separate discourses with different reference objects, threats, policy choices, and orders, which include national security, state security (consisting of external threats to state sovereignty and internal threats to regime security), private security, and network security. This opinion is supported by Hansen and Nissenbaum where in the case of cybersecurity includes the relationship between "network" and "individual" as well as the human collective referent object so that there is no discourse on private security which is individual security as a referent object, but rather that the discourse of individual security is related to social and political referents (Hansen, 2009).

This research uses the National Cybersecurity Strategy framework as the main approach to understanding the HermeticWiper attack on Ukraine. This theory departs from the view that in the modern context, cybersecurity is not only a technical domain, but an integral part of the country's defense strategy), the reference objects of national cybersecurity include the country's digital infrastructure, government, and public stability that are targeted by external threats such as malware. In addition, the International Telecommunication Union (ITU) framework on cybersecurity emphasizes five key elements: legal, technical, organizational, capacity building, and international cooperation measures. Through this theory, this journal analyzes how Ukraine responded to the Russian attack through the integration of a national digital defense system, cross-sector collaboration, and increased cyber resilience within the country's policy framework.

This research uses the desecuritization theory framework developed by Barry Buzan, Ole Wæver, and Jaap de Wilde in the tradition of the Copenhagen School of Security Studies. This theory was first systematically formulated in their monumental work titled Security: A New Framework for Analysis (1998). In the book, Buzan et al. explain that security issues are not objective, but are formed through a social construction process called securitization. This process occurs when an actor (usually a political, military, or state elite) declares that an issue poses an existential threat to the referent object - be it the state, society, or other important values - thus requiring extraordinary measures beyond the norms of ordinary political policy. In this framework, a problem becomes a "security issue" not because it is naturally dangerous, but because it is successfully presented as a threat and accepted by the audience as something that requires an emergency response.

In contrast, Buzan et al. introduce the concept of desecuritization, which is the process of returning issues that have been securitized back into the normal political and handling processes. In other words, desecuritization means de-emergencyizing an issue, and managing it through routine institutional, legal or policy mechanisms. In their words:

"To desecuritize is to move issues out of emergency mode and into the normal bargaining process of the political sphere.". (Barry Buzan, 1998) . In the context of the HermeticWiper attack, Ukraine did not respond frantically to , but rather built a response framework through formal institutions, international collaboration, and cyber civil society participation. This demonstrates the process of desecuritization, where Ukraine managed to manage the threat without extending the conflict into the realm of repression.

METHOD

This research uses a qualitative method that focuses on an in-depth understanding of social phenomena through the analysis of non-numerical data, such as texts and documents (Malahati, 2023).

By collecting secondary data from sources such as academic journals, books and articles from credible media related to Cyber Security. With this method the author can build a fairly clear and comprehensive analysis of Cyber security in the International(Sulung, 2024).

The collection of materials in this study was mostly based on secondary sources, such as academic journals published periodically, technical reports from companies engaged in cybersecurity, such as Microsoft and ESET, official government publications, and internationally recognized news outlets. It is essential to have a thorough understanding of the material covered between 2021 and 2024 and that thoroughly examines the Hermetic Wiper malware, Russian cyberspace, or Ukraine's digital defense strategy. Sources that lack technical or academic credibility, such as unreliable news reports, political or biased commentary, are derived from the analysis. Political opinions or biased commentary are derived from the analysis.

The analysis was conducted using grouping of technical reports, journal articles, websites, news on the internet for patterns of answering problem formulations. The methodology allowed researchers to examine technical discussions regarding malware functionality. malware functionality. It instead positions cyber threats, such as Hermetic Wiper, within broader theoretical and strategic frameworks, reflecting the convergence of information technology, national security, and global political dynamics. Through an inductive and interpretive process, this qualitative study sheds light on how states manage non-traditional security threats in the digital age, using both institutional resilience and strategic cooperation.

The case study or qualitative approach is very suitable for this research, because *HermeticWiper* is a single phenomenon that has a special context, which was launched ahead of the Russian military invasion of Ukraine in February 2022. The study could include an analysis of how the malware spread, its mechanism for permanently deleting data, and how Ukraine's digital security system responded to the threat. Data may be collected through technical reports from cybersecurity companies such as ESET, Symantec or Palo Alto Networks, as well as reports from independent media and government institutions.

