DOI 10.33099/2618-1614-2023-23-4-48-56
UDC 355.4:004.056.5

V. V. Mashtalir,
Doctor of Historical Science, Professor,
Head of the Institute of Information and Communication Technologies and Cyber Defence,
the National Defence University of Ukraine, Colonel,

V. V. Shypovskyi,
PhD Student at the Science and Technology Management Centre,
the National Defence University of Ukraine,
Lieutenant Colonel

Analysis of the cyber domain during the Russian-Ukrainian war 2022: conclusions, recommendations, lessons learned

The Russian invasion of Ukraine demonstrated the spread of modern military operations to almost all aspects of daily life. The development of the internet and widespread use of digital technologies mean that virtually everything, from water supply to banking services, can fall into the hands of criminals and be disrupted. The article analyses events in the cyber domain related to the large-scale Russian Federation's invasion of Ukraine starting from 2014 when Crimea was annexed and armed conflict began in eastern Ukraine. It presents statistical data on cyber-attacks carried out, depicts the structure of both sides' confrontation, and describes new ways of applying cyber influence in conjunction with other dimensions of processes related to Russian occupation actions. Moreover, the article reveals changes in the targets of cyber operations depending on the political situation worldwide or the situation on the battlefield.

Key words: cyber defence, cyber resilience, information technologies, critical infrastructure, cyber operation, cyber warfare.

Introduction. Cyber-attacks on Ukraine began before the invasion. The intensity of cyber-attacks began to increase significantly in January and peaked in February. Only during 23 February 2022, Russia has attacked 19 government and critical infrastructure facilities. This was done by the same hacker group that launched the NotPetya virus in 2017 and that works for Russian military intelligence.

Cyber threats to the Ukrainian state and society can be conditionally divided into two key levels. The first – «classic» cybercrimes – both completely original and already common, they require only modern information technologies for their implementation. The second is crimes characteristic of geopolitical struggle (or such crimes at the local level that have the potential to affect the political situation of the state): hacktivism, cyber espionage and cyber sabotage. At the same time, the attack techniques in both cases show a lot in common. For example, phishing techniques can be used both for seizing citizens' funds and for the purpose of cyber espionage

Statistics and analytics. During 2022 Russian cyber-attacks against 128 targets in 42 countries have been recorded, including against targets allegedly related to aid to Ukraine [1]:

- 49% – for government structures. But there were also attacks on energy, defence and other strategic companies. Most of the attacks are against NATO countries.
- 29% of attacks were successful. A quarter of successful attacks result in stolen data. Figure 1 shows the directions that were most attacked by Russian special forces.

Since the beginning of Russia's full-scale war against Ukraine, DDoS attacks have remained among the most common types of cyberattacks used by hostile hackers [2]. Since the beginning of this year, a number of websites of state bodies and banking institutions, telecom operators, companies in the energy sector, websites of regional authorities, media, etc. have been subjected to DDoS attacks. Usually, DDoS attacks are carried out with the aim of spreading panic and destabilization. Sometimes used to hide destructive actions, that is, when a DDoS attack serves as a cover for another type of attack. However, DDoS attacks themselves do not pose a threat to personal data of citizens. It is worth knowing that hackers often use hacked devices of people to carry out DDoS attacks. Therefore, it is important to follow the basic rules of cyber hygiene, use antiviruses, update software in a timely manner, etc.

The analysis of cyberattacks on the information infrastructure of Ukraine will be expediently considered from 2014 – because it was from this year that Russia began to act beyond the borders of the information space: it was in 2014 that Russia annexed Crimea and began hybrid actions in the East of Ukraine, occupying part of Donbas.

Russian-Ukrainian Cyber War since 2014. The first attacks on information systems of private enterprises and government institutions in Ukraine were recorded during

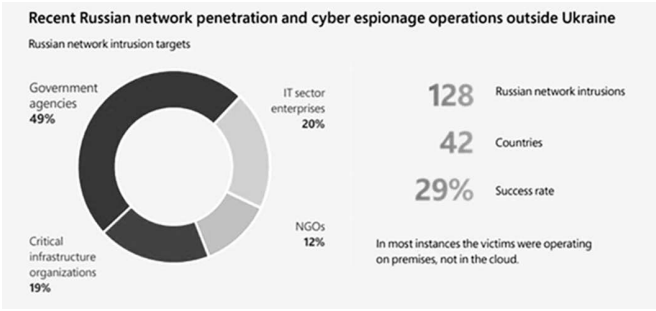

Fig. 1. Russian cyber operations outside Ukraine (source: [1])

the mass protests in 2013. The Russo-Ukrainian cyber war became the first conflict in cyberspace where a successful attack on the energy system with its disruption took place. There were attacks against the «Elections» information system during the presidential elections, numerous denial-of-service attacks, defacements, cyber espionage, and more.

