BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

SSSCIP's Perspective on the cyber-attacks unfolded in the context of the military conflict between Russia and Ukraine (January 2022 – January 2024)

Mihai OLTEANU, Ph.D. Student*
*"Carol I" National Defence University, Bucharest
e-mail: mihaiolteanu48@yahoo.com

Abstract

This paper evaluates the reports of the SSSCIP regarding cyber-attacks carried out against Ukraine from January 2022 to January 2024. From the exploitation of the CaddyWiper malware, attributed by SSSCIP to APT SANDWORM, to the sophisticated campaigns of the FSB and the cyber-attack on Kyivstar, the paper provides an insight into Russian-origin cyber-attacks against Ukraine, as reported by the main Ukrainian authority in the field, SSSCIP.

The purpose of the article is to identify how SSSCIP reported cyber-attacks on Ukrainian IT&C infrastructures, the completeness of the published data, and the way the campaigns are presented. To achieve this goal, all SSSCIP reports from the reference period were evaluated, and only those that materialized and affected IT&C infrastructures were included in the study. In conclusion, the paper will primarily highlight the limitations of SSSCIP reports and, secondarily, SSSCIP's perspective on the domains most frequently targeted by cyber-attacks and the capabilities of Russian actors.

Keywords:

SSSCIP; Ukraine; APT; cyber security; Russia; military conflict.

Article info

Received: 1 February 2024; Revised: 26 February 2024; Accepted: 13 March 2024; Available online: 5 April 2024

Citation: Olteanu, M. 2024. "SSSCIP's Perspective on the cyber-attacks unfolded in the context of the military conflict between Russia and Ukraine (January 2022 – January 2024). *Bulletin of "Carol I" National Defence University*, 13(1): 63-79. https://doi.org/10.53477/2284-9378-24-04

Over the past decades, the continuous evolution of technology and the significant expansion of digitization processes at the state and private company levels have led to a constant increase in the importance of the field of cybersecurity. This growth has brought about substantial changes in the most crucial sectors of society, particularly in political, economic, and military domains. Simultaneously, cyber threats have become more complex, with a broader range of targets, offering financial, political, and military opportunities upon compromise (Furstenau, Sott et al. 2020).

In the political context, cyber-attacks have emerged as a primary concern for states and international organizations, given that compromising IT&C infrastructures can lead to strategic disadvantages. Aspects such as influencing electoral processes, manipulating political decisions, and undermining the stability of governmental institutions have evolved into threats to the political domain. The use of cyber-attacks has been solidified as a strategic means to achieve geopolitical objectives, both for state and non-state actors (Visvizi and Lytras 2020). An example in this regard is the cyber actor APT28, which, according to reports from cybersecurity industry companies, operates to support the interests of the Russian Federation (RUS). It has successfully compromised strategic targets in various states (such as Georgia, Poland, and Hungary) and organizations (including NATO and OSCE) (Mcwhorter 2014).

In the economic sphere, extensive business digitization has inherently introduced cyber threats affecting not only information confidentiality but also financial integrity and organizational reputation. Data theft, industrial espionage, and various forms of cyber extortion pose risks to both public and private sectors, impacting the smooth functioning of economic entities (Hernandez-Castro and Cartwright 2020). Prominent incidents, such as the WannaCry[1] cyber campaign, have illustrated the destructive potential of cyber threats, directly impacting economic and industrial sectors (Hernandez-Castro, Cartwright and Stepanova 2017).

The military sphere, reliant on advanced information systems, faces significant cybersecurity risks due to increased interconnectivity between communication and control systems. Modern military operations' complexity has heightened vulnerabilities to cyberattacks, often employed as instruments in state conflicts, such as the ongoing conflict between RUS and Ukraine (UA) since February 2022. Existing literature offers specific analyses of cyberattacks in certain domains, yet comprehensive assessments of major cyber campaigns against UA, irrespective of their targets, starting from 2022, remain scarce. In this context, the purpose of this study is to analyze the official reports issued by Ukrainian authorities regarding the most significant

[1] WannaCry represented a ransomware cyber campaign that occurred in May 2017. Upon infecting a system, WannaCry encrypted user files and demanded payment in the virtual currency Bitcoin for their release. The attack had a global impact, affecting major organizations, including the healthcare system in the United Kingdom and companies in the energy and financial sectors, highlighting the relevance of vulnerabilities in critical infrastructures to cyber threats. (Mohurle and Patil 2017).

cyberattacks spanning from January 2022 to January 2024, impacting various sectors. Following this analysis, conclusions will be drawn, primarily focusing on the reporting practices of SSSCIP and, secondarily, on SSSCIP view of cyberattacks during the conflict between RUS and UA.

For the conduct of this study, particular emphasis will be placed on the reports issued by SSSCIP UA[2], the primary Ukrainian cyber security service under the control of the President. This agency is engaged in activities related to policy formulation in the field of safeguarding IT&C infrastructures, including classified networks within UA (Cyber Security Intelligence 2022). Additionally, it engages in interventions in the event of cyber-attacks, conducted through CERT-UA (Temple-Raston 2023).

It is important to underline the fact that the cyberattacks included in SSSCIP's reports are characterized by different levels of complexity and relevance, from two perspectives: (1) the impact that these attacks produced against the targeted infrastructures and (2) the level of technical capabilities of the attackers (Agrafiotis et al. 2018). Therefore, it is relevant that one of the most common types of cyberattacks is based on phishing, a technique grounded in social engineering which aims to persuade the target into accessing the malicious attachment (Khonji, Iraqi and Jones 2013). Most of the phishing attempts are unsuccessful, an outcome determined by multiple factors such as the lack of capabilities of the attackers, the use of phishing attempts insufficiently documented or easily detected by cybersecurity software (Patil et al. 2022). Thus, from a methodological point of view, in order for this paper to be more relevant, it will not take into consideration the SSSCIP reports focused only on unsuccessful phishing campaigns, without a real impact on the targeted infrastructures. Furthermore, it is relevant that between January 2022 and January 2024, SSSCIP published 435 reports. Still, after conducting an initial analysis, it has been concluded that 394 of these were strictly focused on phishing campaigns, without having a real impact against the Ukrainian infrastructures. Taking these facts into consideration, 41 articles have been selected, which will be presented and evaluated with the aim of underlining some conclusions regarding the cybersecurity component as a part of the conflict between RUS and UA.