In this qualitative research, the research process is more important than the results. In qualitative research, the process becomes a very important thing to pay attention to, where the researcher as an instrument collector must be able to put himself in a position as objectively as possible so that the data collected becomes data that is able to be accounted for. qualitative research is a research

method used to research on natural conditions, (as opposed to experiments) where the researcher is the key instrument, data collection techniques are triangulated (combined), data analysis is inductive, and qualitative research results emphasize meaning rather than generalizations (Safarudin, 2023).

RESULT AND DISCUSSION

In this literature review or previous research entitled *THE PHENOMENA OF RUSSIAN SYMBOL ATTACK ON UKRAINE: AS LEARNING FOR INDONESIA IN THE DEVELOPMENT OF Cyberspace DEFENSE by (Dina Anjelina 2023)*. In this previous study, it has more or less the same background as the journal that I will research, namely the Russian cyber attack against Ukraine, but in this previous study it discusses how the cyber attack affected Indonesia. The high number of internet users opens up opportunities for cyber attacks, especially if data security is inadequate. The National Cyber and Crypto Agency (BSSN) noted that the total cyberattacks in Indonesia in 2022 reached 370.02 million attacks, showing an increase of about 38.72% compared to the previous year with this data it can be concluded that this research is important for Indonesia's anticipation of cyberattacks with the phenomenon of Rudsia's cyberattacks against Ukraine. The steps taken by Indonesia for learning cyber attacks according to this research are Increased awareness of cybersecurity and the application of encryption or cryptography techniques by individuals can be the first step in protecting data and information These steps reflect the implementation of the theory of cyber defense, which emphasizes the need to maintain the confidentiality, integrity and availability of state information. These efforts are supported by the Indonesian Ministry of Defense, 2014 on Cyber Defense Guidelines. Through this concrete step, it is hoped that Indonesia can continue to develop cyber defense to face threats in the era of rapidly evolving information technology.
In this previous research using the same research method as the journal that I will research, namely using a descriptive qualitative library research method by collecting data from books, journals, and internet news (Anjelina, 2023).

Then for the second previous research that I took was with the title *Significance of Cyber War in the Modern Russia-Ukraine Conflict Case Study: Wizard Spider - It Army by Imma Karisma1, (2023)*. In this study, the researcher discusses the Ukrainian government which formed a special organization in charge of handling cyber security and snooping on all forms of cyber-war attacks from Russia. The organization is known as the "IT Army" which consists of Ukrainian volunteers and international communities from around the world who have Underground hacker capabilities and are willing to protect the infrastructure of the Ukrainian state While from the Russian side itself has also long had a hacker organization that supports Russian cyber security in full. The organization is tasked with providing resistance to countries that are considered enemies of Russia known as the "Wizard Spider". The IT Army focuses on participating in cyber operations with Russia as the target. In this case, IT Army Ukraine can exploit advanced equipment to counter Russian cyber attacks including DDoS then Wizard Spider Organized groups and conduct cyber attacks through malware and ransomware attacks known as Conti or TrickBot to Ukraine. In this previous research, there are differences with the journal that I will study where this previous research

discusses the involvement of non-state actors, such as Wizard Spider (pro-Russia) and IT Army (pro-Ukraine). These groups play a major role in cyber warfare with attacks on critical infrastructure. While the journal that I will research discusses the destructive devices used by Russia to attack Ukraine's cyber security, namely using NotPetya and Sandworm devices.
Then for the research method used in this previous study, it is still the same as the one I used, namely the descriptive qualitative research method, namely finding information whose sources are from journals, news or the internet. (Karisma, 2023)
.

For the last previous research that I listed was with the title *Ukraine-Russia Conflict: Review of international humanitarian law on the involvement of foreign fighters by (Khoirunnisa Khoirunnisa, Brian Matthew, Didi Jubaidi, Agung Yudhistira Nugroho 2025)*. In this previous research, it discusses the role of foreign fighters who are pro-Ukraine and also the main challenge posed by the involvement of foreign fighters in Ukraine lies in the legal uncertainty surrounding their status under International Humanitarian Law (IHL). International humanitarian law (IHL), which governs the conduct of armed conflict and seeks to protect individuals who are not actively participating in hostilities, does not provide clear guidelines for foreign fighters. These fighters, who do not represent a recognized state or party to the conflict, do not clearly fall into categories such as lawful combatants or civilians, so their legal status is ambiguous, Foreign fighters are also an important factor on both sides of the conflict. People from various countries have joined the Ukrainian side, either as volunteers or part of organized military units, while Russia has provided support to pro-Russian factions, including the involvement of Russian foreign fighters (Khoirunnisa, 2025).