On 5 March 2014, a phone call between the foreign ministers of Estonia and the EU surfaced on the Internet, containing fake information claiming that Ukrainian opposition forces were behind the sniper shootings on the Maidan Square. This viewpoint was actively promoted by Russian propaganda. In March 2014, during the early stages of Crimea's occupation, Russian intelligence services blocked communication between Ukrainian parliamentarians and the Security Service of Ukraine units in Crimea using an IP-telephone attack.

From 21 to 25 May, DDoS attacks and website hacking occurred during the presidential elections, leading to the publication of false results on the Central Election Commission's website. Despite reports of the hacking, these data were presented as real election results in Ukraine on Russian Channel One.

In June 2014, harmful programs engaged in cyber espionage, such as Turla/Uroburos/Snake, RedOctober, MiniDuke, and NetTraveler, were discovered on the servers of private companies in Ukraine and NATO countries. Analysis indicated that these programs were developed in Russia.

Since 2014, terrorist groups fighting in Donbas have been conducting signals intelligence, hacking into databases to obtain information on the locations of phones and Wi-Fi networks used by Ukrainian Armed Forces.

In October 2015, a private investigation revealed that Russian cyber espionage targeted data related to the investigation of the MH17 flight disaster, conducted by Dutch, Malaysian, Australian, Belgian, and Ukrainian authorities.

On 23 December 2015, approximately 30 substations of Prykarpattiaoblenergo were disabled using the Trojan program BlackEnergy3, which had been previously associated with Russian hackers. As a result, more than 200,000 residents of Ivano-Frankivsk Oblast were left without electricity for a duration of one to five hours. Similar attacks also occurred on Kyivoblenergo and Chernivtsioblenergo. This was the first cyber-attack against the Critical Infrastructure of Ukraine.

On 6 December 2016, a hacker attack targeted the internal telecommunications networks of the Ministry of Finance, the State Treasury, and the Pension Fund, causing the disruption of several computers and the destruction of critical databases, leading to delays in budgetary payments amounting to hundreds of millions of hryvnias.

On 15 December 2016, Ukrainian hackers, commissioned by an unidentified individual from St. Petersburg, carried out a DDOS attack on the Ukrzaliznytsia website, completely blocking its operation for a day. The attack was believed to be aimed at stealing data on passenger transportation.

On 17 December 2016, a cyber-attack on the North Substation of Ukrenergo led to a failure in the control automation system, leaving several hours without electricity the northern part of the right-bank Kyiv and adjacent areas of the region.

On 27 June 2017, a massive cyber-attack using the NotPetya (also known as Petya.A) virus disrupted the operations of numerous Ukrainian state and private enterprises, including the Borispol airport, Ukrtelecom, Chernobyl Nuclear Power Plant, Ukrzaliznytsia, the Cabinet of Ministers, and several media outlets [3]. *Figure 2* shows a screenshot of the NotPetya deface attack. It was noted on the monitors that the victim could return the encrypted data by sending the ransom to the specified address. But in reality, this option was not available, that is, the attack was an act of ordinary vandalism with the aim of destroying critical information infrastructure.

The Security Service of Ukraine (SBU) attributed the attack to Russian intelligence services.

Analysing the goals of cyber operations against the information infrastructure of Ukraine starting in 2014, the cyber troops of the Russian Federation aimed to physically destroy the state's critical infrastructure. That is why the protection of information systems of critical infrastructure objects is of critical importance during warfare.

Fig.2. NotPetya virus screenshot

In 2014, the leadership of Ukraine understood that the enemy has new tools of invisible and unproven destructive influence on the country. On 27 January 2016, the National Security and Defence Council of Ukraine adopted the Cyber Security Strategy of Ukraine [4], and this became a kind of «vaccination» for how to response to new challenges.

Cyberattacks chronology in 2022. The official website of the State Service of Special Communications and Information Protection of Ukraine [5] notes the following chronology of cyberattacks since the beginning of Russia's large-scale invasion of Ukraine.

13–14 January 2022. Massive Attack on Ukrainian Government Websites. During the night of January 13 to 14, hackers launched a massive attack on Ukrainian government websites. This includes the websites of the Ministry of Education, Ministry of Foreign Affairs, Ministry of Sports, Ministry of Energy, Ministry of Agriculture, Ministry of Veterans Affairs, Ministry of Environment, State Emergency Service, and State Treasury.

The Security Service of Ukraine (SBU) together with the State Special Communications Service and Cyber Police suspect that the government websites were hacked by hacker groups associated with Russian special services. However, the National Security and Defence Council of Ukraine has different suspects and stated: «Preliminarily, we believe that the UNC1151 – a cyber espionage group associated with the Belarusian special services – may be involved in this attack.»