Literature review

Regarding the analysis of cyber-attacks in the context of the conflict between RUS and UA, existing works focus on the impact of attacks on specific sectors or in short time frames. Davydiuk and Zubok evaluate the resilience of UA's energy sector to cyber-attacks and the potential for cascading effects on other industries, providing insights into the disadvantages faced by UA in the conflict (Davydiuk and Zubok 2023). Similar analyses have been

[2] Державна служба спеціального зв'язку та захисту інформації України – The State Service of Special Communications and Information Protection.

published, including on Ukraine's financial sector, focusing on the characteristics of cyber-attacks and cyber threats in the context of the RUS-UA conflict. The studies delve into the trends of cyber-attacks targeting the financial industry, highlighting the active use of SMS messages and emails containing links or malware codes (Kloba and Kloba 2022). CERT-EU has consistently released assessments on cyber-attacks conducted against UA, identified by various public and private entities (CERT-EU 2023). However, these works adopt a perspective focused solely on specific sectors (such as those centered on the energy and financial sectors) or aim for an assessment from the viewpoint of external entities in the conflict. In comparison, this study exclusively focuses on the reports made by UA through its competent institution.

Marcus Willet published an analysis on the possibility of escalating the conflict between RUS and UA at the international level, involving NATO (based on international law), as a result of broader cyber-attacks (Willett 2022). The evolution of the conflict from the perspective of cybersecurity is analyzed, taking into account the involvement of unexpected non-state actors in February 2022, which played a significant role (Lonergan, Smith and Mueller 2023). Wilson and Fitz suggest in their work the possibility that cyber-attacks in the context of the RUS-UA conflict could lead to the triggering of events of a nuclear nature, either intentionally or incidentally (Wilson and Fitz 2023). There are also works that have attempted to construct a cybersecurity strategy to ensure resilience, concluding that the improvement of the UA cybersecurity system is in its early stages (Tarasenko, et al. 2022).

The literature includes several works regarding the involvement of non-state entities in the conflict between RUS and UA, particularly the entity named Ukraine IT Army, created by the authorities in Kiev to gather experts regardless of their location to help UA combat cyber-attacks (Soesanto 2023). Similarly, Smith and Dean evaluate the effectiveness of the Ukraine IT Army and its ability to manage around 200,000 volunteer experts who have chosen to join the entity (Smith and Dean 2023). There are works that assess the involvement of external entities in supporting UA, such as major technology companies (e.g., Google, Microsoft, Meta, Apple, and Amazon), and the impact generated by this aspect (Matania and Sommer 2023). Alongside private companies, there have also been states or international organizations (such as the EU) that have sent teams to support UA in ensuring cybersecurity (Sullivan 2023).

The cyber-attacks reported by SSSCIP through the year 2022

Throughout 2022, a significant number of cybersecurity attacks targeted the IT&C infrastructure within UA, with the most notable incidents including:

- On the night of January 13-14, 2022, several public organizations' websites in UA were targeted in a cyber-attack. According to SSSCIP, the attack involved in some cases the display of provocative images and data encryption or deletion. (SSSCIP 2022a). The attack was considered to be premeditated and involved various types of malware, including a destructive one named WhisperKill, aiming to incapacitate infrastructures (CERT-UA 2022a). SSSCIP did not provide data regarding the potential attribution of the attack campaign to a state or non-state entity. According to Microsoft, the targets included both governmental and non-governmental organizations, among which private companies (Microsoft 2022).

➢ On February 15, 2022, a significant Distributed Denial of Service (DDoS) attack aimed to compromise IT&C infrastructures belonging to both public organizations (including the Ministry of Defense and the Armed Forces websites) and private entities (such as Privatbank and Oschadbank, both of which were compromised) (SSSCIP 2022e). According to Ukrainian authorities, the same cyber-attack campaign was identified on the evening of February 23, 2022, one day before the RUS invasion of UA. This time, the cyber-attacks intensified, targeting the websites of the Cabinet of Ministers, Verkhovna Rada (the Ukrainian Parliament), the Ministry of Foreign Affairs, and the Security Service. On the same day, SSSCIP reported an escalation in malware distribution campaigns, attempts to penetrate public and private IT&C infrastructures, and data destruction attempts. This time, SSSCIP specified that it is clear these campaigns are carried out by the "*aggressor state*" (SSSCIP 2022r).

The relevance in this context lies in the synchronization of the intensified cyber-attacks with the onset of the conflict, creating the conditions for coordinated actions by the RUS against UA (Lewis 2022).

➢ On March 6, 2022, SSSCIP released statistics announcing a record number of cyber-attacks, reaching 2800. Additionally, a record number of 271 DDoS attacks within 24 hours were recorded. These actions are attributed entirely to the RUS, with the Ukrainian authority asserting that they complement attacks from air, water, and land (SSSCIP 2022q). Furthermore, on March 25, SSSCIP announced that in the week of March 15-22 alone, it recorded 60 cyber-attacks, including 11 targeting local and central authorities, 8 against the defense sector, 6 on the financial sector, 6 on commercial organizations, 4 on the telecommunications sector, 2 on the energy sector, and the remaining attacks targeted other public and private entities (SSSCIP 2022p).

➢ On March 15, 2022, SSSCIP released information about a new malware, known in the industry as CaddyWiper, designed to erase data from compromised systems. It is noteworthy that this is the first instance where SSSCIP cites two private companies, Eset and Microsoft, regarding the identification of this malware (SSSCIP 2022b). The campaign targeted entities in the energy sector with the objective of disrupting the electricity supply in UA, and it has been attributed to the Russian cyber actor APT SANDWORM (CERT-UA 2022b).

It is noteworthy that APT SANDWORM was the attributed attacker in the 2015 cyber campaign targeting UA, specifically aimed at the national energy grid (Paverman 2019).