There are significant differences in the focus and scope of the analysis. This journal specifically addresses the technical characteristics and attack patterns of the HermeticWiper malware launched by Russia ahead of its invasion of Ukraine, as well as Ukraine's concrete response in strengthening its cyber defenses, including collaboration with companies such as Microsoft and ESET. The approach is more of an in-depth case analysis, oriented towards the strategic, technical and non-traditional security aspects faced by Ukraine during the conflict. This makes the journal relevant in illustrating the transition of conventional warfare to the cyber domain, as well as demonstrating the importance of digital resilience in the context of modern geopolitics.

In contrast, literature reviews such as Dina Anjelina's take a domestic perspective, namely how Russian cyberattacks against Ukraine can be a lesson for Indonesia in strengthening national cyber defenses. Meanwhile, research by Imma Karisma and Agussalim highlights the role of non-state actors in cyber conflict, such as the IT Army and Wizard Spider, so it has a different focus because it emphasizes the dynamics of participation of volunteer groups and underground hackers. Khoirunnisa's work examines the conflict from the perspective of international humanitarian law and the involvement of foreign fighters, which does not technically discuss malware or cyber attacks in depth. Therefore, Haekal's journal presents a more specific and technical approach to the HermeticWiper malware, as well as highlighting its direct effects in hybrid warfare strategies, making it different from the three literature reviews which are more broad and conceptual.

1. characteristics and patterns of Russia's *HermeticWiper* attacks on Ukraine's digital infrastructure

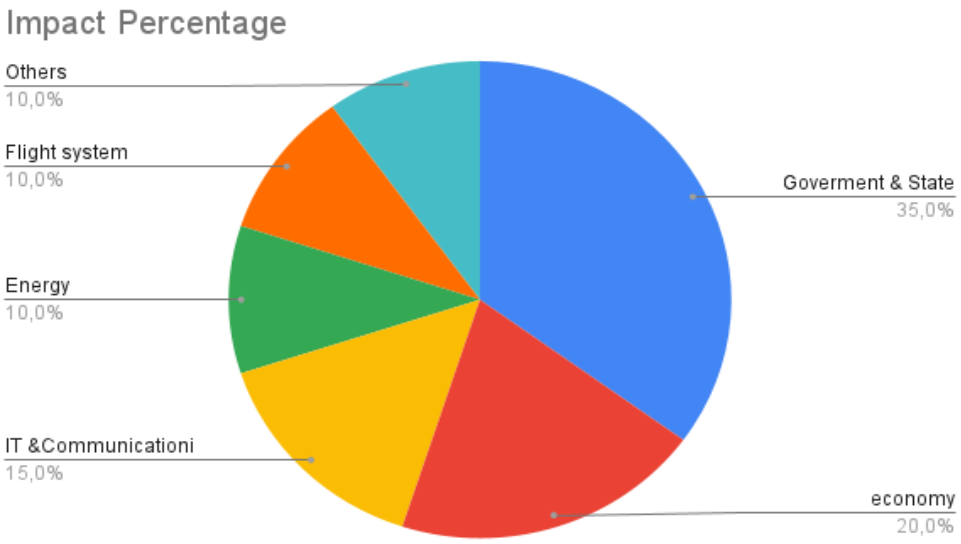
The development of digital technology has significantly changed the dynamics of international conflict, where threats are no longer limited to conventional military forces, but also extend to the cyber domain. In recent years, Russia has utilized cyber power as part of its military strategy against Ukraine. The cyberattacks are not only aimed at stealing information, but also at damaging vital infrastructure and weakening Ukraine's national security. As the conflict escalated, Russia launched different types of attacks, one of which was the use of destructive malware such as HermeticWiper designed to permanently delete data and paralyze the target's computer system. The Russia-Ukraine conflict involved both conventional and unconventional elements, including massive cyberattacks that included espionage, data theft, critical infrastructure sabotage, and propaganda dissemination (BUDIMAN, 2023). The culmination of these attacks occurred on February 24, 2022, coinciding with the start of Russia's open military invasion of Ukraine. Hours before the physical assault began, Russia launched a wave of cyberattacks targeting Ukraine's communications systems, satellites and public services. HermeticWiper was one of the main malware used in this series of attacks. Russia continued its cyberattacks until February 24, 2022 along with the military invasion. Ukraine continues to monitor attack patterns such as the HermeticWiper (2022) and NotPetya (2017) malware (Budiman, 2023). From the perspective of the National Cybersecurity Strategy framework, such attacks are not merely isolated technical incidents, but rather systematic threats to the nation's digital sovereignty. According to Hansen and Nissenbaum (2009), national cybersecurity is not only about protecting systems from harm, but also about safeguarding critical infrastructures, maintaining public trust, and preserving national stability in the face of foreign aggression. The targeting of Ukraine's communication systems, public services, and satellite infrastructure indicates that the digital environment has become a primary battlefield, requiring states to elevate cybersecurity to the level of national defense.