This attack was called a supply chain attack, meaning it was carried out through a chain of supply. The attackers compromised the infrastructure of a commercial company that had administrative access to the affected websites, allowing them to conduct the attack.

It is worth noting that all affected government websites were built on the October CMS content management system, and almost all of them were developed by a single private company. *Figure 3* shows a screenshot of an attack on Ukrainian government websites, which contains a threatening message in Russian, Ukrainian, and Polish.

Fig. 3. Deface cyberattack screenshot

The current working theory suggests a combination of three attack vectors: the supply chain attack and the exploitation of vulnerabilities in October CMS and Log4j. The attack allowed the perpetrators to modify the main pages of the websites and block access to everything else. According to the head of the State Special Communications Service, available data indicates that the cyber-attacks were well-prepared, carried out by a coordinated group of hackers, and executed at a high operational level. The attribution points to the involvement of Russian hacker groups. In 2021, there were identifications of cyber-attacks by Russian special services on a significant portion of the currently affected institutions, as stated by the head of the organization.

26 January 2022. Cyber-Attack on Ukraine.ua Website. During the night of January 26, a cyber-attack was launched on the official website of Ukraine, Ukraine.ua. As a result of the attack, the website was unavailable to users for several hours.

15 February 2022. Cyber-Attacks on Banks and Ministry of Defence Websites. The hackers took advantage of a DDoS attack on the official website of the Ministry of Defence of Ukraine, overwhelming the server's capacity with an excessive number of requests per second. It appears that they were aware that the website was protected against classical DDoS attacks, leading them to seek vulnerabilities in the site's code. As a result, the attack was effective.

The largest Ukrainian bank, Oshchadbank, also faced a DDoS attack, but their systems were well protected and operated in a normal mode. However, there was some slowdown in accessing the Oshchad 24/7 system due to increased communication channel load.

Another target was Privatbank, which experienced a DDoS attack. Although the bank's services were successfully restored, Privat24, a banking service, remained unstable for a period.

Following the attacks on banks and government websites, there was a powerful DDoS attack on the Diia (Action) portal. Initially originating from Russia and China hundreds of thousands of packets of malicious traffic per second, the attack was quickly blocked by Ukrainian experts. However, the attack resumed from servers located in the Czech Republic and Uzbekistan. Fortunately, the attack went unnoticed by Diia portal users.

In addition, the CERT-UA (Computer Emergency Response Team Ukraine) noted the occurrence of DDoS on Ukrainian bank and government website resources. Investigation, including information from partners, revealed the involvement of Mirai and Meris botnets in the attacks. The use of readily available malicious traffic from cybercriminals, known as DDoS-as-a-Service, was also considered. DNS-server-based DDoS attacks were used to prevent access to government websites in the gov.ua domain by disrupting DNS servers.

On 23 February 2022, a new series of mass DDoS attacks targeted the websites of government and banking

institutions. Some of the attacked information systems became inaccessible or operated with disruptions, leading to rerouting traffic to minimize damage. However, other sites effectively resisted the attacks and operated normally.

Phishing attacks on government authorities and critical infrastructure objects, distribution of malicious software, and attempts to breach private and public sector networks for further destructive actions also increased in tandem with the DDoS attacks.

The cybersecurity teams of various institutions, internet providers, and IT teams of critical information infrastructure objects worked around the clock to ensure the availability and integrity of information resources.

The attackers behind these cyber-attacks were blatant in their actions and used botnets for phishing campaigns and DDoS attacks. Ukrainian intelligence agencies attribute the attacks to hackers associated with the aggressor country, Russia.

On 24 February 2022, Viasat, a media company, was subjected to a massive cyber-attack, leading to disruptions in the operation of Ukrainian government websites. The incident is suspected to be connected with Russian hackers. According to SentinelOne, the cyber-attack involved the Wiper virus strain called AcidRain, which was discovered on 15 March. The virus destroys data and renders devices unusable after rebooting. The identities of the hackers behind the attack have not been established. However, researchers noted similarities between AcidRain and the VPNFilter virus, which had been linked to Russian hacking groups Fancy Bear and APT28 by the FBI.

On 25 February 2022, the State Special Communications Service and Information Protection of Ukraine reported mass phishing emails sent to the email addresses of Ukrainian military personnel on i.ua and meta.ua services. These phishing attacks targeted private mailboxes of Ukrainian military personnel and individuals associated with them. After compromising the account, the attackers downloaded the entire mailbox content using the IMAP protocol and obtained contact addresses for further distribution. The UNC1151 group, located in Minsk and consisting of officers of the Ministry of Defence of Belarus, is believed to be behind these actions.