➢ On April 6, 2022, SSSCIP reported a cyber-attack targeting the infrastructure of UKRTELECOM, Ukraine's largest mobile phone company. The attack, characterized by a high level of complexity, originated from territories occupied by RUS at that time, aiming to take control of the communication infrastructure. UKRTELECOM had to reduce infrastructure capacity to 13% to prevent the attackers' intentions. Restoration efforts were successful, though attribution to a specific attacker remains inconclusive according to UKRTELECOM and SSSCIP (SSSCIP 2022c).

➢ On April 11, 2022, an announcement highlighted challenges in maintaining mobile communications in UA. SSSCIP consistently worked to sustain Internet and telecommunication providers, such as Vodafone. At that time, only 65% of the telecom infrastructure remained operational, impacting citizens' communication capabilities within UA (SSSCIP 2022i).

➢ On April 12, 2022, SSSCIP announced efforts to prevent a new cyber campaign by APT SANDWORM, targeting the disruption of electricity supply in UA by compromising network equipment used by private enterprises. Similar to the March 15, 2022 incident, SSSCIP reported collaboration with ESET and MICROSOFT to prevent the cyber-attack. UA maintained cooperation with European states, exchanging information on this cyber threat. However, SSSCIP emphasized that the goal of cooperation was to identify any other compromised energy infrastructure within UA by APT SANDWORM (SSSCIP 2022h).

➢ The following day, on April 13, 2022, SSSCIP reported receiving information from international partners regarding the compromise of an electricity distribution company by the Russian actor APT SANDWORM. The objective was to disrupt the electricity supply for a significant portion of UA. At the time of the intervention, the cyber-attack was underway, successfully compromising some resources but without achieving its final intent. Furthermore, SSSCIP announced a continued increase in the number of cyber-attacks, especially DDoS attacks, with approximately 25 times more incidents identified compared to the entire previous year (SSSCIP 2022l).

➢ Subsequently, on April 16, 2022, SSSCIP reported a new DDoS cyber-attack campaign targeting the websites of public authorities, resulting in their temporary unavailability. Following technical interventions, the websites were restored to operation (SSSCIP 2022n).

➢ Throughout May 2022, attempts to disrupt communications persisted, with attackers successfully permanently disabling them in the Kherson region, occupied by RUS. Residents lost access to mobile and internet communications, and SSSCIP announced its inability to intervene due to military occupation and controlled equipment. Simultaneously, Ukrainian authorities reported that in the absence of communication means, RUS soldiers patrolled and transmitted propagandistic news through audio systems to influence citizens without communication access outside the area. Furthermore, SSSCIP estimated that citizens in the Kherson region would be granted access to RUS's state-controlled telecom network (SSSCIP 2022m). At the end of the year, in November 2022, SSSCIP announced the successful restoration of access to Ukrainian television and radio stations in Kherson with the assistance of the Polish company Emitel SA (SSSCIP 2022t).

➢ On June 6, 2022, SSSCIP reported an ongoing cyber campaign accompanied by propaganda actions, resulting in the compromise of Ukraine's major television networks. During this incident, Russian news was broadcast while Ukrainian television was airing the national football team's World Cup qualification match. The attackers likely gained access to a TV communication node, enabling the transmission of altered content (SSSCIP 2022j).

By the end of 2022, SSSCIP had not reported additional cyberattacks, although private industry sources, such as MANDIANT, disclosed campaigns, including power outages during October 10-12, 2022 (Proska et al. 2023). Furthermore, SSSCIP did not release a report regarding the campaign against VIASAT KA-band satellite modems, which were rendered inoperable in Ukraine and several European countries, including Poland, the UK, and France, as a secondary effect (Boschetti, Gordon and Falco 2022). Nevertheless, multiple European states attributed this cyber campaign to RUS throughout the year 2022 (Steinbrecher 2022). The only mention of this campaign by SSSCIP was on July 2, 2022, when it stated that UA utilizes the STARLINK satellite infrastructure provided by Elon Musk to ensure backup communications in the event of a cyber-attack on the main infrastructure (SSSCIP 2022o).

Throughout 2022, there were additional statistical reports on the intensity of cyber-attacks, which were three times higher than the previous year (SSSCIP 2022u). The targeted sectors were primarily telecommunications, medical, and governmental (SSSCIP 2022g), with attackers consisting mainly of ideologically motivated groups and state actors (SSSCIP 2022d). However, an interesting aspect is a report from May 1, 2022, when SSSCIP announced that existing indicators suggested that the intensity of Russian cyber-attacks against UA had reached a maximum level. The Ukrainian service estimated that there would be no stronger cyber operations (SSSCIP 2022k). This aspect may indicate an attempt to increase social confidence and maintain an offensive attitude towards RUS at a high level, similar to the period preceding the military conflict (Paniotto 2020). On the other hand, it is possible that UA may have acted to promote a strong image against the aggressor state, aiming to weaken the support of the Russian population for the military actions conducted by RUS, which was at 60% in 2022 (Kizilova 2022). The initiative was supported two months later when SSSCIP announced that the intensity of cyber-attacks continued to remain at the same high level, but their quality was on a declining trend (SSSCIP 2022f).

Another aspect indicating a distinct approach from SSSCIP is revealed in a statement from May 1, 2022, in which Ukraine states that Russian cyber-attacks directed against its infrastructure are also a potential attack on other partner states. As an example, SSSCIP mentions that in 2014, Ukrainian elections were targeted by cyber-attacks of Russian origin, and two years later, the same modus operandi was observed in the electoral processes in the United States (SSSCIP 2022s). Thus, considering the precedents in terms of cyber security, UA indirectly reiterates the need for support throughout the conflict, emphasizing that it is not only of interest to the two participating states (Ratten 2022).