The focus of the current journal is on cyber operations, specifically 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 cyberattacks on numerous occasions, both as part of military action and to disrupt societal stability, as seen in the 2016 United States presidential election. In addition, in response to specific incidents, Russia has also utilized cyberattacks as a form of intimidation against other governments. For example, when Finland invited Ukrainian President Volodymyr Zelensky to speak in parliament in April, Russia launched a cyberattack as a show of force. This situation demonstrates the complexity and importance of cyber operations in the context of global geopolitics.

The cyberattacks used by Russia in the Russia-Ukraine conflict exemplify how the country utilizes cyber operations in armed warfare and hybrid warfare against Western countries, with the aim of avoiding a direct military response. The invasion of Ukraine became a moment to test theories about how cyberattacks could be used in conventional warfare. Some predictions suggest that a cyber war is possible, where Russia will initiate attacks with offensive cyber capabilities to create surprise and weaken Ukraine's defenses and morale. Some experts even argue that Russia does not need to use military force directly to achieve its goals, as cyberattacks can provide significant strategic advantages. They can serve as a complement to military force or even as a standalone instrument. Therefore, understanding the effectiveness of cyber operations accompanying the

Russian invasion is crucial in the context of the current situation and conditions of the Russia-Ukraine conflict (Panggabean, 2023).

HermeticWiper is a disk wiper malware used by the Iridium group, part of the Russian military intelligence (GRU), in an attempt to cyberattack various vital sectors in Ukraine ahead of the February 24, 2022 invasion. The malware is specifically designed to fit the target system and has the ability to overwrite and delete critical data structures on computer disks, rendering them unusable. This attack is part of a *hybrid warfare* strategy that aligns conventional military attacks with destructive digital attacks (Firdini, 2023). This malware is designed to maximize the damage done to the system. It does not just overwrite the MBR, but goes beyond that: it infiltrates many filesystem structures and corrupts them all, destroying individual files as well (Hasherezade, 2022). Hermeticwiper malware attack targeting Ukrainian organizations via Windows systems for deletion A data cyberattack or "wiper" was launched against 100 organizations in the financial, IT and aviation sectors. These cyberattacks are already on the rise in early 2022. As on January 13, 2022, Microsoft reported that malware was detected targeting the Ukrainian government and several non-profit and Information Technology (EPRS) organizations. Some of the destructive malware identified targeting Ukraine are WhisperGate / WhisperKill, FoxBlade, SonicVote, CaddyWiper, DesertBlade, Industroyer2, Lasainraw, and FiberLake (DoubleZero). (BUDIMAN, 2023).



Graph 1. Sectors Impacted by HermeticWiper
Source: writer's journal

The *National Cybersecurity Strategy* theory explains that cybersecurity is an integral part of a country's national defense strategy, which includes protecting vital digital infrastructure, government, and public stability. In this context, the HermeticWiper attack launched by Russia against Ukraine is not only understood as a technical attack, but as a form of threat to the existence of the state. HermeticWiper is a *disk wiper* malware that targeted more than 12 strategic Ukrainian organizations, including the government, financial and energy sectors, just hours before the physical military invasion. This strategy demonstrates the close synergy between conventional military power and

digital attacks within the framework of *hybrid warfare*. Through the lens of *National Cybersecurity Strategy* theory, this attack can be classified as a systematic attempt to digitally shake the foundations of Ukraine's national defense, while demonstrating the importance of capacity building, international cooperation, and strengthening the cyber institutional framework as an effective and structured national strategic response.