Russian cyber war actors. According to the information available up to that point, it was believed that the Russian cybertroops operated under the umbrella of the Russian military and intelligence agencies. Here is a general overview of their structure and assigned next roles. The structure of the state cyber forces of the Russian Federation is shown in *Figure 4*.

Main Intelligence Agency (GRU) Cyber Units:

The GRU, known as the Main Intelligence Agency, serves as Russia's military intelligence agency. Its responsibilities include gathering and analysing intelligence and conducting cyber operations to support Russia's military objectives. GRU cyber units are highly

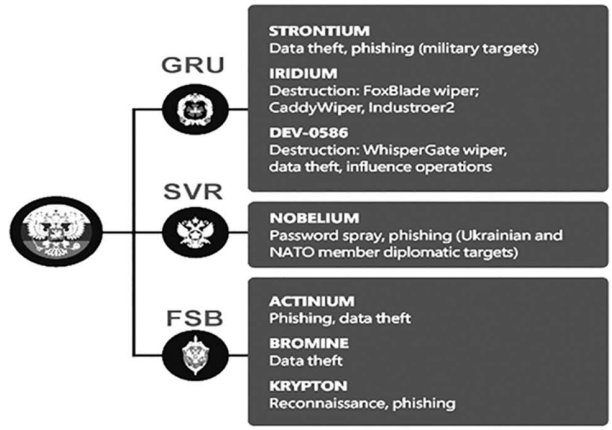

Fig. 4. Russian cyber troops structure (source: [1])

advanced and engage in offensive cyber activities, such as hacking, infiltrating networks, and conducting cyber espionage.

Federal Security Service (FSB) Cyber Division:

The FSB is Russia's domestic security agency responsible for counterintelligence, counterterrorism, and national security matters. The FSB Cyber Division focuses on carrying out cyber operations against domestic and foreign targets considered threats to Russia's national security.

Ministry of Defence Cyber Commands:

The Russian Ministry of Defence is in charge of the country's military affairs and national defence. Within the Ministry of Defence, specific cyber commands or units are likely responsible for conducting cyber operations to support military objectives and safeguard critical military infrastructure.

Presidential Executive Office:

The Presidential Executive Office plays a crucial role in Russia's governance, advising and assisting the President in policy-making and administrative matters.

While specific details may be limited, this office is believed to be involved in coordinating and directing strategic cyber efforts in alignment with Russia's broader foreign policy goals.

State-sponsored Hacktivist and Proxy Groups:

Russia has faced accusations of employing state-sponsored hacktivist groups or utilizing proxy groups to conduct cyber operations on its behalf. These groups may have varying degrees of affiliation with Russian intelligence agencies or government entities. They are often engaged in disinformation campaigns, propagating propaganda, and launching cyber-attacks against political opponents and other countries.

It's essential to emphasize that attributing actions in the cyber domain can be challenging, and specific

responsibilities and affiliations of various cyber units may not always be transparent. It's crucial that the landscape of cyber warfare is constantly evolving, and governments worldwide continuously adapt their cyber capabilities and organizational structures in response to emerging threats and challenges.

To understand the forces and means that effectively oppose the Russian invaders and protect the Ukrainian national cyberspace, it will be important to understand the directions of work of the elements of the National Cyber Security System of Ukraine.

National Cybersecurity System of Ukraine. For a broad understanding of Ukrainian forces and means of defence in cyberspace, it is necessary to consider the National Cyber Defence System, the elements of this system and the features of its application.

The National Cybersecurity System is a combination of cybersecurity assurance entities and interconnected measures of organizational, legal, political, socio-economic, scientific-technical, law enforcement, defence, informational, and educational nature, as well as measures for information protection and cybersecurity.

The main entities of the national cybersecurity system are the State Special Communications and Information Protection Service of Ukraine, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defence of Ukraine, the General Staff of the Armed Forces of Ukraine, intelligence agencies, and the National Bank of Ukraine [6].

Ukraine has taken major steps to improve its cyber resilience in recent years. The creation of the National Cybersecurity Coordination Centre in 2016 and proposed updates to cybercrime laws align with international best practices. Ukraine's close cooperation on cyber defence with other nations also enhances its capabilities [7].

However, Ukraine's National Cybersecurity Strategy identifies ongoing cybersecurity threats. These include Ukraine's outdated electronic communications infrastructure, insufficient critical infrastructure protections, unsystematic cyber defences, and ineffective security sector activities against cyber threats. Additional challenges are inadequate coordination and information sharing among Ukrainian cybersecurity entities. Overall, while Ukraine has made progress, vulnerabilities remain due to outdated systems, uneven protections, and uncoordinated efforts. Further modernization, strengthened critical infrastructure defences, systematic approaches, enhanced security sector activities, and improved collaboration are needed to bolster Ukraine's cyber resilience.