The cyber-attacks reported by SSSCIP through the year 2023

During the year 2023, SSSCIP published a reduced number of statements regarding cyber-attacks against its own networks and information systems. The most notable ones include:

- ➢ On January 1, 2023, a statement was released attributing the cyber-attacks carried out through the CaddyWiper malware in January 2022 to the Russian cyber actor APT SANDWORM (SSSCIP 2023l), publicly attributed towards the RUS military intelligence service (Akimenko and Giles 2020).
- ➢ On January 18, 2023, SSSCIP published an analysis regarding a cyber campaign targeting the compromise of media entities, particularly the news agency UKRINFORM. The statement emphasized Russia's attempts to compromise information sources for the population, with the main goal being the disinformation of citizens and subsequent influence (SSSCIP 2023a).
- ➢ On February 1, 2023, a series of technical investigations were published concerning cyber campaigns carried out by the Russian FSB against information infrastructures within Ukraine. It was specified that the activity is conducted through cyber-attacks with a high level of complexity and precision, in contrast to DDoS attack campaigns. Furthermore, SSSCIP stated that these types of operations conducted by the FSB represent the most significant cyber threat identified during the military conflict (SSSCIP 2023k).
- ➢ One day later, SSSCIP released information about a watering hole cyber-attack[3], which involved creating a website using the image of the Ukrainian Ministry of Foreign Affairs to give the appearance of a legitimate site. Once accessed, the website offered visitors a program to be downloaded, disguised as an application that could identify whether the user's system was compromised. However, the application contained malware that would infect the visitor's computer if installed (SSSCIP 2023f). The campaign is the only one of its kind reported by SSSCIP and was based on exploiting citizens' desire to be informed about the status of the conflict, using a trusted government source.
- ➢ On July 1, 2023, an analysis was published regarding the increase in the number of cyber-attacks targeting companies in the IT&C sector

[3] Watering hole – A cyber-attack that relies on identifying websites frequently used by the target group and cloning or modifying them to compromise visitors to that domain (Krithika 2017).

in UA. The stated purpose of these attacks was to compromise these companies to gain control over the software products sold in Ukraine and, subsequently, over the users of these solutions. Additionally, SSSCIP mentions that the private sector assesses its ability to handle this type of threat independently, but recent examples indicate that major companies in the field have been compromised (SSSCIP 2023c).

➢ On July 5, 2023, SSSCIP reported on a cyber campaign that successfully compromised the Facebook page used by the National Statistics Service of Ukraine. Attackers posted on this page claiming that the institution's infrastructure had also been compromised, thereby disrupting access to economic and social statistical data. According to SSSCIP, the attackers only managed to compromise the Facebook page without gaining access to the National Statistics Service's infrastructure, and the message posted in the institution's name was false (SSSCIP 2023e). It is possible that the purpose of these actions was to destabilize public trust in the official statistics published by UA. Such propaganda actions have been consistently carried out by RUS throughout the conflict with UA, aiming to reduce society's trust in the governmental authorities (Geissler et al. 2023).

➢ On July 19, 2023, SSSCIP published a technical investigation into two highly sophisticated malware applications named CAPIBAR and KAZUAR. These were utilized by APT TURLA, attributed to the FSB intelligence service of the Russian Federation. The purpose of these applications was to compromise targets within Ukraine. SSSCIP highlighted that it shared all technical investigation results, including with the private sector in the cybersecurity industry (SSSCIP 2023j).

➢ On December 13, 2023, SSSCIP reported that the IT&C infrastructure of the telecommunications operator Kyivstar was compromised the day before, leading to the disruption of specific services for approximately 24 million customers for several days (Balmforth 2024). In order to successfully restore the operator's functionality, SSSCIP recommended temporarily suspending the provision of roaming services, resulting in customers being unable to communicate outside Ukrainian territory for a limited period (SSSCIP 2023d). It is relevant to note that SSSCIP did not announce the impact of the cyber-attack on the official website. However, additional statements provided by the director of the institution to European publications revealed that the IT&C infrastructure of Kyivstar was fully affected, with the malware used successfully deleting most of the data (Gatlan 2024), while the cyber-attack was being characterized as the greatest in the history of telecom (Sapuppo 2023).

➢ The latest cyber-attack published by SSSCIP during the reference period involves a campaign conducted by the Russian cyber actor APT28. This campaign targeted not only entities within Ukraine but also networks and information systems in Poland. SSSCIP thus conveys the message that cyber-attacks on UA are not geographically isolated incidents but can also impact member states of the EU or NATO (SSSCIP 2023i).

It is noteworthy that, throughout 2023, SSSCIP has had a series of statistical reports regarding the most targeted domains by cyber attackers, thus listing commercial organizations, the telecom industry, software developers, government institutions, the industry and defense sector, as well as local authorities (SSSCIP 2023h). Furthermore, SSSCIP specifies that, starting from September 2022, it has been monitoring at least seven cyber actors consistently targeting Ukrainian infrastructures, all of them being associated with the Russian government (SSSCIP 2023g), as well as 23 groups known as hacktivists (SSSCIP 2023b).

Additionally, it is important to note that until the end of January 2024, no new reports have been published regarding other cyber-attacks targeting the IT&C infrastructure in UA.

Conclusions

From a methodological standpoint, this article initially aimed to select and present the 41 reports issued by SSSCIP between January 2022 and January 2024 concerning cyberattacks of high complexity levels that managed to impact Ukrainian IT&C infrastructures, thereby excluding phishing cyber campaigns. After the presentation of the reports by SSSCIP, several noteworthy aspects emerge regarding the functioning of the institution, its reporting on cyber-attacks against Ukrainian IT&C infrastructure, and the operating methods of Russian cyber actors.

First and foremost, it is notable that the most targeted sectors in cyber campaigns were those related to communications and energy. This can be explained by the fact that the energy sector is a critical resource for both the attacked state, ensuring its basic functioning (Kozak, Klaban and Šlajs 2023), and for the aggressor state, representing a factor that can induce panic among the population once compromised (Lee 2022). As for the telecommunications sector, its main roles are determined by informing the population about the conflict's status (especially through TV and radio stations) and enabling citizens to communicate with each other for safety reasons or to reach individuals outside the state (Bratich 2020). The impact is particularly noticeable in the Kherson region, where Russian forces have acted to restrict access to Ukrainian information and the ability to communicate with individuals outside the area. Regarding hacktivist groups, their goal was to compromise the websites of public authorities, both to decrease trust in public institutions and to create a sense of panic among civilians who, even if not directly involved in the conflict, could realize its effects (Hupperich 2023). An example highlighted in this regard is the compromise of the Facebook page of the National Statistics Service of Ukraine, an action that, although not affecting the institution's data, aimed to decrease public trust in the information published by the agency.