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

Malware Name	Type	Target Sectors	Date Detected	Key Features	Malware Name
HermeticWiper	Disk Wiper	Government, Finance, Energy	23 Feb 2022	Corrupts MBR and system files	HermeticWiper
WhisperGate	Wiper + Ransom	NGOs, IT	Jan 2022	Two-stage fake ransomware	WhisperGate
CaddyWiper	Data Wiper	Military, Infrastructure	28 March 2022	Deletes user files, avoids domain admins	CaddyWiper
IsaacWiper	Disk Wiper	Gov't Systems	24 Feb 2022	Used after HermeticWiper, less complex	IsaacWiper
FoxBlade	Trojan Malware	Government, Banking	23 Feb 2022	Used for backdoor access	FoxBlade

Source: (GROUP, 2022)

On February 23, 2022, a destructive campaign using HermeticWiper targeted several Ukrainian organizations. This cyberattack occurred hours before the start of the invasion of Ukraine by Russian Federation forces (E.S.E.T., 2022).

The deployment pattern of HermeticWiper suggests close coordination with Russian military operations. The malware attacked more than 12 organizations in critical sectors of Ukraine, including government, finance, energy, and agriculture. Microsoft noted that the HermeticWiper attack occurred just hours before the physical invasion began, and was carried out alongside other cyberattacks such as FoxBlade, WhisperGate, and CaddyWiper. According to a report by the European Cyber Conflict Research Initiative (ECCRI), these attacks form a unified *hybrid warfare* strategy, where military power and cyber power are combined to create simultaneous pressure on targets. This strategy aims to demoralize, undermine logistics, and weaken the coordination

capabilities of the Ukrainian government(Kaminska, 2022). From the lens of the **National Cybersecurity Strategy**, such an attack represents a calculated effort to degrade **Ukraine's digital sovereignty**, targeting its governance, financial, and public infrastructures.

2. The influence and response of HermeticWiper attacks on the de-escalation process of the Russia-Ukraine conflict

The escalation of conflict and war between Russia and Ukraine in the last decade has brought international relations into a complicated situation. In 1991, Ukraine declared its independence from the Soviet Union and its relationship with Russia remained very good, which can be seen from its cultural closeness and the location of the two countries, even Russia is the closest country to Ukraine compared to other Soviet Union fragments. However, this closeness broke into conflict when Russia began invading the Crimea region in 2014 (Priyono, 2022).

In the context of the HermeticWiper attack, it appears that the main target of the cyberattack was not military infrastructure directly, but civilian sectors such as public services, government institutions, and financial systems. These attacks cause major disruptions to people's daily operations. Interestingly, this kind of attack cannot be directly confirmed by the military or the public, although the impact is very real for civilians (Padmi, 2022). This condition reflects that the military has limitations in conducting direct cyber counterattacks, because cyberspace is invisible, not bound by territory, and does not always involve formal state actors. Therefore, the response to cyberattacks requires a cross-sector approach involving state agencies, the private sector and public participation through a collaborative digital defense strategy.

What people see is a war between the Russian and Ukrainian armies, what is less known is the scale of hybrid warfare. A term coined by NATO to describe the kinetic combination of war and information. The ongoing reality is a potent mix of kinetic attacks with weapons and munitions, used in combination with cyber attacks, and disinformation campaigns. It is a relief that how international relations work has changed in the last decade. Most international relations experts and diplomats agree that this revolution is an essential component of the ongoing digital transformation across society, and therefore cyber warfare is becoming more of a reality than a theory (Eevee, 2022).
However, the Hermeticwiper attack did not make Ukraine submit or surrender but rather increase their cyber security. Quite the contrary, they increased their cyber defenses and coordinated efforts with the international community.

They also mobilized an "IT Army" of volunteers from around the world to counter Russian cyberattacks. However, even though its cyber security capabilities are not fully optimized in the management of technology and information, Ukraine still provides a counterattack. As a defense strategy, the Ukrainian government formed a special organization in charge of handling cyber security and scouting for any form of cyber-war attacks from Russia. The organization is known as the "IT Army" which consists of Ukrainian volunteers and internationals from around the world who have Underground hacker skills and are willing to protect Ukraine's state infrastructure (roy,

2022). It contains thousands of programmers, ethical hackers, cybersecurity analysts from Ukraine and other countries.