Cyber warfare evolution. In [8], in order to analyse what has contributed to the success of Ukraine's cyber defence, Russia's approach to offensive operations and the tactical adaptations its cyber forces have made to operate under conditions of war were studied. The trends of changing directions of target selection by the Russian special services were successfully reflected. *Figure 5* shows the main phases of cyber warfare during 2022.

Examining Russia's cyber offensive in parallel with its conventional military campaign revealed significant correlations between the two. Throughout each phase, the pattern of cyber operations and their impact on Ukraine's Critical infrastructure underwent adjustments that aligned with Russia's evolving war objectives Russian cyber actors displayed a discernible evolution in their operational priorities, target selection, and tactics, adapting to the shifting dynamics and challenges in the highly contested operating environment [8].

The initial phase of the war showcases Russia's utilization of cyber operations to create shock and surprise, complementing its invasion force. Subsequent phases shed light on Russia's deployment of cyber units in a prolonged war of attrition. Monitoring these changes chronologically provides a unique perspective on the versatile role that cyber operations might assume in future conflicts. It also highlights the specific obstacles Russia encountered in wielding cyber power when rapidly changing operational requirements were driven by events on the ground. Overall, studying Russia's cyber offensive through different phases offers a comprehensive understanding of its strategic intentions and the multifaceted challenges posed by cyber warfare in complex and fast-paced military scenarios. Let's consider the phases of cyber operations and analyse the state in other dimensions for the time intervals indicated in the phases.

Phase 1: Active Preparation (*March 2021 – 23 February 2022*). During the March 2021 phase, Russian cyber groups escalated efforts to gain access to critical infrastructure networks in Ukraine. Russia's cyberattacks on Ukraine aligned with its military escalation, foreshadowing the invasion. As Russian troops amassed near Ukraine's borders, Russian intelligence cyber units reactivated old intrusions of Ukrainian networks dating back to 2019. The GRU cyber

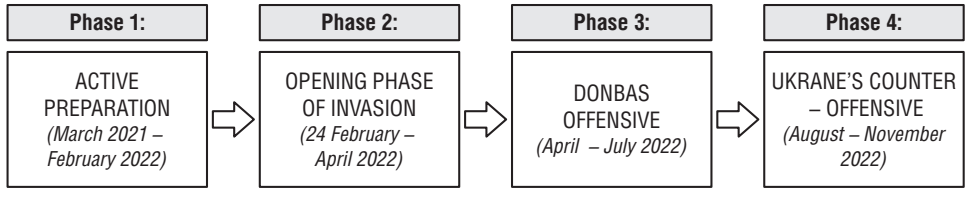

Fig. 5. Cyber warfare phases during 2022 (source: [8])

warfare branch leveraged these dormant access points to launch attacks. The cyber operations employed relatively basic tactics like stealing login credentials, brute-force hacking, and exploiting known security flaws. The goal was to degrade Ukrainian systems and wear down cyber defenders, setting the stage for larger cyberattacks once the planned invasion commenced. Rather than advanced cyber techniques, Russia relied on rudimentary methods to disrupt Ukraine before the kinetic phase. This exemplified Russia's cyber-enabled hybrid warfare strategy, coordinating cyber and military aggression to overwhelm the adversary. However, this move proved a miscalculation, exposing GRU activities prematurely, serving as an early warning for global cyber defenders over a month before the invasion. Russia's invasion anticipated swift success, but the cyber operation drew heightened attention and vigilance from the global cybersecurity community instead [8].

There is a large amount of evidence that Russian hackers were preparing for the invasion in advance, namely from 2021. Consider the report of the company Microsoft for 2021. Data from Microsoft reveals Russia's growing cyber threat. In 2021, over half of all nation-state cyberattacks observed by Microsoft originated from Russia. Moreover, Russian cyber operations were becoming more successful – their compromise rate rose from 21% in 2020 to 32% in 2021. Russian actors primarily targeted government agencies, comprising 53% of attacks versus just 3% in 2020. Their focus was intelligence gathering, especially targeting agencies handling foreign affairs, national security, and defence. The top 3 countries Russia cyber actors struck were the United States, Ukraine, and the United Kingdom [9].

Overall, these statistics highlight the escalating scale, effectiveness, and strategic nature of Russian cyber campaigns against critical government systems and Western nations. This fact also indicates that the Russian foreign intelligence services anticipated help to Ukraine from Great Britain and the United States after the large-scale Russian invasion.