Regarding the capabilities of Russian-origin cyber actors, it is noteworthy that they exhibited a wide range, ranging from destructive attacks, such as the one carried out through the CaddyWiper malware, to DDoS cyber campaigns aimed at temporary resource unavailability (Liedekerke and Frankenthal 2023). According to SSSCIP reports, the identified Russian services were primarily the FSB and GRU, with the cyber actor APT SANDWORM being highlighted, attributed to the military intelligence service (McFail, Hanna and Rebori-Carretero 2021). Additionally, a level of synchronization between military forces and cyber capabilities can be noted, considering the SSSCIP report that announced a cyber campaign a day before the invasion of Ukraine, likely aimed at supporting the military forces of RUS in the upcoming conflict (Radu 2022). Furthermore, it is noteworthy the significant increase in the number of cyber-attacks, leading to the conclusion that the cyber segment played a significant role in the unfolding of the conflict from January 2022 through January 2024. Regarding the functioning of SSSCIP and the institution's reporting on cyber campaigns, it is notable that initially, cyber-attacks were not attributed with a high degree of confidence to the RUS, a situation that changed over time. However, SSSCIP did not publish sufficient technical data to prove these public attribution actions, suggesting that the reports had strategic political foundations rather than technical ones. Thus, the rhetoric in the reports shifted towards expressions emphasizing that the aggressor state undoubtedly carried out the attacks. Furthermore, over time, SSSCIP increasingly emphasized in its reports that the level of cooperation with the private sector in the IT&C field is high, specifically naming companies such as ESET and MICROSOFT. This aspect could aim to highlight the existence of developed cooperation that supports UA in preventing and countering cyber-attacks (Lilly et al. 2023). Another aspect repeatedly emphasized by SSSCIP is that the impact of offensive cyber actions is not only felt within UA but also affects partners, regardless of their location. Thus, it is possible that SSSCIP aimed to increase solidarity with UA in the conflict with RUS.

Another important aspect to note is that in the two years of analysis, no cyber-attacks were presented as being associated or attributed to entities other than Russian. SSSCIP did not report cyber-attacks of Chinese, Iranian, or North Korean origin, even though cyber actors associated with these states typically exhibit a high level of activity (Assoudeh 2020). Thus, a hypothesis in this regard could be that SSSCIP aimed to construct a rhetoric focused entirely on RUS (rather than on the authentic presentation of facts), in which case it avoided publishing reports that would have shown that there are other entities seeking to compromise networks and systems in UA.

Finally, it is necessary to emphasize that SSSCIP reports have proven in some instances to be incomplete or lacking. A relevant example in this regard is the cyber campaign against the VIASAT satellite infrastructure, not fully reported by SSSCIP, especially from a technical standpoint. Another example is related to the report dated December 13, 2023, regarding the cyber-attack on the Kyivstar operator, which did not specify the extent of the impact of the cyber-attack on UA infrastructure. These aspects lead to two possible conclusions: (1) the decision to report incidents incompletely or not at all was a strategic one to avoid a decrease in public trust, or (2) the high rate of cyber-attacks generated communication errors, and SSSCIP was unable to maintain the reporting pace aligned with the number of cyber-attacks.

References

Agrafiotis, Ioannis, Jason R.C. Nurse, Michael Goldsmith, Sadie Creese and David Upton. 2018. "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate." *Journal of Cybersecurity* 4 (1). https://doi.org/10.1093/cybsec/tyy006.

Akimenko, Valeriy and Keir Giles. 2020. "Russia's Cyber and Information Warfare." *Asia Policy, National Bureau of Asian Research* 27 (2): 67-75. doi:10.1353/asp.2020.0014.

Assoudeh, Mitra. 2020. "Shaping Cybersecurity Strategy: China, Iran, and Russia in a Comparative Perspective." *Reno ProQuest Dissertations Publishing*. http://hdl.handle.net/11714/7624.

Balmforth, Tom. 2024. "Exclusive: Russian hackers were inside Ukraine telecoms giant for months". https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/.

Boschetti, Nicolò, Nathaniel G. Gordon and Gregory Falco. 2022. "Space Cybersecurity Lessons Learned from the ViaSat Cyberattack." https://doi.org/10.2514/6.2022-4380.

Bratich, Jack. 2020. "Civil Society Must Be Defended: Misinformation, Moral Panics, and Wars of Restoration." *Communication, Culture and Critique* 13 (3): 311-332. https://doi.org/10.1093/ccc/tcz041.

CERT-EU. 2023. "Russia's war on Ukraine: one year of cyber operations". https://cert.europa.eu/static/threat-intelligence/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf.

CERT-UA. 2022a. "Fragment of the study of cyberattacks 14.01.2022". https://cert.gov.ua/article/18101.

—. 2022b. "Sandworm Group Cyberattack (UAC-0082) on Ukrainian energy objects using INDUSTROYER2 and CADDYWIPER malware (CERT-UA#4435)". https://cert.gov.ua/article/39518.

Cyber Security Intelligence. 2022. "State Service of Special Communications & Information Protection of Ukraine (SSSCIP)". https://www.cybersecurityintelligence.com/state-service-of-special-communications-and-information-protection-of-ukraine-ssscip-7222.html.

Davydiuk, Andrii and Vitalii Zubok. 2023. "Analytical Review of the Resilience of Ukraine's Critical Energy Infrastructure to Cyber Threats in Times of War." *15th International Conference on Cyber Conflict: Meeting Reality (CyCon).* Tallinn, ESTONIA: IEEE. 121-139. doi:10.23919/CyCon58705.2023.10181813.