In addition to the support and participation of several external actors in the cyber attack, the Ukrainian government itself also has several official institutions that play a strategic role in stemming Russian cyber attack activities. Furthermore, Jari Juutilainen (2022) stated in his research that these institutions do not have other units but rather direct assignments, including:

1. State Service of Special Communication and Information Protection of Ukraine (SSSCIP) SSSCIP is a Defense Agency as well as a special agency tasked with protecting and enhancing Ukraine's cyberspace security. In carrying out its duties, SSSCIP provides several services including conducting cyberspace threat analysis, investigative national operations, issuing data release edicts and assisting private organizations in dealing with cyberspace threats.
2. Security Service of Ukraine (SSU/SBU) If SSSCIP is in charge of improving cyberspace security, then SSU is more about protecting the state order of the Ukrainian nation, counter-terrorism and counter-intelligence activities and countering various Ukrainian cyberspace threats such as cyber-attack and cyber-terror.
3. Cyber Police of Ukraine This is a unit of the national police of Ukraine whose duties and powers are regulated by the Ministry of Internal Affairs of Ukraine. As the name implies, Ukraine's cyber police is tasked with enforcing the law, sanctioning cybercriminals and warning Ukrainian citizens of cyberspace crimes.
4. Defense Intelligence of Ukraine (GUR) The Defense Intelligence Agency is one of the units under the Ministry of Defense of Ukraine. It is in charge of collecting and analyzing important information related to the development of military capabilities, military and military technical defense in maintaining cyberspace security. In addition, there is also another unit, Ukraine's Defense Intelligence Service (GURMO), which is run by a special cyber unit. However, its tasks and roles are almost related to the Defense Intelligence of Ukraine.
5. IT Army of Ukraine The IT Army of Ukraine is a Ukrainian activist group that was initially established through the merger of several Ukrainian cyberspace security companies and later expanded through the use of volunteers based on the creation of a cyber security army through the Ministry of Digital Transformation of Ukraine. This IT Army focuses on its participation in cyber operations with Russia as the target of attack. In this case, IT Army Ukraine can exploit advanced equipment to counter Russian cyber attacks including DDoS. Cyber security attacks that are able to create a cyber-war conflict between Russia and Ukraine are actually also inseparable from the participation of several actors who are reliable in the cyber field. In addition to official institutions that handle cyber issues in each country, cyber-war is also created due to the participation of actors such as Private Companies and Hacktivism. In this case, both Russia and Ukraine formed cooperation with several private companies that were able to provide cyber services that were certainly profitable. These private companies include Microsoft, ESET and Starlink (Juutilainen, 2022). This coordinated response exemplifies what Desecuritization Theory, introduced by Buzan, Wæver, and de Wilde (1998), describes as the return of an issue from emergency mode to normal political handling. Rather than amplifying fear or invoking exceptional powers, Ukraine chose to manage the threat as a governance challenge ntegrating legal, technical, and diplomatic responses through its existing institutions. This action fulfills the core principle of desecuritization: moving an issue away from being a "security threat" that justifies extraordinary

measures, and instead addressing it through regular policy, civilian participation, and rule-based solutions.

Then the form of cooperation carried out by Ukraine with the Microsoft Threat Intelligence Center is Microsoft's cybersecurity division which specializes in detecting high-level cyber threats, including malware, ransomware, and digital espionage operations. On February 23, 2022, MSTIC detected an unusually unusual series of cyberattacks: computer systems in various Ukrainian institutions began to experience sudden total data corruption, unlike typical data theft attacks.

Through rapid analysis, MSTIC identified the presence of a new malware, later named HermeticWiper. This malware uses a "disk wiping" technique, which destroys the file structure of the operating system until the device is unusable. MSTIC also discovered that the malware was signed using a valid digital certificate, as if it came from a legitimate company called Hermetica Digital Ltd, a technique used to trick security and antivirus systems. Furthermore, Ukraine's collaboration with international actors such as Microsoft's Threat Intelligence Center (MSTIC) and ESET underscores its reliance on non-militarized, cooperative responses rather than state-centric, coercive approaches. Microsoft's early detection and sharing of HermeticWiper signatures allowed rapid containment, while ESET's technical analysis supported national and global cyber defenses. These responses reflect a strategic shift from "securitizing" the cyberattack into a state of emergency, toward "desecuritizing" it by reinforcing civilian and technological resilience.

Following this identification, Microsoft immediately sent an alert to the Ukrainian government, and shared the malware signature and technical prevention methods with the global security community. This quick action allowed security systems in Ukraine and their partners to update their defense software and firewalls before the malware spread further(Stepanic, 2022).