Phase 2: Phase of Invasion (*24 February – April 2022*). The preparatory activities carried out during Phase 1 were extensively leveraged to support Russia's initial campaign aimed at swiftly capturing Kyiv and toppling Ukraine's democratically elected government. Offensive cyber operations (OCOs) were instrumental in disrupting essential elements of Ukrainian society as part of a long-standing campaign to portray Ukraine as a failed state incapable of recovering or maintaining critical services [8].

At the onset of the invasion, Russia aggressively exploited its pre-established access to Ukrainian networks, focusing primarily on high-priority strategic targets within Ukraine. This opening onslaught involved the use of more advanced destructive cyber tools to disrupt command and control (C2) infrastructure, weaken Ukraine's resolve, and create favourable conditions for the success of the invading forces. The intensity of these early cyber operations aligned with Russia's approach of using cyber disruptions as a precursor to military actions and the strategic value of leveraging pre-positioned cyber capabilities at the outset of a conflict [8].

During this phase, Russia's cyber campaign was largely oriented towards counter-value targets, systematically disrupting the Ukrainian government's ability to function and communicate with the public, as well as undermining critical infrastructure functions in civilian areas. For example, HermeticWiper targeted numerous organizations across a broad spectrum of Ukraine's critical infrastructure sectors, including government, aviation, IT, energy, defence industry, agriculture, and financial services. In addition to using more potent cyber tools, Russia also employed less sophisticated ones to disrupt critical infrastructure networks in government, financial services, and media organizations [8].

The experience of cyber defence measures on the part of Ukraine indicates the need for special protection of critical infrastructure objects. The study [10] highlights the most common approaches to assessing the level of cyber protection of information systems, which have a wide range of applications in different countries of the world, and developed a methodology that provides the largest number of solutions. The system of indicators of cyber resilience of information systems of critical infrastructure objects, proposed in [10] provides opportunities for a more qualitative and effective assessment of the level of cyber protection and allows for a comprehensive assessment of cyber resilience of information systems, taking into account various technical and organizational aspects of critical infrastructure information protection. An improved method of factor analysis of information risks for assessment and management of information risks in critical infrastructure systems is given in [11].

The Russian special services had high hopes for Phase 2, as evidenced by the large amount of effort invested immediately before the invasion. Let's consider the relationship between cyber operations by the Russian Federation and key political events related to the Russian government (*Figure 6*).

Despite extensive planning, Russia struggled to sustain its initial intensity of cyberattacks on Ukraine beyond the first week of the war. Russia's cyber operations paused for an extended period after its blitz on Kyiv stalled, forcing a shift in military strategy. It appears Russian cyber units rapidly lost access to Ukrainian systems, hampering efforts to maintain nonstop effects after the initial onslaught. Consequently, later cyberattacks became more tactical and opportunistic as planners hastily leveraged any new network access. Defensive actions by Ukraine and partners from late 2021 onward further degraded Russia's attack capabilities, revealing a disconnect between the GRU's envisioned phase 1 strategy and actual execution [8].

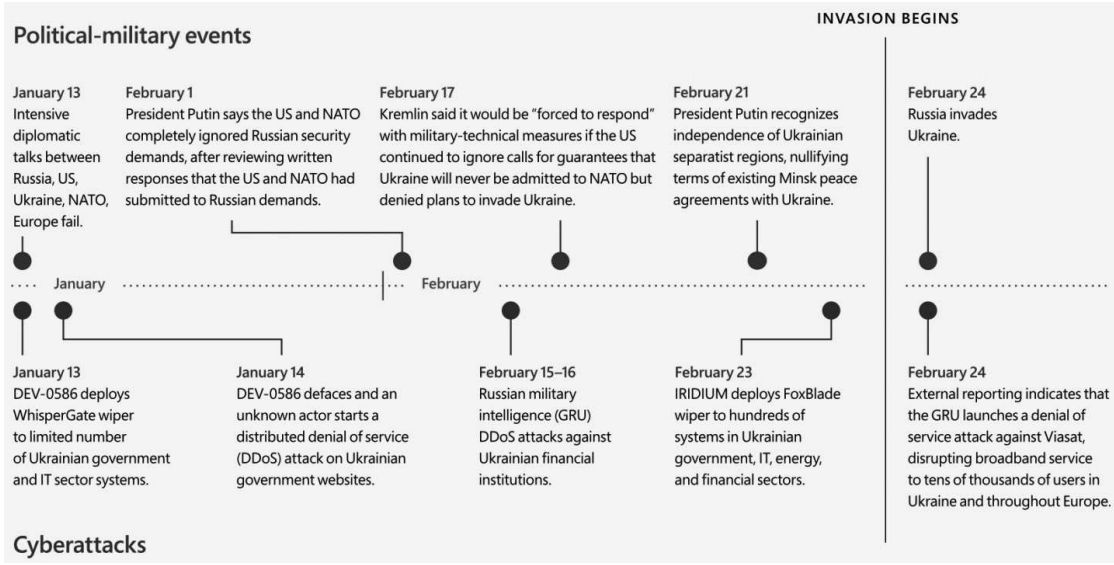

Fig. 6. Political-military events/Cyber-attacks (source: [12])