Furstenau, Leonardo Bertolin, Michele Kremer Sott, Andrio Jonas Ouriques Homrich and Liane Mahlmann Kipper. 2020. "20 Years of Scientific Evolution of Cyber Security: a Science Mapping." *International Conference on Industrial Engineering and Operations Management.* Dubai, UAE: IEOM Society International. https://www.researchgate.net/publication/340413661_20_Years_of_Scientific_Evolution_of_Cyber_Security_a_Science_Mapping.

Gatlan, Sergiu. 2024. *"Russian hackers wiped thousands of systems in KyivStar attack"*. https://www.bleepingcomputer.com/news/security/russian-hackers-wiped-thousands-of-systems-in-kyivstar-attack/.

Geissler, Dominique, Dominik Bär, Nicolas Pröllochs and Stefan Feuerriegel. 2023. ”Russian propaganda on social media during the 2022 invasion of Ukraine.” *EPJ Data Science* 12 (1). doi:10.1140/epjds/s13688-023-00414-5.

Hernandez-Castro, Julio, Edward Cartwright and Anna Stepanova. 2017. ”Economic Analysis of Ransomware.” https://ssrn.com/abstract=2937641.

Hernandez-Castro, Julio andEdward Cartwright. 2020. ”An economic analysis of ransomware and its welfare consequences.” *The Royal Society Open Science.*

Hupperich, Thomas. 2023. ”On DDoS Attacks as an Expression of Digital Protest in the Russo-Ukrainian War 2022.” *2023 International Symposium on Networks, Computers and Communications.* Doha, Qatar: IEEE. doi:10.1109/ISNCC58260.2023.10323968.

Khonji, Mahmoud, Youssef Iraqi and Andrew Jones. 2013. ”Phishing Detection: A Literature Survey.” *IEEE Communications Surveys & Tutorials* 15 (4): 2091 - 2121. doi:10.1109/SURV.2013.032213.00009.

Kizilova, Kseniya. 2022. ”Assessing Russian Public Opinion on the Ukraine War.” *Social Science Open Access Repository* 2-5. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-86994-6.

Kloba, Lev andTaras Kloba. 2022. ”Cyber threats of the banking sector in the conditions of the war in Ukraine.” *Financial and Credit Activity - Problems of Theory and Practice* 5 (46): 19-28. doi:10.55643/fcaptp.5.46.2022.3883.

Kozak, Pavel, Ivo Klaban and Tomáš Šlajs. 2023. ”Industroyer cyber-attacks on Ukraine's critical infrastructure.” *2023 International Conference on Military Technologies (ICMT).* Brno, Czech Republic: IEEE. 1-6. doi:10.1109/ICMT58149.2023.10171308.

Krithika, N. 2017. ”A study on wha (watering hole attack)–the most dangerous threat to the organisation.” *International Journal of innovations in Scientific and Engineering Research (IJISER)* 4 (8): 196-198. https://web.archive.org/web/20180421102442id_/http://www.ijiser.com/paper/2017/vol4issue8/Aug2017p101.1.pdf.

Lee, Chia-yi. 2022. ”Why do terrorists target the energy industry? A review of kidnapping, violence and attacks against energy infrastructur.” *Energy Research & Social Science* 87 (8): 102459. doi:10.1016/j.erss.2021.102459.

Lewis, James A. 2022. ”Cyber War and Ukraine.” https://www.csis.org/analysis/cyber-war-and-ukraine.

Liedekerke, Arthur de and Kira Frankenthal. 2023. ”The Cyber Dimension in Russia's War of Aggression.” doi:10.5771/9783748917205-239.

Lilly, Bilyana, Kenneth Geers, Greg Rattray and Robert Koch. 2023. ”Business@War: The IT Companies Helping to Defend Ukraine.” *15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (IEEE) 71-83. doi:10.23919/CyCon58705.2023.10181980.

Lonergan, Erica D, Margaret W Smith and Grace B. Mueller. 2023. ”Evaluating Assumptions About the Role of Cyberspace in Warfighting: Evidence from Ukraine.” *15th International Conference on Cyber Conflict (CyCon).* Tallinn, ESTONIA: IEEE. 85-102. https://doi.org/10.23919/CyCon58705.2023.10182101.

Matania, Eviata and Udi Sommer. 2023. ”Tech titans, cyber commons and the war in Ukraine: An incipient shift in international relations.” https://doi.org/10.1177/00471178231211500.

McFail, Michael, Jordan Hanna and Daniel Rebori-Carretero. 2021. ”Detection Engineering in Industrial Control Systems. Ukraine 2016 Attack: Sandworm Team and Industroyer Case Study.” *The MITRE Corporation* 2-3. https://www.mitre.org/sites/default/files/2022-04/pr-22-0094-detection-engineering-in-industrial-control-systems-ukraine-2016-attack-case-study.pdf.

Mcwhorter, Dan. 2014. ”APT28 Malware: A Window into Russia’s Cyber Espionage Operations?”. https://www.mandiant.com/resources/blog/apt28-a-window-into-russias-cyber-espionage-operations.

Microsoft. 2022. ”Destructive malware targeting Ukrainian organizations”. https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

Mohurle, Savita and Manisha Patil. 2017. ”A brief study of Wannacry Threat: Ransomware Attack 2017.” *International Journal of Advanced Research in Computer Science* 8 (5). https://www.ijarcs.info/index.php/Ijarcs/article/view/4021.

Paniotto, Volodymyr. 2020. ”The Attitude of Ukraine’s Population to Russia and Russia’s Population to Ukraine (2008–2020).” *NaUKMA Research Papers Sociology* 3: 3-14. doi:10.18523/2617-9067.2020.3.3-14.

Patil, Dharmaraj, Tareek Pattewar, Shailendra Pardeshi, Vipul Punjabi and Rajnikant Wagh. 2022. ”Learning to Detect Phishing Web Pages Using Lexical and String Complexity Analysis.” https://eudl.eu/doi/10.4108/eai.20-4-2022.173950.

Paverman, Joseph Herbert. 2019. ”An Examination of Cyber-Attacks Carried Out by Russia to Perpetuate Expansion.” *Utica College ProQuest Dissertations Publishing.* https://www.proquest.com/openview/a0cb326bdab5e2f4c65f0baca4d2ab47/1?pq-origsite=gscholar&cbl=18750&diss=y.