The Copenhagen School's *Desecuritization* Theory views that a security issue is not objective, but rather socially formed through a *securitization* process. In the context of Ukraine, the HermeticWiper attack was indeed presented as an existential threat to the state, but interestingly, Ukraine did not respond with a repressive approach or expand the conflict to the military arena alone. Instead, they chose the path of *desecuritization* by managing this threat institutionally and collaboratively through formal institutions such as SSSCIP, Cyber Police, and IT Army, as well as collaborating closely with international actors such as Microsoft and ESET. This approach shows that Ukraine is not responding to cyberattacks as an emergency crisis that must be met with violence, but rather as a technical and strategic challenge that can be addressed through the normal mechanisms of politics, public policy, and civil society participation. Thus, Ukraine's response to HermeticWiper not only demonstrates digital resilience, but also reflects a *desecuritization* process that contributes to stabilizing the situation and minimizing the potential for conflict escalation in the region.

CONCLUSION

This research shows that Russia's HermeticWiper cyberattack against Ukraine in 2022 is part of a planned attack strategy integrated in a modern hybrid warfare scheme. The HermeticWiper

malware is not just a digital sabotage tool, but a cyber weapon designed to cripple critical infrastructure, permanently erase data and create systemic chaos just before the start of the Russian military invasion. The deployment of HermeticWiper just hours before the physical attack suggests close coordination between digital operations and conventional military tactics.

HermeticWiper's characteristics of bypassing Windows security systems and targeting vital sectors such as government, finance, energy and communications, prove that Russia is leveraging the cyber domain to maximize pressure on the opposing country. However, this attack did not succeed in subduing Ukraine**.** On the contrary, Ukraine demonstrated considerable cyber resilience, enhancing its digital defense capabilities through collaboration with international actors such as Microsoft and ESET, as well as forming an IT Army of local and global volunteers.

Ukraine's response to this attack also reflects a shift in the security paradigm, from a traditional military-based focus to a non-traditional security approach involving civilian actors, technology and digital infrastructure. Through the use of non-traditional security concepts and a case study approach, this research asserts that cyber threats such as HermeticWiper have become a strategic element in contemporary international conflicts. As such, war is no longer confined to the physical terrain, but has expanded to cyberspace as a new battlefield that is not only a strategic element, but also a strategic element in contemporary international conflicts.

REFERENCE

Afiah, R. D. (2021). *Serangan siber notpetya oleh rusia terhadap ukraina berdasarkan prinsip pembedaan dalam hukum humaniter internasional*. Usakti.

AM, B. S. (2021). *ANCAMAN PERANG SIBER DI ERA DIGITAL DAN SOLUSI KEAMANAN NASIONAL INDONESIA*. JURNAL ORATIO DIRECTA.

Anjelina, D. (2023). *FENOMENA SERANGAN SIBER RUSIA TERHADAP UKRAINA: SEBAGAI PEMBELAJARAN BAGI INDONESIA DALAM PENGEMBANGAN PERTAHANAN SIBER*. JURNAL PERTAHANA DAN BELA NEGARA.

Aris Hardinanto, V. O. (2024). *PENGGUNAAN DRONE PENYERANG DALAM PEPERANGAN*. Jurnal Hukum Progresif.

Barry Buzan, O. W. (1998). *Security: A New Framework for Analysis*. Lynne Rienner publisher.

Budiman. (2023). CYBERSECURITY ANALYSIS IN THE CONTEXT OF THE RUSSIAUKRAINE CONFLICT: CHALLENGES, THREATS. *AND DEFENSE. Jurnal Ekonomi*.

BUDIMAN, L. S. (2023). *PERANG RUSIA UKRAINA DALAM PERSPEKTIF SIBER*. Politeknik Siber dan Sandi Negara Press.

Eevee. (2022). *Serangan Keamanan Siber Melonjak saat Perang Ukraina-Rusia Berkecamuk*. https://nagacyberdefense.net/tag/hermeticwiper/

E.S.E.T. (2022). *IsaacWiper dan HermeticWizard: Wiper dan worm baru yang menargetkan Ukraina*. https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

Firdini. (2023). The Role of Russian Cyber Operations in The Russian–Ukraine War in Achieving Russia's Strategic Objectives. *Jurnal Perencanaan Pembangunan*, 118 – 131.

GROUP, I. (2022). *12). Tinjauan Umum 9 Penghapus Data Berbeda yang Digunakan dalam Perang Ukraina*. https://www.recordedfuture.com/research/overview-9-district-data-wipers-ukraine-war

Hansen, L. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 1155–1175.