Analysis of phase 2 prerequisites shows Russian cyberattacks clearly adapted based on changing conditions in Ukraine and globally. This exemplifies Russia synchronizing cyber operations with political developments to maximize its war impact. Despite meticulous preparation, Russia's cyber units failed to sustain the intensity of early operations due to defenders' actions and Russia's military setbacks. This forced a reactive, makeshift approach relying on fleeting access, underscoring the importance of resilient cyber defences to frustrate an aggressor's designs.

Phase 3: Donbas Offensive (*April – July 2022*). Following Russia's unsuccessful initial invasion and pivot to eastern Ukraine, destructive cyberattacks on Ukrainian critical infrastructure declined. Russia refocused its cyber capabilities to enable the impending Donbas offensive.

Rather than continuing disruptive strikes on Ukrainian systems, Russia conserved its cyber resources. This likely aimed to support military operations in eastern Ukraine. By curtailing broad cyberattacks and reserving its most potent cyber weapons, Russia prepared its cyber arsenal to complement the ground assault on Donbas. The shift in cyber strategy indicates Russia learned from the failed Kyiv blitz. By aligning cyber with realistic military plans, Russia hoped to avoid overextending its cyber capabilities early on. This adaptation highlights Russia's efforts to better integrate cyber operations with its larger strategic aims in Ukraine.

GRU hackers used Industroyer2 to attempt power outages in eastern Ukraine, redirecting attention from Kyiv. Reasons for reduced cyber disruptions are unclear. It could be due to the conflict narrowing, making cyber less strategic. Russian cyber forces might have transitioned to intelligence gathering, away from frontline. Aggressive earlier phase took a toll on Russian cyber forces. Challenges in sustaining operations during invasion's second phase emerged. Russia's strategic priorities adapted, targeting Eastern European countries and defence organizations. Simple tactics like phishing, cookie theft, and exploiting known vulnerabilities persisted. Russia incorporated more intermediary tools from criminal markets. Destructive capabilities narrowed, with CaddyWiper emerging as preferred wiper [8].

During phase 3, experts observed a change not only in the intensity of cyber operations, but also in the ways and means of cyber-attacks, which indicates, first of all, a change in the managers of cyber operations against the Ukrainian information infrastructure and the infrastructure of partner countries [13].

Russia's cyber arsenal expanded, but capabilities focused. Adaptive learning demonstrated GRU's aptitude for prolonged conflict. Russia built up cyber forces and refined tools, concentrating them on key targets. Through training, GRU gained proficiency in effectively deploying cyberweapons, integrating them into military strategy. This underscores the systemic nature of the threat. Countering requires robust security and flexible defence adjustment. Critically important are investments in personnel, decision-making, and institutional learning.

In summary, Russia methodically honed its cyber capabilities for wartime application, enabling integrated cyber-kinetic operations. This systemic threat demands durable safeguards and adaptive preparedness. Vital priorities are workforce development, streamlined decisions, and organizational learning to match Russia's focused cyber advances.

Phase 4: Ukraine's Counter-offensive (*August – November 2022*). Russia continued to adjust its operations to address previous challenges in balancing access and action. Russian cyber units exhibited a continued diversification of methods for gaining access to Ukrainian critical infrastructure.

Moreover, they deepened their longstanding preference for commodity tools to quickly supplement their arsenals, alongside internal development resources. Starting in October 2022, there was an increase in reported network attacks, suggesting a more prepared and reinvigorated Russian cyber program compared to the summer period. Particularly noteworthy was the surge in Russian network attacks against energy, water, and logistics organizations, coinciding with deliberate targeting of Ukraine's energy infrastructure using missiles and loitering munitions. This coordination indicated a strategy to intensify cross-domain pressure and deprive civilians of essential services as the winter season approached [8].

Summarizing the 4 phases of 2022, it was found that just like resistance on the battlefield, Russia did not expect resistance in cyberspace from the components of the National Cyber Security System of Ukraine and volunteers of the civilian sector. Analysing the data of the Cyber Incidents Response Operational Centre of the State Cyber Protection Centre of the State Service of Special Communication and Information Protection of Ukraine [14], it is possible to say that Ukraine is now in the phase 5 – Cyber war of attrition. Since the beginning of 2023 (compared to the 4th quarter of 2022), there has been a decrease in the total number of cyberattacks organized by pro-Russian hacktivist groups, but their systematicity and intensity continues to be on a high level. However, Kremlin intensified information operations to justify the unprovoked invasion of Ukraine creating conditions for a protracted war in Ukraine, so there is no fundamental reason to believe that the downward trend in the number of cyber-attacks targeting Ukrainian organizations of various forms of ownership and industries will continue.