Proska, Ken, John Wolfram, Jared Wilson, Dan Black, Keith Lunden, Daniel Kapellmann Zafra, Nathan Brubaker, Tyler Mclellan and Chris Sistrunk. 2023. ”Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology”. https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology.

Radu, Claudiu-Cosmin. 2022. ”Russia’s approach to cyberspace.” *International Scientific Conference Strategies XXI. Volume XVIII.* Bucureşti: “Carol I” National Defence University Publishing House. 533-544. https://doi.org/10.53477/2971-8813-22-61.

Ratten, Vanessa. 2022. ”The Ukraine/Russia conflict: Geopolitical and international business strategies.” *Thunderbird - International Business Review* 65 (2): 265-271. https://doi.org/10.1002/tie.22319.

Sapuppo, Mercedes. 2023. ”Ukrainian telecoms hack highlights cyber dangers of Russia’s invasion”. https://www.atlanticcouncil.org/blogs/ukrainealert/ukrainian-telecoms-hack-highlights-cyber-dangers-of-russias-invasion/.

Smith, Margaret W. and Thomas Dean. 2023. ”The Irregulars: Third-Party Cyber Actors and Digital Resistance Movements in the Ukraine Conflict.” *15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* 103-119. doi:10.23919/CyCon58705.2023.10182061.

Soesanto, Stefan. 2023. ”Ukraine's IT Army.” *Global Politics and Strategy* 65 (2): 93-106. https://doi.org/10.1080/00396338.2023.2218701.

SSSCIP. 2022a. ”A fragment of the January 14 cyber attack investigation has been published”. https://www.cip.gov.ua/en/news/opublikovano-fragment-doslidzhennya-kiberatak-14-sichnya.

—. 2022b. ”A new program erasing data from computers has been detected”. https://www.cip.gov.ua/en/news/viyavleno-novu-programu-yaka-stiraye-dani-z-komp-yuteriv.

—. 2022c. ”Cyberattack against Ukrtelecom on March 28: the details”. https://www.cip.gov.ua/en/news/kiberataka-na-ukrtelekom-28-bereznya-detali.

—. 2022d. ”Cyberattacks against Ukraine are carried out by Russian military hackers”. https://www.cip.gov.ua/en/news/cyberattacks-against-ukraine-are-carried-out-by-russian-military-hackers.

—. 2022e. ”Cyberattacks on the sites of military structures and state banks”. https://www.cip.gov.ua/en/news/shodo-kiberataki-na-saiti-viiskovikh-struktur-ta-derzhavnikh-bankiv.

—. 2022f. ”Four Months of War: Cyberattack Statistic”. https://www.cip.gov.ua/en/news/chotiri-misyaci-viini-statistika-kiberatak.

—. 2022g. ”Hackers mainly attack state institutions, telecommunication operators, local authorities, logistics companies and medical resources of Ukraine”. https://www.cip.gov.ua/en/news/khakeri-atakuyut-perevazhno-derzhavni-ustanovi-operatoriv-zv-yazku-miscevi-organi-vladi-logistichni-kompaniyi-ta-mediaresursi-ukrayini.

—. 2022h. ”Heavy cyberattack on Ukraine's energy sector prevented. https://www.cip.gov.ua/en/news/poperedzhena-masshtabna-kiberataka-na-energetichnii-sektor-ukrayini.

—. 2022i. ”Latest update on networks operation in Ukraine as of April 11, 15:00”. https://www.cip.gov.ua/en/news/operativna-informaciya-derzhspeczv-yazku-pro-robotu-mobilnogo-zv-yazku-internetu-ta-cifrovogo-telebachennya-v-ukrayini-stanom-na-15-00-11-kvitnya-2022-roku.

—. 2022j. ”Russian cyberattack on the OLL.TV service”. https://www.cip.gov.ua/en/news/kiberataka-rosiyi-na-servis-oll-tv.

—. 2022k. ”Russian cyberwarfare against Ukraine seem to have reached its peak”. https://www.cip.gov.ua/en/news/rosiiski-kibernastupalni-operaciyi-na-ukrayinu-imovirno-dosyagli-svogo-maksimalnogo-potencialu.

—. 2022l. ”Russian hackers attempted to cut electricity supply to many Ukrainians”. https://www.cip.gov.ua/en/news/rosiiski-khakeri-namagalisya-pozbaviti-dostupu-do-elektroenergiyi-znachnu-kilkist-ukrayinciv.

—. 2022m. ”Russian Invaders Disabled Communication Services in the South of Ukraine”. https://www.cip.gov.ua/en/news/rosiiski-okupanti-vidklyuchili-zv-yazok-na-pivdni-ukrayini.

—. 2022n. ”SSSCIP's State Centre of Cybersecurity has neutralized an attack on public authorities' websites”. https://www.cip.gov.ua/en/news/derzhavnii-centr-kiberzakhistu-derzhspeczv-yazku-neitralizuvav-ataku-na-saiti-derzhavnikh-organiv.

—. 2022o. ”Starlink in Ukraine: How Elon Musk's Satellite Internet is Helping Now and What the Prospects Are”. https://www.cip.gov.ua/en/news/starlink-v-ukrayini-yak-suputnikovii-internet-vid-ilona-maska-dopomagaye-zaraz-ta-yaki-perspektivi.

—. 2022p. *"Statistics of Cyber Attacks on Ukrainian Critical Information Infrastructure: 15-22 March"*. https://www.cip.gov.ua/en/news/statistika-kiberatak-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-15-22-bereznya.

—. 2022q. "The war continues not only on land, in the air and at sea. Cyberspace has also become an arena for hostilities". https://www.cip.gov.ua/en/news/the-war-continues-not-only-on-land-in-the-air-and-at-sea-cyberspace-has-also-become-an-arena-for-hostilities.

—. 2022r. "Today's attacks are a continuation of the attacks that took place on February 15". https://www.cip.gov.ua/en/news/23-lyutogo-2022-roku-stavsya-chergovii-akt-kiberagresiyi-proti-ukrayini.