Hasherezade. (2022). *HermeticWiper: Analisis terperinci tentang malware perusak yang menargetkan Ukraina*. https://www.threatdown.com/blog/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine/

Imma Karisma1, A. B. (2023). Signifikansi Perang Siber dalam Konflik Modern Rusia-Ukraina. In *JISHUM (Jurnal Ilmu Sosial dan Humaniora* (pp. 800–817).

Junior, R. M. A. C., & D, N. (2024). *PERTANGGUNGJAWABAN RUSIA ATAS TINDAKANNYA MELAKUKAN CYBER WARFARE DALAM KONFLIK BERSENJATA DENGAN UKRAINA BERDASARKAN HUKUM HUMANITER INTERNASIONAL*. DIPONEGORO LAW JOURNAL.

Juutilainen, J. (2022). *Cyber Warfare: A Part of the RussoUkrainian War in 2022*. JAMK University of Applied Sciences.

Kaminska. (2022). *Cyber Operations during the 2022 Russian Invasion of Ukraine: Lessons Learned (So Far*. ECCRI.

Karisma, I. (2023). *Signifikansi Perang Siber dalam Konflik Modern Rusia-Ukraina Studi Kasus: Wizard Spider - It Army*. JISHUM (Jurnal Ilmu Sosial dan Humaniora.

Khoirunnisa, K. (2025). Konflik Ukraina-Rusia: Tinjauan hukum humaniter internasional tentang keterlibatan pejuang asing. *ScienceDirect*.

Khoirunnisa Khoirunnisa, I. A. (2025). Cyber Warfare and National Security: Modernizing Defense Strategies in the Context of China's Evolving Cyber Influence. *China Quarterly of International Strategic Studies*, *4*.

Malahati, F. (2023). *KUALITATIF : MEMAHAMI KARAKTERISTIK PENELITIAN SEBAGAI METODOLOGI. jurnal pendidikan dasar*.

Padmi, M. F. (2022). Japanese and ASEAN Security Strategies in Cyber Crime in 2021 - 2025. In *Jurnal Institut Penelitian dan Kritik Internasional Budapest* (pp. 23047,).

Panggabean, J. U. (2023). The Role of Russian Cyber Operations in The Russian–Ukraine War in Achieving Russia's Strategic Objectives. *Jurnal Perencanaan Pembangunan*, 119.

Priyono, U. (2022). CYBER WARFARE AS PART OF RUSSIA AND UKRAINE CONFLICT. *Jurnal Diplomasi Pertahanan*, 44–45.

roy, C. I. (2022). *MARCH 3). Bukan Dunia Nyata, Perang Rusia-Ukraina Ngeri di Dunia Maya*. https://www.cnbcindonesia.com/tech/20220303100401-37-319748/bukan-dunia-nyata-perang-rusia-ukraina-ngeri-di-dunia-maya

Safarudin, R. (2023). Penelitian Kualitatif. *INNOVATIVE: Journal Of Social Science Research*, 9680–9694.

Samad, M. Y. (2022). *Memahami Perang Siber Rusia dan Peran Badan Intelijen Negara dalam Menangkal Ancaman Siber*. Jurnal IPTEK-KOM (Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi.

Setiyono, A. (2024). DINAMIKA STRATEGI PERTAHANAN RUSIA MELALUI PERANG HIBRIDA (HYBRID WARFARE) DALAM KONFLIK DENGAN UKRAINA TAHUN 2020 - 2023. *DIPLOMACY AND GLOBAL SECURITY JOURNAL*, 561–576.

Stepanic, D. (2022). *Elastic protects against data wiper malware targeting Ukraine: HERMETICWIPER*. https://www.elastic.co/security-labs/elastic-protects-against-data-wiper-malware-targeting-ukraine-hermeticwiper?utm_source=chatgpt.com

Sulung, U. (2024). MEMAHAMI PENELITIAN DATA SUMBER : PRIMER, SEKUNDER, DAN TERSIER. *Jurnal Penelitian Pendidikan*, 110–116.

Sya'roni, A. (2019). *ANALISIS YURIDIS PENYELESAIAN SENGKETA CYBERATTACK PADA KONFLIK RUSIA DAN UKRAINA DALAM HUKUM HUMANITER INTERNASIONAL*. JURNAL HUKUM.