Conclusions and Lessons learned.

We have one enemy, and this enemy is well-prepared for future strikes. They are ready to carry out cyber-attacks on democratic countries. To effectively counter Russian hackers, we need to concentrate efforts on strengthening cyber resilience and preventing aggression in cyberspace. It is crucial to enhance rapid response teams, work on standards, build mutually beneficial partnerships, and establish joint cyber aggression response teams.

The main goal is to raise awareness about the threats. Digital security and cyber hygiene must become part of everyday life for both ordinary citizens and leaders.

Security standards serve as the barrier between us and the enemy. This barrier exists in every smartphone, computer, registry, and company system.

Russia's cyberattacks on Ukraine show how cyber can enable military and political goals. Russian criminal groups coordinate closely with intelligence agencies like the GRU, FSB, and military. Objectives are not just extortion, but collecting intelligence on infrastructure and citizens to disrupt systems and undermine trust in government. Russia deliberately targets civilians, confirming its global cyber threat as a rogue state. Sanctions to isolate Russia from the internet are warranted.

With the war ongoing, critical infrastructure protection must be a top priority to defend civilians, especially in winter. Cyber threats are the main danger to NATO members, who have increased cyber spending and policymaking in response. Critical infrastructure cyber resilience remains vital. All of Ukraine's cyber defences must prioritize securing critical systems.

Overall, Russia weaponizes cyber to support kinetic operations and political aims. Close coordination between Russian state hackers, military, and criminals make cyberattacks a systemic threat. Protecting civilians and critical systems is imperative, requiring global isolation of Russia from the internet, together with resilient cyber defences, especially of critical infrastructure of Ukraine and partner countries.

References

1. Defending Ukraine: Early Lessons from the Cyber War [Електронний ресурс] // Microsoft. – Режим доступу : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

2. *Lewis J. A.* Cyber War and Ukraine [Електронний ресурс] / J. A. Lewis // SCIS. – Режим доступу : https://www.csis.org/analysis/cyber-war-and-ukraine.

3. *Пшетачник Я.* Війна Росії проти України: хронологія кібератак [Електронний ресурс] / Я. Пшетачник, С. Тарпова ; Дослідницька служба Європейського парламенту // European Parliament. – Режим доступу : https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf.

4. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс] : Указ Президента України № 96/2016 від 15 березня 2016 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/96/2016#n2.

5. News [Електронний ресурс] // State Service of Special Communications and Information Protection of Ukraine. – Режим доступу : https://cip.gov.ua/en/news.

6. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України № 2163-VIII від 5 жовтня 2017 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/ 2163-19#Text.

7. *Spinu N.* Ukraine Cybersecurity Governance Assessment [Електронний ресурс] / N. Spinu // DCAF. – Режим доступу : https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf.

8. *Black D.* Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences [Електронний ресурс] / D. Black // IISS. – Режим доступу : https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/03/russias-war-in-ukraine-examining-the-success-of-ukrainian-cyber-defences.pdf.

9. *Burt T.* Russian cyberattacks pose greater risk to governments and other insights from our annual report

[Електронний ресурс] / T. Burt // Microsoft. – Режим доступу : https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021.

10. *Шиповський В. В.* Система показників оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури [Електронний ресурс] / В. В. Шиповський // Захист інформації. – 2023. – Том 25, № 1. – С. 37–45. – Режим доступу : https://doi.org/10.18372/2410-7840.25.17597.

11. *Shypovskyi V.* Enhancing the factor analysis of information risk methodology for assessing cyberresilience in critical infrastructure information systems [Електронний ресурс] / V. Shypovskyi // Political Science and Security Studies Journal. – 2023. – Vol. 4, No 1. – P. 25–33. – Режим доступу : https://doi.org/10.5281/zenodo.7876556.

12. An overview of Russia's cyberattack activity in Ukraine [Електронний ресурс] : Special Report: Ukraine // Microsoft. – Режим доступу : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

13. Cyber Threats Snapshot, the latest report on attacks, vulnerabilities and threat actors in Q2 2022 [Електронний ресурс] // Leonardo. Cyber & Security. – Режим доступу : https://cybersecurity.leonardo.com/en/news-and-stories-detail/-/detail/cyber-threats-snapshot-q2-2022.

14. Q3 2023 Report [Електронний ресурс] // State Cyber Protection Center of the State Service of Special Communications and Information Protection. – Режим доступу : https://scpc.gov.ua/en/articles/327.