—. 2022s. "Ukraine is not the only target for russian hackers, but a major one". https://www.cip.gov.ua/en/news/ukrayina-ne-yedina-cil-rosiiskikh-khakeriv-prote-odna-z-golovnikh.

—. 2022t. "Ukrainian television and radio are back in Kherson". https://www.cip.gov.ua/en/news/do-khersona-povernulosya-ukrayinske-telebachennya-i-radio.

—. 2022u. "Within a month of war, there were already three times more hacker attacks than during the same period last year". https://www.cip.gov.ua/en/news/za-misyac-viini-vzhe-stalosya-maizhe-vtrichi-bilshe-khakerskikh-atak-riznogo-vidu-nizh-za-analogichnii-period-minulogo-roku.

—. 2023a. "A Cyberattack Failed to Disrupt Ukrinform News Agency". https://www.cip.gov.ua/en/news/kiberataka-ne-zmogla-zupiniti-robotu-informaciinogo-agentstva-ukrinform.

—. 2023b. "At least 23 russian cyber terrorist groups act against Ukraine". https://www.cip.gov.ua/en/news/proti-ukrayini-pracyuyut-shonaimenshe-23-rosiiski-kiberteroristichni-khakerski-grupi.

—. 2023c. "Attacks against IT companies and specialized software developers as a threat to critical infrastructure". https://www.cip.gov.ua/en/news/ataki-na-it-kompaniyi-ta-specializovanikh-rozrobnikiv-pz-yak-zagroza-kritichnii-infrastrukturi.

—. 2023d. "CERT-UA experts are investigating a cyberattack against Kyivstar telecom operator's network". https://www.cip.gov.ua/en/news/fakhivci-cert-ua-doslidzhuyut-kiberataku-na-merezhu-telekom-operatora-kiyivstar.

—. 2023e. "Cyberattack on the State Statistics of Ukraine: the enemy reports another non-existent «victory»". https://www.cip.gov.ua/en/news/kiberataka-na-derzhstat-ukrayini-vorog-ukotre-prozvituvav-pro-peremogu-yakoyi-ne-bulo.

—. 2023f. "Cybercriminals tried to steal data, disguising themselves as Ukrainian MFA". https://www.cip.gov.ua/en/news/kiberzlovmisniki-namagalisya-vikradati-dani-maskuyuchis-pid-ukrayinske-mzs.

—. 2023g. "How russian and pro-russian hackers attack Ukraine". https://www.cip.gov.ua/en/news/yaki-rosiiski-ta-prorosiiski-khakeri-atakuyut-ukrayinu.

—. 2023h. "Local public authorities are among the key targets for russian hackers". https://www.cip.gov.ua/en/news/miscevi-organi-vladi-odna-z-osnovnikh-mishenei-rosiiskikh-khakeriv.

—. 2023i. ”Russian hackers attacked users in Ukraine and Poland once again: this time they used emails containing links to «documents»”. https://www.cip.gov.ua/en/news/rosiiski-khakeri-vchergove-atakuvali-koristuvachiv-ukrayini-ta-polshi-cogo-razu-za-dopomogoyu-elektronnikh-listiv-z-posilannyami-na-dokumenti.

—. 2023j. ”Russian hacking group Turla attacks defense forces using CAPIBAR and KAZUAR malware — CERT-UA investigation”. https://www.cip.gov.ua/en/news/rosiiske-ugrupuvannya-turla-spryamovuye-ataki-proti-sil-oboroni-vikoristovuyuchi-shkidlivi-programi-capibar-ta-kazuar-doslidzhennya-cert-ua.

—. 2023k. ”Targeted cyberattacks remain among the major cyber threats posed by the FSB hackers — Report”. https://www.cip.gov.ua/en/news/targetovani-kiberataki-zalishayutsya-odniyeyu-z-osnovnikh-kiberzagroz-vid-khakeriv-iz-fsb-zvit.

—. 2023l. ”The attack on Ukrinform might have been carried out by the Sandworm hacking group, associated with russian GRU: preliminary results of CERT-UA investigation”. https://www.cip.gov.ua/en/news/ukrinform-mogli-atakuvati-khakeri-z-ugrupuvannya-sandworm-pov-yazanogo-z-rosiiskim-gru-poperedni-dani-doslidzhennya-cert-ua.

Steinbrecher, Dominique. 2022. ”Viasat KA-SAT attack (2022)”. https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_(2022).

Sullivan, Scott. 2023. ”Unpacking Cyber Neutrality.” *15th International Conference on Cyber Conflict (CyCon)*. Talinn, ESTONIA: IEEE. 9-23. https://www.ccdcoe.org/uploads/doc/CyCon_2023_book_print.pdf.

Tarasenko, Oleh, Dmytro Mirkovets, Artem Shevchyshen, Oleksandr Nahorniuk-Danyliuk and Yurii Yermakov. 2022. ”Cyber security as the basis for the national security of Ukraine.” *Cuestiones Politicas* 40 (73): 583-599. https://doi.org/10.46398/cuestpol.4073.33.

Temple-Raston, Dina. 2023. ”In recent interview, ousted Ukrainian cyber official spoke about new Russian attacks, long-term plans”. https://therecord.media/victor-zhora-interview-click-here-ousted.

Visvizi, Anna and Miltiadis D. Lytras. 2020. ”Government at risk: between distributed risks and threats and effective policy-responses.” *Transforming Government: People, Process and Policy* 14 (3): 333-336. https://doi.org/10.1108/TG-06-2020-0137.

Willett, Marcus. 2022. ”The Cyber Dimension of the Russia–Ukraine War.” *Global Politics and Strategy* 64 (5): 7-26. https://doi.org/10.1080/00396338.2022.2126193.

Wilson, Richard L. and Alexia Fitz. 2023. ”Nuclear Weapons, Cyber Warfare, and Cyber Security: Ethical and Anticipated Ethical Issues.” *Proceedings of the 18th International Conference on Cyber Warfare and Security Vol. 18 No. 1.* Baltimore, MD: Towson University. 440-448. https://doi.org/10.34190/iccws.18.1.1050.